DIGITAL VURDERING OG EKSAMEN

-

EN JURIDISK VURDERING

VÅREN 2014

VERSJON 1.0

Et samarbeidsprosjekt utført på oppdrag fra Ekspertgruppen for Digital vurdering og eksamen av representanter fra:

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn

Norgesuniversitetet og Universitets- og høgskolerådet har i samarbeid opprettet en ekspertgruppe for digital vurdering og eksamen. I lys av at det nasjonalt er et behov for å få en oversikt og gjennomgang av juridiske utfordringer knyttet til gjennomføringen av digitale vurderinger og eksamen, ble Märtha Felton og Maren Jegersberg ved Universitetet i Oslo bedt om å lede et arbeid hvor juridiske problemstillinger knyttet til digital vurdering og eksamen skulle vurderes. Arbeidet er gjennomført med dugnadsinnsats, hvor ti representanter fra UiB, NTNU, UiT, UiA, UiN, HiST og UiO deltok. Av disse ti deltok fem jurister samt fem representanter med studieadministrativ kompetanse.

I begynnelsen av april 2014 ble det avholdt et to dagers arbeidsmøte i Oslo. Målet med møtet var å avklare, diskutere og systematisere problemstillinger knyttet til digital vurdering og eksamen, slik at vi hadde et så godt som mulig utgangspunkt før vi startet å skrive utredningen. Utredningen har blitt utformet som et samarbeid på den måten at juristene fra UiB, UiA, NTNU og UiO har hatt ansvar for å utrede hver sine grupper av problemstillinger, mens de resterende i gruppen har bidratt med kommentarer, innspill og praktisk informasjon.

Universitets- og høyskolesektoren er i full utvikling og omstillingsprosess når det kommer til digitalisering, og vi er sikre på at vi bare har sett begynnelsen. Per i dag har noen institusjoner kommet godt i gang med digitalisering av eksamen og vurderingsformer, mens andre ikke har startet opp. I alle tilfeller må alle institusjonene forberede seg på en ny hverdag med digitalisering av læremidler, undervisning og vurderingsformer. Dette betyr at vi alle må tilpasse oss nye juridiske problemstillinger – som allerede eksisterer. I tillegg må vi være forberedt på at nye dukker opp i fremtiden. Vi anser at det derfor vil være behov for å foreta en revidering av dette arbeidet om et år eller to, og arbeidsgruppen har derfor valgt å kalle denne utredningen versjon 1.0.

1.2 Deltakere i arbeidsgruppen

Greta Hilding	Leder Studiesekreteriatet	Universitetet i Agder
Marianne Seim	Rådgiver, Universitetsdirektørens kontor	Universitetet i Bergen
May Liz Bjørnevik Tho	Rådgiver, Rektors stab	Norges teknisk-naturvitenskapelige universitet
Märtha Felton	Seniorrådgiver, IT-direktørens stab	Universitetet i Oslo
Maren Magnus Jegersberg	Rådgiver, IT-direktørens stab	Universitetet i Oslo
Liv Tande	Rådgiver, Studieadministrasjonen	Universitetet i Nordland
Agnes Gullingsrud Fjeldstad	Rådgiver, Utdanningstjenester	Universitetet i Tromsø

Kjersti Møller	Seniorrådgiver, Studier, kommunikasjon og bibliotek	Høgskolen i Sør-Trøndelag
Judith Morland	Kontorsjef, Studieadministrativ avdeling	Universitetet i Bergen
Knut Veium	Seksjonssjef, Seksjon for studieadministrative støttesystemer	Norges teknisk-naturvitenskapelige universitet

1.3 Definisjon, avgrensning og plan for utredningen

Arbeidsgruppen har i arbeidet med utredningen lagt til grunn at *digital eksamen* må forstås som *skriftlig eksamen ved bruk av digitale verktøy / hjelpemidler.* Vi har avgrenset mot muntlig eksamen og andre typer vurderingsformer.

Slik vi ser det vil ikke innføring av en digital eksamen endre vurderingsformen, og det betyr også at rettighetene og pliktene etter blant annet universitets- og høyskoleloven og forvaltningsloven ikke endres. I arbeidet med å identifisere relevante juridiske problemstillinger knyttet til digital eksamen har vi sett at det på sikt også kan være et behov for sektoren å foreta juridiske vurderinger knyttet til andre og eventuelt nye vurderingsformer.

I arbeidet med utredningen har vi lagt til grunn eksamensprosessen fra begynnelse til slutt. Det vises her til en skisse laget ved NTNU, se vedlegg 1. Ut i fra denne prosessen har vi tatt utgangspunkt i tre gjennomføringssituasjoner for digital eksamen som ligger til grunn for vurderingene i utredningen selv om de ikke eksplisitt nevnes konsekvent:

- Eksamen på institusjon på institusjonens utstyr
- Eksamen på institusjon med eget utstyr
- Eksamen utenfor institusjon på eget utstyr

Vi har valgt å dele utredningen i fem hovedtemaer med underproblemstillinger.

Hovedtemaene er:

- Bruk av studentens eget utstyr ved gjennomføring av digital eksamen.
- Administrative problemstillinger.
- Rettigheter, plikter og ansvar.
- Krav til autentisering.
- Behandlinger av personopplysninger relatert til gjennomføring av digital eksamen.

For å gjøre innholdet i utredningen leser- og bruksvennlig har vi der hvor det er naturlig laget problemstillinger med påfølgende vurderinger og konklusjoner. Underveis har vi definert de ulike begrepene som brukes med henvisning til kilder. For noen av problemstillingene vil det ikke være mulig å konkludere generelt for hele sektoren ettersom det er vurderingen hver enkelt institusjon må foreta selv for hvert tilfelle som dukker opp. Vår sektor består av institusjoner av forskjellige størrelser, som tilbyr forskjellige typer studier og som har mange forskjellige typer studenter. Det gjør at en vurdering kan konkluderes forskjellig avhengig av hvilken institusjon som foretar den. I disse tilfellene har vi forsøkt å sette opp de vurderingstemaene som kreves etter lov og forskrift, samt de vurderingstemaene vi mener må eller bør være med slik at institusjonen bedre skal være i stand til å foreta de lovpålagte vurderingene.

For noen av delene i utredningen har det ikke vært naturlig å sette opp problemstillinger, men vi har gitt en oversikt over hva gjeldende regelverk omfatter og hva det betyr for den enkelte institusjon.

Vi ser at særlig for de problemstillingene hvor vi ikke kan gi en generell konklusjon, kan det være utfordrende for den enkelte institusjon selv å foreta vurderingen. Her må institusjonen være oppmerksom på at de, for å kunne ta i bruk en løsning, må foreta de lovpålagte vurderingene ellers vil de bryte loven. Noen institusjoner kan hende ikke har nødvendig kompetanse for å foreta disse vurderingene, og i disse tilfeller må dette hentes eksternt.

2 Bruk av studentens eget utstyr ved gjennomføring av digital eksamen

Kapittelet er skrevet av Greta Hilding, UiA.

2.1 Problemstilling

Kan institusjonene stille krav om at studenter bruker egen bærbar datamaskin under eksamen på institusjonen?

Avgrensning: I de tilfeller der studenter søker om å avlegge digital eksamen utenfor institusjonen vil det normalt være en forutsetning at studenten benytter egen datamaskin. Denne situasjonen drøftes derfor ikke.

Jeg vil også vurdere om det foreligger noen juridiske hindringer til at studenten frivillig bruker eget utstyr til å gjennomføre eksamen.

2.1.1 Rettslig grunnlag

Spørsmålet om hvorvidt universiteter og høyskoler kan kreve at studenter bruker egen datamaskin under gjennomføring av digital eksamen må drøftes med utgangspunkt i bestemmelsene i lov om universiteter og høyskoler[1] (heretter kalt uhl) § 7-1 om egenbetaling samt forskrift om egenbetaling ved universiteter og høyskoler[2], fastsatt av Kunnskapsdepartementet (heretter kalt egenbetalingsforskriften).

Uhl § 7-1 (1) lyder:

§ 7-1. Egenbetaling

(1) Statlige universiteter og høyskoler kan ikke kreve egenbetaling fra studenter for ordinære utdanninger som fører frem til en grad eller yrkesutdanning. Departementet kan i særskilte tilfeller, etter søknad, godkjenne unntak fra denne bestemmelse.

§ 3-3 (1) i forskrift om egenbetaling ved universiteter og høyskoler lyder:

§ 3-3. Andre utgifter knyttet til studiene

(1) For studieprogrammer eller fag/emner der institusjonene ikke kan kreve egenbetaling etter forskriftens § 3-1 og § 3-2, kan institusjonen heller ikke kreve betaling av studenter utover reelle

[1] Lov om universiteter og høyskoler, LOV-2005-04-01-15
[2] FOR-2005-12-15-1506

kostnader knyttet til læremidler. Eventuelt vederlag for vernet materiale etter opphavrettslovgivningen kan inngå i betalingsgrunnlaget. Institusjonene kan ikke ta betaling for studieinformasjon.

2.1.2 Vurdering

Det har skjedd betydelige endringer i høyere utdanning siden 2005, da egenbetalingsforskriften ble fastsatt. Digitale verktøy tas i økende grad i bruk i studier innen alle fagområder. Digitale læringsplattformer som Fronter eller It's learning har i mange år vært brukt til innlevering av ulike typer oppgaver og til kommunikasjon mellom lærere og studenter. Tilsvarende endringer har skjedd på de fleste samfunnsområder, i tråd med en ønsket politikk som blant annet kommer til uttrykk i det årlige digitaliseringsrundskrivet og i endringer i forvaltningsloven med forskrifter som i økende grad legger til rette for elektronisk kommunikasjon med forvaltningen. Prisen på bærbare datamaskiner har gått betydelig ned de siste årene. Studenter som har fullført videregående skole de senere år, er vant til å bruke bærbar datamaskin på skolen.

Spørsmålet er om disse endringene har betydning for hva som skal regnes som læremidler etter egenbetalingsforskriften § 3-3, dvs. om den generelle utviklingen i samfunnet gjør at det er rimelig at studenter finansierer bærbar datamaskin, på samme måte som det forventes at de finansierer lærebøker, kalkulator o.l.

Utdanningsutvalget i universitets- og høyskolerådet (UHR) behandlet spørsmålet i møte 12. februar 2013[3], og konkluderte da med at digitale hjelpemidler kan regnes som studiemateriell og at man kan forutsette at studenter stiller med PC. Det framgår imidlertid også at studentrepresentantene mente det ikke er en selvfølge at alle studenter har PC, og ikke ønsker at studentene blir tillagt et ansvar for å skaffe seg pc. Vedtaket i UHRs utdanningsutvalg er ikke basert på en juridisk utredning.

Kunnskapsdepartementet uttalte seg i 2006 om hvorvidt en institusjon under Uhl. kan pålegge studenter å kjøpe en bærbar PC[4]. Departementet uttalte da:

Det følger av forskrift av 15.12.2005 nr. 1506 om egenbetaling ved universiteter og høyskoler §3-3 første ledd at institusjonene ikke kan kreve betaling av studenter utover reelle kostnader knyttet til læremidler. Med «læremidler» menes materiell som studentene med rimelighet har

[3] http://www.uhr.no/rad_og_utvalg/utvalg/utdanningsutvalget/motereferat?d=2013
[4] Brev til Politihøgskolen dat. 05.05.2006

måttet finansiere slik som lærebøker, kompendier, kopier, utskrifter, papir og lignende. Infrastruktur som PC og materiell som kan sidestilles med undervisning faller utenfor.

Det følger av overstående at et pålegg fra høyskolen om bærbar PC, vil være i strid med gjeldende regelverk om egenbetaling for institusjoner som faller inn under lov om universiteter og høyskoler.

Kunnskapsdepartementet har våren 2014 bekreftet at man fortsatt anser et krav om at studenter skal ha egen bærbar datamaskin å være i strid med Uhl. og egenbetalingsforskriften.

Konklusjon: Universiteter og høyskoler har pr. i dag ikke hjemmel for å kreve at studenter skal benytte egen bærbar datamaskin ved gjennomføring av digital eksamen.

Foreligger det juridiske hindringer til at studenten frivillig bruker eget utstyr til å gjennomføre eksamen?

Jeg ser ikke noe til hinder for at institusjonene tillater studenter å bruke egen datamaskin under eksamen så lenge eksamen kan foregå på en betryggende måte. Med betryggende menes her f.eks. at kandidatene ikke får tilgang til materiale som er lagret på deres private maskiner under digital eksamen med ingen eller begrensede hjelpemidler.

På den annen side vil det ikke være en rettighet for studentene å bruke egen datamaskin ved digital eksamen. Institusjonene vil kunne pålegge studentene å bruke institusjonens datamaskiner. En slik avgjørelse vil ikke være et enkeltvedtak etter fvl. § 2 første ledd bokstav b) bl.a. fordi avgjørelsen ikke er bestemmende for studentenes rettigheter og plikter. Studentene vil dermed ikke kunne påklage en avgjørelse om at digital eksamen skal gjennomføres på institusjonens datamaskiner.

Inntil universiteter og høyskoler har en klar hjemmel for å pålegge studentene å ha egen bærbar datamaskin, vil enhver student kunne kreve å bruke institusjonens utstyr ved digital eksamen. Av hensyn til planleggingen av digital eksamen vil institusjonene kunne sette en frist for at studentene melder behov for å benytte institusjonens datautstyr. Det er ikke anledning til å kreve at studentene begrunner hvorfor de ønsker å bruke universitetets/høyskolens datamaskin.

Institusjonene har sannsynligvis heller ikke hjemmel for å nekte studenter adgang til digital eksamen selv om de ikke på forhånd har meldt behov for å bruke institusjonens datautstyr eller har bekreftet at de vil bruke eget utstyr, ettersom bestemmelsene i uhl og

egenbetalingsforskriften vil gjelde foran eventuelle avtaler med studentene. Institusjonene må ta høyde for dette enten ved å ha et visst antall maskiner i reserve eller legge til rette for at studenter kan gjennomføre eksamen uten datamaskin. Sistnevnte løsning kan imidlertid medføre klage over formelle feil etter uhl § 5-2 dersom studentene mener at eksamen uten bruk av datamaskin kan ha påvirket deres prestasjon under eksamen.

2.2 Konklusjon

En institusjon har ikke hjemmel til å kreve at studenter skal benytte egen bærbar datamaskin ved gjennomføring av digital eksamen på institusjonen.

3 Administrative problemstillinger

Kapittelet er skrevet av Greta Hilding, UiA.

3.1 Innledning

Innledningsvis i dette kapittelet drøftes hvorvidt henholdsvis studenter og ansatte kan reservere seg mot digital eksamen og i hvilken grad institusjonene er forpliktet til å legge til rette for alternativ gjennomføring av eksamen. Videre drøftes spørsmål knyttet til bl.a. lagring av, og innsyn i, ulike typer dokumenter i tilknytning til eksamen. Avslutningsvis i kapittelet pekes det på noen momenter som bør vurderes ved revisjon av lokalt regelverk for å tilpasse dette til digital eksamensgjennomføring.

3.2 Kan studenter reservere seg mot digital eksamen?

3.2.1 Problemstilling

Kan studenter reservere seg mot digital eksamen, dvs. er det en rettighet for studenter å kunne avlegge eksamen uten bruk av digitale verktøy?

3.2.2 Rettslig grunnlag

Problemstillingen er ikke direkte regulert i lov eller forskrifter.

Forvaltningsloven[5] (fvl) § 15 a og forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) inneholder generelle bestemmelser om adgangen for forvaltningsorganer til å benytte elektronisk kommunikasjon, og vilkårene for dette. Iflg. eForvaltningsforskriften[6] § 9 kan privatpersoner reservere seg mot å motta bestemte typer meddelelser elektronisk fra forvaltningen, bl.a. melding om enkeltvedtak og forhåndsvarsel. Fvl og eForvaltningsforskriften kan være relevante for drøftingen av spørsmålet om studenters eventuelle rett til å reservere seg mot digital eksamen. Problemstillingen må også drøftes i lys av uhl. med forskrifter.

3.2.3 Vurdering

Det kan tenkes at studenter vil søke om eksamen uten bruk av digitale verktøy som særordning/tilrettelegging – se punkt 3.3. I slike tilfelle vil det være opp til institusjonen å

[5] Lov om behandlingsmåten i forvaltningssaker, LOV-1967-02-10
[6] Forskrift om elektronisk kommunikasjon med og i forvaltningen, FOR-2004-06-25-988

avgjøre om vilkårene for tilrettelegging er oppfylt, og studenten vil kunne få avslag på søknaden. Hvis studenter derimot har rett til å reservere seg mot digital eksamen på samme måte som man kan reservere seg mot å motta informasjon elektronisk fra forvaltningen, vil institusjonene være forpliktet til å legge til rette for en alternativ gjennomføring av eksamen uavhengig av studentens begrunnelse for å ønske dette.

Spørsmål om rett til reservasjon mot digital eksamen bør sees i sammenheng med det faglige innholdet i studiene. Nasjonalt kvalifikasjonsrammeverk for høyere utdanning[7] er fastsatt med hjemmel i uhl § 3-2. Iflg. dette kvalifikasjonsrammeverket skal kandidater på bachelornivå bl.a. ha oppnådd følgende læringsutbytte i form av kunnskaper, ferdigheter og generell kompetanse:

- kan oppdatere sin kunnskap innenfor fagområdet
- kan beherske relevante faglige verktøy, teknikker og uttrykksformer
- kan planlegge og gjennomføre varierte arbeidsoppgaver og prosjekter som strekker seg over tid, alene og som deltaker i en gruppe

Det er vanskelig å se for seg hvordan dette, og andre elementer i kvalifikasjonsrammeverket, skal kunne oppnås uten bruk av digitale verktøy underveis i studiene. Allerede i dag er bruk av digitale verktøy en forutsetning for å oppnå læringsutbyttet i mange studier, og det må antas at bruken av slike verktøy vil øke i takt med den teknologiske/digitale utviklingen. Læringsutbytte som forventes oppnådd ved bruk av digitale verktøy i studiene, må kunne testes ved digital eksamen. En rett til å reservere seg mot digital eksamen vil dermed kunne komme i konflikt med Uhl. med forskrifter.

Jeg mener at bestemmelsene om reservasjonsrett i eForvaltningsforskriften ikke gir støtte for at det foreligger en rett for studenter til å reservere seg mot digital eksamen. En person som reserverer seg mot å motta meddelelser fra det offentlige, vil kunne kommunisere med forvaltningen på en alternativ, fullgod måte. For studenter som måtte ønske å reservere seg mot digital eksamen, vil det ikke alltid foreligge et fullgodt, ikke-digitalt alternativ.

3.2.4 Opplæring i bruk av verktøyet for digital eksamen

Med utgangspunkt i institusjonenes generelle ansvar for gjennomføringen av eksamen, vil institusjonene ha plikt til å tilby eksamenskandidatene opplæring i bruk av verktøyet som

[7] http://www.regjeringen.no/nb/dep/kd/tema/hoyere_utdanning/nasjonalt-kvalifikasjonsrammeverk.html?id=564809

brukes ved digital eksamen, enten før eksamen eller i form av brukerstøtte under eksamen. Manglende tilbud om opplæring vil kunne bli ansett som en formell feil etter uhl. § 5-2 dersom dette medfører at en kandidat ikke kommer i gang med eksamen eller ikke får lastet opp sin besvarelse.

Tilbud om opplæring kan f.eks. være i form av en opplæringsvideo. Hvis institusjonene har et tilbud om opplæring før eksamen, vil det være studentenes ansvar å tilegne seg nødvendig kunnskap. Det anbefales likevel å ha beredskap for brukerstøtte under eksamen. En problemstilling i denne sammenheng er hvorvidt studentoperatører (dvs. studenter som er ansatt/engasjert for å gi brukerstøtte), kan gi brukerstøtte til medstudenter under digital eksamen. Det kan oppstå spørsmål om habilitet og mulige formelle feil i disse situasjonene, så institusjoner som velger å bruke studentoperatører under eksamen bør ha rutiner for, i den grad det er mulig, å unngå at studentoperatørene hjelper i eksamenslokaler der gode venner, familie eller samboere/kjærester har eksamen.

3.2.5 Konklusjon

Studenter har ikke en ubetinget rett til å reservere seg mot å gjennomføre eksamen digitalt.

3.3 Særordning/tilrettelegging for studenter ved digital eksamen

3.3.1 Problemstilling

I dag er det mange studenter, eksempelvis dyslektikere, som har tilrettelagt eksamen i form av å bruke datamaskin der andre gjennomfører eksamen ved bruk av penn og papir. *Kan studenter søke om «omvendt» tilrettelegging, dvs. å gjennomføre eksamen ved bruk av penn og papir der andre studenter gjennomfører eksamen ved bruk av datamaskin?*

3.3.2 Rettslig grunnlag

Uhl. § 4-3 (5) lyder:

Institusjonen skal, så langt det er mulig og rimelig, legge studiesituasjonen til rette for studenter med særskilte behov. Tilretteleggingen må ikke føre til en reduksjon av de faglige krav som stilles ved det enkelte studium.

Ny diskriminerings- og tilgjengelighetslov[8] trådte i kraft 01.01.2014. Lovens § 17 lyder:

***§** 17. Rett til individuell tilrettelegging i skole- og utdanningsinstitusjoner*

Elever og studenter med nedsatt funksjonsevne ved skole- og utdanningsinstitusjoner har rett til egnet individuell tilrettelegging av lærested, undervisning, læremidler og eksamen for å sikre likeverdige opplærings- og utdanningsmuligheter.

Retten gjelder tilrettelegging som ikke innebærer en uforholdsmessig byrde. Ved vurderingen av om tilretteleggingen innebærer en uforholdsmessig byrde skal det særlig legges vekt på tilretteleggingens effekt for å nedbygge funksjonshemmende barrierer, de nødvendige kostnadene ved tilretteleggingen og virksomhetens ressurser.

Det kan også helt unntaksvis tenkes at diskrimineringsloven om etnisitet[9] kan komme til anvendelse i forhold til studenter som av religiøse- eller livssynsgrunner ikke forholder seg til datamaskiner og dermed ikke kan gjennomføre digital eksamen. Denne loven gjelder på alle samfunnsområder, og dermed også for utdanning, men har ingen spesielle bestemmelser om tilrettelegging i skole- og utdanningsinstitusjoner.

De fleste institusjonene har i tillegg bestemmelser om tilrettelegging av eksamen i sine lokale forskrifter.

I medhold av diskriminerings- og tilgjengelighetsloven er det fastsatt en forskrift om universell utforming av IKT-løsninger[10]. Iflg. forskriftens § 2 gjelder den «IKT-løsninger som retter seg mot allmennheten i Norge», og er begrenset til å gjelde nettløsninger og automater. Forskriften regulerer informasjon på universiteters og høyskolers nettsider, men har neppe direkte betydning for lukkede systemer som brukes ved digital eksamen, og i alle tilfeller vil den ikke omfatte tilrettelegging for enkeltpersoner, jf. § 2, 2. ledd, 2. setning.

3.3.3 Vurdering

Studenter som mener de har behov for tilrettelegging ved en digital eksamen, vil kunne søke om dette på samme måte som studenter i dag søker om tilrettelegging ved tradisjonell skriftlig eksamen. Søknader må behandles med utgangspunkt i nasjonalt og lokalt regelverk og studentens begrunnelse og dokumentasjon av sitt behov. Avgjørelsen vil være et enkeltvedtak som kan påklages etter reglene i forvaltningsloven. For studenter som omfattes

[8] Lov om forbud mot diskriminering på grunn av nedsatt funksjonsevne, LOV-2013-06-21-61
[9] Lov om forbud mot diskriminering på grunn av etnisitet, religion og livssyn, LOV-2013-06-21-60
[10] Forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger, FOR-2013-06-21-732

av diskriminerings- og tilgjengelighetsloven eller diskrimineringsloven om etnisitet vil sakene også kunne bringes inn for likestillings- og diskrimineringsombudet og likestillings- og diskrimineringsnemnda, jfr. diskriminerings- og tilgjengelighetsloven kap. 6 og diskrimineringsloven om etnisitet kap. 5.

Mange former for tilrettelegging, eksempelvis i form av utvidet eksamenstid, vil måtte håndteres på samme måte som ved tradisjonell skoleeksamen men ut fra en noe annen vurdering (se punkt 3.3.4). Videre drøftes bare den type tilrettelegging som innebærer at studenten gis anledning til å gjennomføre eksamen uten bruk av datamaskin.

Iflg. Forarbeidene til universitets- og høyskoleloven av 1995[11] tar bestemmelsen som tilsvarer nåværende uhl § 4-3(5) sikte på å «sikre funksjonshemmede og andre studenter med særskilte behov, muligheter til å ta høyere utdanning». Noen studenter vil dermed kunne ha krav på tilrettelegging med hjemmel i uhl., men ikke i diskriminerings- og tilgjengelighetsloven.

Vilkåret i uhl. § 4-3 (5) om at tilrettelegging ikke skal medføre reduksjon av faglige krav må være oppfylt også ved tilrettelegging for studenter som omfattes av diskriminerings- og tilgjengelighetsloven eller diskrimineringsloven om etnisitet. Det vises her til følgende uttalelse i forarbeidene til uhl. av 1995[12]: «Bestemmelsen vil omfatte en stor og uensartet gruppe studenter, med ulike særskilte behov og varierende ønsker om tilrettelegging. Departementet mener derfor at bestemmelsen om at tilrettelegging ikke må føre til en reduksjon av de faglige krav, må bli stående. Bare de studenter som oppfyller alle de faglige krav som stilles i utdanningen, kan få vitnemål.»

Hvis studenter med nedsatt funksjonsevne kan dokumentere at de på grunn av funksjonsnedsettelse ikke kan gjennomføre digital eksamen, vil de ha krav på tilrettelegging dersom dette ikke fører til reduksjon av faglige krav (jfr. uhl § 4-3 (5)) og ikke innebærer en uforholdsmessig byrde (jfr. diskriminerings- og tilgjengelighetsloven § 17 andre ledd).

Når det gjelder studenter som ikke har nedsatt funksjonsevne men likevel søker om å gjennomføre eksamen uten bruk av datamaskin, antas det at søknader normalt vil være begrunnet i manglende kunnskaper/ferdigheter i bruk av datamaskin.

Som nevnt i punkt 3.2 er bruk av digitale verktøy i mange studier en forutsetning for å oppnå det angitte læringsutbyttet, og det vil ofte ikke være mulig å gjennomføre et studium uten å

[11] Ot.prp. nr. 40 (2001-2002) kap. 12.1.10, Til § 44 Læringsmiljø
[12] Ot.prp. nr. 40 (2001-2002) kap.9.1.4

bruke datamaskin. Innen noen studier vil imidlertid bruken av digitale verktøy underveis i studiet være så begrenset at manglende kjennskap til bruk av datamaskin kan være en reell problemstilling for noen studenter. Det samme vil kunne gjelde privatister, som etter uhl. § 3-10 på visse vilkår har rett til å gå opp til eksamen uten å være tatt opp til studiet, dvs. rett til å dokumentere sin kunnskap uten å ha vært student.

Hensynet til likebehandling av studenter er en viktig begrunnelse for bestemmelsene om tilrettelegging for studenter med funksjonsnedsettelse, men dette kan også være et moment i vurderingen av søknader om tilrettelegging for studenter uten nedsatt funksjonsevne. Institusjonene har et ansvar for at studentene har mest mulig like vilkår under eksamen, men studentene har også et ansvar for å lære seg bruk av datamaskin. Som et utgangspunkt må det antas at det er studentenes eget ansvar å lære seg grunnleggende bruk av datamaskin, men institusjonens ansvar å gi undervisning i bruk av spesialprogramvare. Hvis en student behersker bruk av datamaskin så dårlig at dette vil være en vesentlig ulempe under digital eksamen, må det vurderes om vedkommende kan ha krav på tilrettelegging etter uhl. § 4-3(5). Jeg kan ikke se at studenter uten nedsatt funksjonsevne vil ha noe rettslig krav på tilrettelegging i form av å gjennomføre eksamen uten datamaskin. Institusjonene vil likevel kunne innvilge søknad om å skrive besvarelsen med penn dersom dette ikke medfører reduksjon av faglige krav. For studenter flest anses bruk av datamaskin under eksamen som en stor fordel, så det er liten grunn til å frykte at en ordning med «omvendt tilrettelegging» blir misbrukt.

For en svært liten studentgruppe kan religion eller livssyn være begrunnelsen for å søke om å gjennomføre eksamen uten bruk av datamaskin. For disse studentene må søknad om tilrettelegging også vurderes i forhold diskrimineringsloven om etnisitet. Hvis tilrettelegging kan gjennomføres uten reduksjon av faglige krav, antas det at diskrimineringsloven om etnisitet gir studenter krav på tilrettelegging. Institusjonene må vurdere hvilke krav som skal stilles til dokumentasjon i disse tilfellene.

Et spørsmål man bør ta stilling til ved «omvendt tilrettelegging» er hvorvidt studenter som skriver sin besvarelse med penn, skal få utvidet eksamenstid. Normalt skriver man fortere på datamaskin enn med penn, og man har fordelen av redigering i tekstbehandlingsprogram. Eventuelle bestemmelser om utvidet eksamenstid for studenter med «omvendt tilrettelegging» bør tas inn i institusjonenes lokale forskrifter, se punkt 3.8.

3.3.4 Studentgrupper som har hatt tilrettelegging i form av bruk av datamaskin ved tradisjonell skriftlig eksamen

Som nevnt innledningsvis i kapittelet har mange studenter hatt tilrettelagt eksamen i form av å bruke datamaskin der andre gjennomfører eksamen ved bruk av penn og papir. Ved mange institusjoner innvilges f.eks. dyslektikere normalt også utvidet eksamenstid. Disse studentene har hatt dokumentasjon fra f.eks. logoped eller lege som dokumenterer hvilken tilrettelegging de har behov for å kompensere for nedsatt funksjonsevne ved tradisjonell skriftlig eksamen. Ved digital eksamen må det gjøres en ny vurdering m.h.t. behovet for særordning. Det skal nå vurderes om studentene har nedsatt funksjonsevne ved digital eksamen, og hvilken tilrettelegging de evt. har behov for i en slik eksamenssituasjon. Dette vil stille andre krav til dokumentasjonen av behovet for tilrettelegging, og kanskje også til den informasjonen institusjonene gir om tilrettelegging på sine nettsider. Hver institusjon vil måtte vurdere behovet for endrede rutiner og/eller oppdatering av informasjon til studentene.

Noen institusjoner gir studenter med dysleksi anledning til å legge attest fra logoped ved eksamensbesvarelsen. Det må finnes tekniske løsninger for å håndtere slike og eventuelle andre vedlegg til sensorer, digitalt. Opplysninger om studenters helseforhold er sensitive personopplysninger, jfr. personopplysningsloven[13]§ 2. Behandling (herunder oppbevaring) av for eksempel logopedattester som inneholder opplysninger om studentens helseforhold må dermed oppfylle kravene til behandling av sensitive personopplysninger i personopplysningsloven.

3.3.5 Konklusjon

Eksamenskandidater vil kunne ha krav på tilrettelegging i form av å ta eksamen ved bruk av penn og papir i stedet for å gjennomføre digital eksamen. Slik tilrettelegging må ikke medføre at faglige krav reduseres.

3.4 Kan ansatte pålegges digital eksamensgjennomføring

3.4.1 Problemstilling

Ved digital eksamen får sensorene tilgang til studentenes besvarelser digitalt. Noen av de verktøyene som brukes til digital eksamen (eks. WISEflow) gir muligheter bl.a. for å skrive inn kommentarer, og legger til rette for at hele sensurjobben kan gjøres digitalt. En heldigitalisert eksamensprosess vil innebære at all kommunikasjon mellom faglærere,

[13] Lov om behandling av personopplysninger, LOV-2000-04-14-31

sensorer og eksamensadministrasjonen skjer digitalt, bl.a. oversending av eksamensoppgaver, tilgang til studentenes besvarelser og oversending av sensurprotokoll.

Kan ansatte reservere seg mot å forholde seg til en slik digital prosess, herunder reservere seg mot å sensurere studentenes eksamensbesvarelser digitalt?

3.4.2 Rettslig grunnlag

Lov om universiteter og høyskoler[14] (universitets- og høyskoleloven) inneholder i § 4-3 bestemmelser om studentenes arbeidsmiljø, men loven har ingen tilsvarende bestemmelser om ansattes arbeidsmiljø. Ansattes arbeidsmiljø reguleres av de generelle reglene i arbeidsmiljøloven[15] (Aml). I tillegg gjelder diskriminerings- og tilgjengelighetsloven og diskrimineringsloven om etnisitet også i forhold til ansatte.

Aml § 4-1 (2) lyder:

Ved planlegging og utforming av arbeidet skal det legges vekt på å forebygge skader og sykdommer. Arbeidets organisering, tilrettelegging og ledelse, arbeidstidsordninger, lønnssystemer, herunder bruk av prestasjonslønn, teknologi mv. skal være slik at arbeidstakerne ikke utsettes for uheldige fysiske eller psykiske belastninger og slik at sikkerhetshensyn ivaretas.

Aml § 4-2 (2) lyder:

I utformingen av den enkeltes arbeidssituasjon skal:

……..

e) det gis tilstrekkelig informasjon og opplæring slik at arbeidstaker er i stand til å utføre arbeidet når det skjer endringer som berører vedkommendes arbeidssituasjon.

3.4.3 Vurdering

En eventuell rett for ansatte til å reservere seg mot digital eksamen måtte også gjelde i forhold til andre digitale verktøy, eks. digitale læringsplattformer og ulike administrative systemer. Det er neppe tvil om at det, blant annet med utgangspunkt i arbeidsgivers styringsrett, ikke er adgang for ansatte til å reservere seg mot bruk digitale verktøy. Det kan

[14] Lov om universiteter og høyskoler, LOV-2005-04-01-15
[15] Lov om arbeidsmiljø, arbeidstid og stillingsvern mv., LOV-2005-06-17-62

være tvil om hvorvidt eksterne sensorer i denne sammenheng skal regnes som ansatte. Uansett kan spørsmål vedrørende digital eksamen reguleres i avtale mellom ekstern sensor og institusjonen. Denne problemstillingen drøftes derfor ikke nærmere.

Ansatte som ikke ønsker å benytte verktøy for digital eksamen og/eller sensurere digitalt, antas å ville begrunne dette enten med at de foretrekker å sensurere på papir og/eller ikke behersker verktøyet som brukes til digital sensurering, eller ut fra helsemessige forhold.

Arbeidsgiver vil etter aml. § 4-2(2) bokstav e) ha ansvar for å tilby opplæring i nye verktøy, og vil, med utgangspunkt i sin styringsrett, kunne pålegge ansatte å gjennomføre opplæring i bruk av verktøy for digital eksamen. Ansatte som påberoper seg unntak fra digital eksamen bare fordi de foretrekker en annen ordning, vil ikke ha noe rettslig krav på tilrettelegging.

Hvis en ansatt av helsemessige årsaker har problemer med å sensurere digitalt, vil arbeidsgiver måtte vurdere tilrettelegging av vedkommendes arbeidssituasjon ut fra bestemmelsene i aml. og diskriminerings- og tilgjengelighetsloven. Utskrift av besvarelsene vil sannsynligvis i de fleste tilfeller være tilstrekkelig.

I og med at verktøyene som brukes til digital eksamen, som nevnt gir muligheter for utskrift, vil ansatte som ønsker det, kunne skrive ut besvarelsene med mindre institusjonene innfører restriksjoner m.h.t. utskrift. Den pålagte endringen vil dermed først og fremst bestå i at tilgangen til besvarelsene og kommunikasjonen med eksamenskontoret skjer via et digitalt system.

3.4.4 Konklusjon

Ansatte har ikke rett til å reservere seg mot digital eksamen. For ansatte med spesielle behov må det vurderes tilrettelegging etter reglene i arbeidsmiljøloven og diskrimineringslovene.

3.5 Lagring av eksamensoppgaver, eksamensbesvarelser m.m.

3.5.1 Problemstilling

I forbindelse med digital eksamen utarbeides det en rekke dokumenter: eksamensoppgaver, oppmøteprotokoller, eksamensbesvarelser, eksamens-/sensurprotokoller og klage på sensur.

Må disseprotokollene lagres i godkjent arkivsystem, og eventuelt hvor lenge? Medfører digital eksamen noen endringer når det gjelder krav om lagring?

3.5.2 Rettslig grunnlag

Arkivlova[16] med tilhørende forskrifter inneholder bestemmelser om bl.a. arkivering og kassasjon. Arkivforskriften[17] § 2-6 stiller krav om journalføring av alle inngående og utgående dokumenter som etter offentleglova[18] regnes som saksdokumenter for virksomheten og er gjenstand for saksbehandling eller har dokumentasjonsverdi. Iflg. arkivlova § 9 kan arkivmateriale ikke avhendes eller kasseres uten at dette er i samsvar med forskrifter gitt i medhold av loven eller etter særskilt samtykke fra Riksarkivaren. Etter § 9 første ledd bokstav c kan personregister eller deler av personregister likevel slettes etter bestemmelsene i bl.a. personopplysningsloven, men først etter at det er innhentet uttalelse fra Riksarkivaren.

Eksamensbesvarelser, oppmøteprotokoller og sensurprotokoller inneholder personopplysninger[19], og omfattes dermed også av personopplysningsloven med forskrifter. Pol. § 28 første ledd lyder:

Den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.

Riksarkivaren har i medhold av arkivlova fastsatt regler for bevaring og kassasjon av eksamensbesvarelser m.v. ved universitet og høyskoler, se vedlegg 2 og 3. Reglene for universitetssektoren og de vitenskapelige høyskolene er fastsatt 13.03.2007. I vedtak av 03.10.2007 er de samme reglene gjort gjeldende for statlige høyskoler. Reglene omfatter lagring av eksamensbesvarelser, eksamensoppgaver og eksamensprotokoller. De to vedtakene følger som vedlegg, se vedlegg 2 og 3.[20]

Arkivforskriften §2-9 sier at offentlige organer normalt skal benytte et Noark-godkjent system ved elektronisk journalføring og arkivering. Noark ble utarbeidet som en kravspesifikasjon for

[16] Lov om arkiv, LOV-1992-12-04-126
[17] Forskrift om offentlege arkiv, FOR-1998-12-11-1193

[18] Lov om rett til innsyn i dokument i offentleg verksemd, LOV-2006-05-19-16
[19] Se punkt 6.2 for definisjon av personopplysninger og behandling av personopplysninger.
[20] Merk at kassasjonsreglene er under endring.

elektroniske journalsystemer i statsforvaltningen i 1984. Noark 5 er gjeldende standard i dag.[21]

Verktøyene som brukes ved digital eksamen er per i dag ikke utviklet for å tilfredsstille kravene til offentlige arkiv. For dokumenter som skal lagres i henhold til reglene i arkivlova, arkivforskriften og Riksarkivarens vedtak, vil dermed ikke lagring i de digitale eksamensverktøyene være tilstrekkelig. Med Noark 5 er det imidlertid enklere for systemleverandører å utvikle løsninger som tilfredsstiller kravene for elektronisk arkivering. Man trenger da en såkalt kjerne, som er beskrevet i Noark 5. Hvis verktøyene for digital eksamen utvikles med en slik Noark-kjerne, vil eksamensoppgaver, eksamensbesvarelser m.m. kunne lagres lovlig i disse systemene og da trenger man ikke overføring til sak/arkivsystemet. Når den tid kommer, vil man kunne ta uttrekk fra eksamensverktøyet og avlevere til Riksarkivet/Statsarkivet.

3.5.3 Lagring av eksamensoppgaver

Digital eksamen medfører ingen endringer m.h.t. krav om lagring av eksamensoppgaver. Iflg. Riksarkivarens vedtak om bevaring og kassasjon av eksamensbesvarelser skal eksamensoppgaver bevares, og ikke kasseres. Dette innebærer at eksamensoppgaver lagres for alltid, først i institusjonenes arkiv og senere i Riks- eller Statsarkivet.

Konklusjon: Eksamensoppgaver kan lagres i elektronisk eller manuelt arkiv.

3.5.4 Lagring av oppmøteprotokoller

Foreligger det en plikt til å lagre oppmøteprotokollen?

En oppmøteprotokoll er protokollen som gir oversikt over de eksamenskandidatene som er meldt opp og som oppfyller vilkårene for å gå opp til den konkrete eksamen. Ved oppmøte til tradisjonell skoleeksamen må kandidaten identifisere seg og normalt signere oppmøteprotokollen.

Lagring av oppmøteprotokoller er ikke regulert av Riksarkivarens vedtak om bevaring og kassasjon av eksamensbesvarelser m.m..

Eksamenskandidatenes oppmelding til eksamen skjer via utdanningsplanen i StudentWeb[22]. Oppmøteprotokollen er dermed en konsekvens av oppmeldingene, og ikke i seg selv en dokumentasjon av at en kandidat er oppmeldt til eksamen.

[21] Kilde: http://arkivverket.no/arkivverket/Offentleg-forvalting/Noark

Når det gjelder kontroll/dokumentasjon av at vilkår for å gå opp til eksamen i form av obligatoriske arbeidskrav o.l. er oppfylt, varierer rutinene fra institusjon til institusjon. Opplysninger om hvem som oppfyller vilkår for å gå opp til eksamen, kommer fra faglærer/emneansvarlig. Med mindre disse selv registrerer opplysningene i FS[23], vil det foreligge et eget dokument som viser hvem som fyller kravene for å gå opp til eksamen. Oppmøteprotokollen blir dermed en konsekvens ikke bare av studentenes oppmeldinger, men også av de opplysningene som kommer fra faglærer/emneansvarlig.

Endelig benyttes oppmøteprotokollen til at eksamenskandidatene ved signatur bekrefter at de er til stede under eksamen, eventuelt at eksamensinspektørene noterer hvem som er til stede. Ved digital eksamen logger studentene seg på det aktuelle verktøyet via Feide eller på annen måte, og institusjonene vil dermed ha dokumentasjon på hvem som har vært til stede.

Forutsatt at studentenes oppmeldinger og opplysninger om obligatoriske oppgaver o.l. finnes i andre dokumenter, og at opplysninger om tilstedeværelse under eksamen ivaretas i verktøyet for digital eksamen, kan jeg ikke se at oppmøteprotokoll ved digital eksamen vil være «saksdokumenter for virksomheten og er gjenstand for saksbehandling eller har dokumentasjonsverdi», jfr. arkivforskriften § 2-6 (se punkt 3.5.2). Dette innebærer at oppmøteprotokollen ikke er arkivverdig, men oppbevares så lenge den har administrativ betydning, og kan deretter kasseres.

Konklusjon: Oppmøteprotokollen er ikke arkivverdig. Den skal oppbevares så lenge den har administrativ betydning, og kan deretter kasseres. Det er opp til den enkelte institusjon å avgjøre hvor lenge den skal oppbevares.

3.5.5 Lagring av eksamensbesvarelser

Utdrag fra Riksarkivarens vedtak om bevaring og kassasjon av eksamensbesvarelser:

For eksamensbesvarelser (vurderingsmateriale) fra og med Kvalitetsreformen skal følgende bevares:

· *For Mastergraden eller tilsvarende utdanningsløp med klart forskningspreg bevares avsluttende oppgave.*

[22] Eksempelvis StudentWeb ved UiO: https://studweb.uio.no/as/WebObjects/studentweb2?inst=UiO
[23] http://www.fellesstudentsystem.no/

· *For Ph.d.-graden eller andre doktorgrader organisert som forskerutdanningsprogram bevares ett eksemplar av avhandlingen.*

· *For Dr.philos. bevares ett eksemplar av avhandlingen. Dokumentasjon av innholdet i prøveforelesninger bevares hvis det er krav om at slikt materiale skal innleveres.*

· *Refuserte avhandlinger skal bevares, dersom det ikke finnes en revidert versjon som er godkjent ved en senere innlevering etter fastsatt frist. Refuserte avhandlinger skal være godt merket for å hindre misbruk. Arkivverket vil gi innsyn etter gjeldende regler.*

Iflg. Riksarkivarens vedtak må institusjonene oppbevare eksamensbesvarelsene hos seg så lenge de er pliktige til det av administrative, forvaltningsmessige eller regnskapsmessige hensyn. Dette må reguleres i hver institusjons interne retningslinjer og rutiner.

Riksarkivarens vedtak omhandler ikke andre besvarelser enn masteroppgaver og doktorgradsavhandlinger etter kvalitetsreformen. En eksamensbesvarelse inneholder et kandidatnummer – besvarelsen ansees som avidentifisert[24], og med det inneholder den fremdeles personopplysninger. I henhold til bestemmelsene i personopplysningsloven §§ 8 og 9 kan ingen behandle personopplysninger uten å ha et rettslig grunnlag – behandlingsgrunnlag, og opplysningene skal etter § 28 ikke oppbevares lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Formålet med behandlingen av eksamensbesvarelsen er å vurdere den slik at kandidaten kan få en karakter. Når alle klagefrister er utløpt, klagebehandlingen er avsluttet og eventuell tilsynssensor[25] har avsluttet arbeidet med den aktuelle eksamen, bortfaller det opprinnelige formålet.

Det kan være aktuelt å lagre eksamensbesvarelser for vitenskapelige formål, eksempelvis for å undersøke utviklingen i faglig nivå over tid. Personopplysningsloven § 28 andre ledd gir hjemmel for likevel å lagre personopplysninger for historiske, statistiske eller vitenskapelige formål, «dersom samfunnets interesse i at opplysningene lagres klart overstiger de ulempene det kan medføre for den enkelte». Institusjonen må her foreta en dokumentert vurdering. Kravet til dokumentert interesseavveining innebærer at det må kunne påvises i hvilken sammenheng opplysningene skal brukes. Med andre ord kan man ikke beholde oppgavene fordi de kanskje en gang i fremtiden kan komme til å bli bruk i forskning. I denne vurderingen bør man bør man vurdere om man kan anonymisere oppgavene. I tillegg må man kjenne til at man skal foreta en streng avveining hvor hensynet til den enkelte registrerte

[24] Se nærmere forklaring av begrepet under punkt 6.2.
[25] Person som kvalitetssikrer sensuren som ledd i institusjonens kvalitetssikringsarbeid, ulik benevnelse og ulike ordninger ved institusjonene.

skal veie tungt. Dersom det er mulig å fjerne alle personidentifiserende opplysninger og allikevel beholde forskningsverdien så skal dette gjøres. Institusjonene vil i slike tilfelle kunne ha hjemmel for å lagre aktuelle besvarelser så lenge behovet er tilstede, men bestemmelsen gir ikke hjemmel for å lagre besvarelser for alltid. Ut over disse tilfellene må behandlingen (lagringen) opphøre når den ikke lenger er nødvendig for å gjennomføre det opprinnelige formålet. Behandlingen (lagringen) opphører ved at besvarelsene kasseres.

Konklusjon: Eksamensbesvarelser skal som hovedregel slettes når det ikke lenger foreligger administrative, forvaltningsmessige eller regnskapsmessige hensyn for lagring. Den enkelte institusjon må selv etablere rutiner, med frister, for sletting.

3.5.6 Lagring av eksamensprotokoller

Iflg. vedtakene om bevaring og kassasjon av eksamensbesvarelser skal eksamensprotokoller bevares. Det antas at Riksarkivaren her mener sensurprotokoll. Dette betyr at institusjonene ikke kan kassere/makulere sensurprotokollen, men skal overføre dem til Riksarkivet eller Statsarkivet (dette kan være ulikt for ulike institusjoner) når det ikke lenger er behov for å oppbevare protokollene ved institusjonen.

Iflg. Riksrevisjonen er sensurprotokollen i henhold til bestemmelser i Reglement for økonomistyring i staten[26] å anse som (indirekte) regnskapsmateriale fordi det er en del av den dokumentasjon som viser grunnlaget for de økonomiske bevilginger som gis det enkelte lærested, og skal derfor oppbevares i 10 år.

Reglene om lagring av eksamensprotokoller gjelder for både ordinær sensur og klagesensur.

Konklusjon: Eksamensprotokoller skal bevares ved institusjonen i 10 år, for så å overføres til Riks- eller statsarkivet.

3.5.7 Lagring av sensurklager

En sensurklage er et «saksdokument for virksomheten» som skal arkiveres i henhold til reglene i arkivlova og arkivforskriften. Heller ikke for sensurklager er det gitt bestemmelser om kassasjon verken i forskrifter eller i vedtakene om bevaring og kassasjon av eksamensbesvarelser m.m.. Med mindre det foreligger særskilt samtykke fra Riksarkivaren til å kassere sensurklager, skal disse oppbevares for alltid.

Konklusjon: Sensurklager skal som hovedregel bevares ved institusjonen for alltid.

[26] http://www.regjeringen.no/upload/FIN/Vedlegg/okstyring/Reglement_for_okonomistyring_i_staten.pdf

3.6 Innsyn i eksamensoppgaver, eksamensbesvarelser og sensurnotater

3.6.1 Problemstilling

I dette kapittelet drøftes retten til innsyn i ulike typer dokumenter som utarbeides i forbindelse med digital eksamen.

3.6.2 Rettslig grunnlag

Innsyn fra allmennheten reguleres av offentleglova[27] og innsyn fra parter i en forvaltningssak reguleres av forvaltningsloven.

Etter offentleglova § 3 kan alle som hovedregel kreve innsyn i «Saksdokument, journalar og liknande register for organet...».

Bestemmelser om partsinnsyn finnes i forvaltningsloven §§ 18 flg. Som part regnes «*person som en avgjørelse retter seg mot eller som saken ellers direkte gjelder*», jfr. fvl. § 2.

Overgang til digital eksamen medfører ingen endringer m.h.t. til retten til innsyn i de ulike dokumenttypene.

3.6.3 Innsyn i eksamensoppgaver

Innsyn etter offentleglova

Offentleglova § 26 gir hjemmel for å gi unntak fra innsyn for eksamensoppgaver «*inntil vedkommende eksamen eller prøve er halden*». Etter at eksamen er avholdt, har allmennheten dermed som utgangspunkt rett til innsyn i eksamensoppgaver.

Det foreligger en uttalelse fra Justisdepartementets lovavdeling vedr. innsynsrett i eksamensoppgaver til multiple choice-eksamener, JDLOV-2010-3631[28]. Det er spesielle problemstillinger knyttet til slike eksamener fordi universiteter og høyskoler ofte vil ønske å gjenbruke spørsmål som er gitt til multiple choice-eksamener. I nevnte uttalelse fra Justisdepartementets lovavdeling konkluderes det slik: «*Dette tilseier at offentleglova § 26 fyrste ledd andre punktum bør tolkast slik at ein eksamen med oppgåver som skal brukast på nytt, ikkje er «halden» etter denne føresegna, i den forstand at unntakshøvet for slike oppgåver ikkje opphøyrer sjølv om ein aktuell eksamen er gjennomført.*» Institusjonene vil ut

[27] Lov om rett til innsyn i dokument i offentleg verksemd, LOV-2006-05-19-16

[28] http://www.regjeringen.no/nb/dep/jd/agenda/tolkningsuttalelser/forvaltningsrett/tolkningsuttalelse-om-offentleglova/-26-forste-ledd-annet-punktum---sporsmal.html?id=623942

fra dette kunne avslå innsynsbegjæringer for multiple choice-oppgaver som inneholder spørsmål som skal gjenbrukes. Unntaket i offentleglova vil også kunne omfatte andre typer eksamener der de samme hensynene gjør seg gjeldende.

Innsyn etter forvaltningsloven

En kandidat som har vært oppe til en eksamen eller prøve vil kunne begjære partsinnsyn etter reglene i forvaltningsloven. Fvl. § 19 andre ledd lyder:

Med mindre det er av vesentlig betydning for en part, har han heller ikke krav på å få gjøre seg kjent med de opplysninger i et dokument som gjelder

…

b) andre forhold som av særlige grunner ikke bør meddeles videre.

I uttalelsen fra Justisdepartementets lovavdeling forutsettes det at det kan være av vesentlig betydning for en student å gjøre seg kjent med en eksamensoppgave, eksempelvis i forbindelse med begrunnelse og klage, og at innsyn dermed må gis. Spørsmålet er videre om studenter vil ha rett til kopi av eksamensoppgaven. Iflg fvl. § 20 første ledd bestemmer forvaltningsorganet ut fra hensynet til forsvarlig saksbehandling hvordan dokumentene skal gjøres tilgjengelig for partene. Hovedregelen i fvl. § 20 er at en part har rett til kopi av dokumentet. Flg. siteres fra JDLOV-2010-3631 vedr. multiple choice-oppgaver:

På bakgrunn av brevet hit legg vil til grunn at det vil føre til vanskar for NIH (og truleg andre utdanningsinstitusjonar) dersom det skal gjelde rett til kopi av eksamensoppgåver av den typen det her er tale om. Faren for at desse kopiane blir spreidde til andre studentar vil vere stor, og det vil ikkje vere praktisk mogleg å avgrense spreiinga om kopi fyrst blir gjeve. Konsekvensen vil etter alt å døme bli at oppgåvene ikkje kan brukast på nytt, noko som vil vanskeleggjere sjølve gjennomføringa av eksamen. Alternativet vil vere at eksamen ikkje får den funksjonen han skal ha, sidan studentane kan stå til eksamen gjennom rein pugging av aktuelle oppgåver. Det er klart at føremåla med retten til kopi etter forvaltningslova § 20 andre ledd fyrste punktum ikkje omfattar slike verknader.

Ein rett til kopi av eksamensoppgåver som er meint brukte på nytt, let seg såleis ikkje sameine med eksamenssystemet, heller ikkje ved partsinnsyn. Vidare er det eit sentralt moment at kandidatar som har reelt behov for å sjå oppgåvene i samband med klage og liknande, langt på veg vil kunne oppnå det same gjennom å få studere oppgåvene utan å få kopi, jf. konklusjonen i vårt brev 15. oktober 2002.

På denne bakgrunnen ligg det føre sterke grunnar som taler for at forvaltningslova § 20 fyrste ledd andre punktum i bestemte tilfelle bør tolkast innskrenkande. Vi går derfor ut frå at det ved partsinnsyn ikkje gjeld nokon absolutt rett til kopi av eksamensoppgåver når utlevering av kopi ikkje let seg sameine med eksamenssystemet.

Konklusjon:
Offentleglova: Som hovedregel kan innsyn i eksamensoppgaver avslås før eksamen er gjennomført. Etter at eksamen er avholdt må det som hovedregel gis innsyn.

Forvaltningsloven: Den som er part i en forvaltningssak – her eksamen, kan som hovedregel få innsyn i saksdokumenter - her eksamensoppgaven.

3.6.4 Innsyn i eksamensbesvarelser

Iflg. offentleglova § 26 kan det gjøres unntak fra innsyn for eksamensbesvarelser. Det er ikke satt noen vilkår i loven for slikt unntak. Hver institusjon må dermed fastsette rutiner for hvordan begjæringer om innsyn i eksamensbesvarelser etter offentleglova skal håndteres.

En eksamensbesvarelse vil kunne være et åndsverk etter åndsverkloven[29] § 2. Åndsverkloven gir opphavsmannen enerett til bl.a. å gjøre sitt åndsverk tilgjengelig for allmennheten. Studenten vil dermed måtte samtykke f.eks. til at besvarelsen gjøres tilgjengelig for andre studenter, ettersom offentleglova kun gir rett til innsyn og ikke til å publisere dokumenter man får innsyn i. Universiteter og høyskoler vil heller ikke ha noen hjemmel for å gjøre eksamensbesvarelser tilgjengelig for f.eks. andre studenter uten samtykke fra den/de aktuelle kandidater.

Dersom studenter ber om innsyn i sin egen besvarelse, reguleres dette av fvl. Fvl. § 20 første ledd 3. punktum lyder:

Eksamensbesvarelser og liknende prøver kan den som avlegger eksamen eller prøve, nektes adgang til inntil bedømmelsen er avsluttet.

Begrunnelse for bestemmelsen er at det kan skape vanskeligheter for sensurarbeidet om kandidater kunne kreve innsyn mens besvarelsene er hos sensorene. Ved digital eksamen vil studentene normalt få en elektronisk kopi av sin egen besvarelse slik at begjæringer om innsyn i egen besvarelse sjelden vil være aktuelt. Dersom en student ber om innsyn i andre kandidaters besvarelser, reguleres dette av offentleglova.

[29] Lov om opphavsrett til åndverk m.v., LOV-1961-05-12-2

Konklusjon:
Offentleglova: Som hovedregel kan innsyn i eksamensbesvarelser avslås. Hvordan denne bestemmelsen skal håndheves må besluttes på den enkelte institusjon. Ved etablering av rutiner må bestemmelsen om «merinnsyn» i offentleglova § 11 tas med i vurderingen.

Forvaltningsloven: Den som er part i en forvaltningssak – her eksamen, kan som hovedregel få innsyn i egen besvarelse etter at sensur foreligger.

3.6.5 Innsyn i sensurnotater

Enkelte verktøy for digital eksamen legger til rette for at sensorene kan legge inn kommentarer til den enkelte besvarelsen. Sensorene vil kunne benytte disse kommentarene i forbindelse med begrunnelse for sensur.

En eksamensbesvarelse med sensors kommentarer må anses som et internt dokument som er unntatt fra offentlighet etter offentleglova § 14.

Også i forhold til kandidatene antas det at besvarelsen med sensors kommentarer må anses som et organinternt dokument som kan unntas fra partsinnsyn etter fvl § 18 a. Kandidatene har rett til begrunnelse etter uhl § 5-3 (1). I begrunnelsen skal det etter uhl § 5-3 (2) gjøres rede for de generelle prinsipper som er lagt til grunn for bedømmelsen og for bedømmelsen av kandidatens prestasjon. Begrunnelse kan gis skriftlig eller muntlig etter sensors valg. Kommentarer til den enkelte besvarelse vil normalt ikke si noe om de generelle prinsippene som er lagt til grunn for bedømmelsen, og dermed ikke tilfredsstille lovens krav til en begrunnelse. Det vil imidlertid ikke være noe i veien for at institusjonene gir en kandidat innsyn i en kommentert versjon av sin besvarelse.

Konklusjon: Det er opp til den enkelte institusjon om de vil la studentene få innsyn i sensurnotater knyttet til studentens eksamen.

3.7 Rett til å gå opp til eksamen der kandidaten ikke er oppmeldt til eksamen

3.7.1 Problemstilling

Ved tradisjonell skriftlig eksamen følger mange institusjoner en praksis der kandidater som ikke står på kandidatlista, gis adgang til å gjennomføre eksamen mot å signere en erklæring om at vedkommende er innforstått med at besvarelsen ikke blir sensurert dersom hun/han ikke er oppmeldt og fyller vilkårene for å avlegge eksamen. Hvordan bør slike tilfeller håndteres ved digital eksamen?

3.7.2 Rettslig grunnlag

Det finnes ikke noe regelverk som direkte regulerer disse situasjonene, men bestemmelsene om formelle feil i uhl § 5-2 kan være relevante.

3.7.3 Vurdering

Studenter som er registrert i FS

Ved digital eksamen må kandidater som ikke står på kandidatlista, meldes opp til eksamen i FS og registreres i verktøyet for digital eksamen. Etter det som er opplyst, kan dette normalt ordnes raskt nok til at kandidaten kan gjennomføre eksamen uten forsinkelser. Alternativt vil man kunne gi personer som ikke er oppmeldt, anledning til å gjennomføre eksamen med penn og papir. Det siste kan imidlertid i ettertid medføre klage over formelle feil etter uhl. § 5-2 dersom studenten hadde rett til å avlegge eksamen, og det kan også tenkes at eksamensoppgaven forutsetter bruk av digitale verktøy slik at eksamen ikke lar seg gjennomføre uten datamaskin.

Med mindre man kan få avklart før eksamen om de aktuelle kandidatene er oppmeldt og oppfyller vilkårene for å gå opp til eksamen, bør kandidatene signere en erklæring om at besvarelsen bare vil bli sensurert dersom de nevnte vilkårene er oppfylt.

Studenter som ikke er registrert i FS

Helt unntaksvis kan det tenkes at personer møter til eksamen uten å være registrert i FS. Sannsynligheten for at dette skal skje er svært liten, men institusjonene bør ha rutiner for å håndtere eventuelle slike situasjoner. Hvis en person møter til eksamen uten å være registrert i FS, vil man ikke vite om vedkommende har noen tilknytning til institusjonen. Det kan dermed være en risiko ved å slippe personen inn i eksamenslokalet. Videre vil det være mer arbeidskrevende å få klargjort vedkommende for digital eksamen.

Sannsynligheten for at feilen i disse tilfellene ligger hos universitetet eller høyskolen vil være svært liten. Dette, i tillegg til den risiko som kan ligge i å gi uvedkommende adgang til et eksamenslokale, gjør at det anbefales å ikke la personer som ikke er registrert i FS få anledning til å gjennomføre digital eksamen. Hvis det skulle vise seg at det er gjort feil fra institusjonens side, må forholdet sannsynligvis anses som en formell feil etter uhl § 5-2 og vedkommende må tilbys ny eksamen.

Konklusjon: Den enkelte institusjon må før gjennomføring av eksamen etablere gode rutiner for hvordan de vil håndtere kandidater som møter opp til eksamen uten at de er oppmeldt.

3.8 Revidering av lokalt regelverk

Digital eksamen vil for de fleste institusjoner medføre behov for å revidere lokalt regelverk rundt eksamen. Digital eksamen medfører ikke grunnleggende endringer i rettigheter og plikter, se punkt 1.3, men regelverket må tilpasses digitaliseringen av eksamensprosessen.

Jeg vil i det følgende peke på noen momenter som bør vurderes:

- Behov for definisjon av digital eksamen?
- Behov for endringer m.h.t. type(r) eksamen som er tillatt?
- Behov for å endre regler om tillatte hjelpemidler?
- Skal åpent nett tillates ved digital skoleeksamen, eller bare ved hjemmeeksamen?
- Rutiner/frister for å avklare om studenter bruker egen datamaskin eller har behov for å bruke institusjonens utstyr
- Krav til type datamaskin, operativsystem og eventuelle andre krav når studenter bruker eget utstyr
- Rutiner/frister for å laste ned programvare på studentenes datamaskiner (bør være gjort før studenten møter i eksamenslokalet)
- Krav til opplæring i bruk av verktøy for digital eksamen
- Behov for at studentene møter tidligere i eksamenslokalet enn ved tradisjonell skoleeksamen?
- Behov for endringer i generelle regler om tilrettelegging/særordning?
- Regler for «omvendt» tilrettelegging, jfr. kap. 3.3?
- Behov for endringer i regler om fusk?
- Behov for endringer i eventuell instruks for eksamenskandidater?
- Behov for endringer i eventuell instruks for eksamensinspektører?

- Behov for endringer i eventuell instruks for faglærer/emneansvarlig?
- Behov for endringer i avtale med og/eller eventuell instruks for ekstern sensor?

For noen institusjoner kan det være hensiktsmessig å utarbeide egne retningslinjer for digital eksamen. Et eksempel på slike retningslinjer er fra Det juridisk fakultet ved Universitetet i Oslo: http://www.jus.uio.no/studier/regelverk/retningslinjer-for-digital-eksamen-ved-det-juridiske-fakultet.html

4 Rettigheter, plikter og ansvar

Kapittelet er skrevet av Marianne Seim, UiB.

4.1 Innledning

Dette kapittelet behandler institusjonenes plikter for utstyr og infrastruktur gjennom hele eksamensprosessen og hvilket ansvar institusjonene kan tenkes å ha for studenter som omfattes i denne sammenheng. I tillegg vil studentenes rettigheter og plikter knyttet til dette også bli gjennomgått. Gjennomgangen er ikke uttømmende, men behandler overordnede og sentrale spørsmål for eksamen. Tilsvarende er heller ikke regelverket uttømmende angitt og andre rettsregler enn de som gjennomgås her kan tenkes å være relevant.

4.2 Handlingsrom innenfor gjeldende lovverk

Universitets- og høyskolesystemet er i en rivende utvikling og omstillingsprosess når det gjelder digitale utfordringer.

Status per i dag er at institusjonene har ulik progresjon i forhold til de digitale utfordringene. Noen har ikke startet opp, noen er i utprøvningsstadiet og noen er relativt godt etablert. Det er imidlertid ingen av institusjonene som har digitalisert i sin fulle bredde. Det må kunne legges til grunn at den dagen institusjonene er kommet over i en ny fase med full digitalisering, både av lærebøker, undervisning og eksamen, vil nok både institusjonene og studentene forholde seg til et noe annet rettslig bilde med hensyn til innholdet av rettigheter og plikter.

Det er vanskelig å gi en uttømmende angivelse av lovverket i denne sammenheng, som en klar og entydig rettesnor knyttet til digitale spørsmål her. Overordnet regelverk knyttet til erstatningsrettslige spørsmål og universitets- og høyskoleloven selv, gir føringer for håndteringen av denne typen spørsmål. Imidlertid er klare rettslige hjemler for de ulike problemstillingene ikke alltid opplagt, slik at en del av vurderingene beror på skjønnsvurderinger og risikovurderinger, herunder hvor det er rimelig at risiko og ansvar plasseres mellom partene (institusjonen og studenten).

Utgangspunktet for denne delen vil imidlertid være bestemmelser i universitets- og høyskoleloven (uhl.) og skadeserstatningsloven (skl.).

4.3 Erstatningsrett/forsikring og generelle utgangspunkt

I det følgende er det erstatning knyttet til skade på studentens utstyr/PC som omtales. Det avgrenses mot skade på institusjonens eget utstyr påført av institusjonens egne ansatte eller av studenten selv. Dersom studenten volder skade på institusjonens utstyr, uaktsomt eller forsettlig, vil nok utgangspunktene i denne gjennomgangen kunne legges til grunn, men med annet ansvarsgrunnlag enn omtalt. Hvor praktisk denne gjennomgangen er, avhenger noe av i hvilken grad institusjonene har noe med privat PC å gjøre i det hele tatt (fysisk) eller om det er studenten selv som (fysisk) utfører installeringen i henhold til institusjonens instrukser. Dersom institusjonen selv utfører fysisk arbeid på studentenes PCer, vil denne gjennomgangen kunne gi noen føringer og også dersom institusjonens instrukser/pålegg (som type PC, type programvare) medfører skade.

Institusjonens potensielle erstatningsansvar vil kunne foreligge både i forhold til institusjonens «fysiske håndtering» av privat utstyr, men også et ansvar for at de instruksene som pålegges studenten, for å kunne gjennomføre eksamen på eget utstyr, fungerer. Institusjonene kan nok ikke fraskrive seg ansvar for studentens PC ved å la studenten selv utføre installeringen på egen PC. Det må imidlertid i hver sak vurderes konkret om skade skyldes studenten og/eller institusjonen. Det er ikke mulig å gi en uttømmende oversikt over alle typetilfeller her.

Utgangspunktene her kan brukes både i forhold til skade på studentenes utstyr oppstått i forberedelsesfasen og selve gjennomføringen av digital eksamen.

Institusjonen bør først og fremst jobbe preventivt for å forebygge skader. Skulle skade likevel skje, gis det her en kort oversikt over rettslige utgangspunktene for erstatningsvurdering samt at forsikringsaspektet kommenteres også i noen grad.

Institusjonene bør organiseres slik at de kan håndtere erstatningskrav fra studenter i forbindelse med skade oppstått i eksamenssammenheng. Når en skade oppstår, er det viktig at studenten melder raskt fra om dette til institusjonen, eller at institusjonen selv organiserer seg i forhold til å informere studenten om skade som oppstår når institusjonen selv har påført utstyret skade. Hvordan institusjonen organiserer seg for dette, ligger innenfor den enkelte institusjons egen autonomi å avgjøre, men det må kommuniseres tydelig til studentene hva som er rutinene i denne sammenheng.

Dersom skade inntreffer, er det viktig at institusjonen kartlegger fakta og får en oversikt over hendelsesforløpet:

- Hva har skjedd?
- Hvor har det skjedd?
- Hvem er involvert?
- Når skjedde det?
- Hvem er varslet?
- Mulig årsak?

Det er viktig å få kartlagt om skaden skjedde i forbindelse med institusjonens eller studentens aktivitet, og hva studentene er informert om på forhånd (hva er studenten ansvarlig for å holde seg orientert om av informasjon knyttet til digital eksamen) ol.

Denne kartleggingen er viktig for en mest mulig korrekt saksbehandling, samt vurdering av potensielt krav. Den er også viktig for å sikre at studentens rettigheter blir ivaretatt, sikre at like tilfeller blir behandlet likt (likebehandlingsprinsippet), at institusjonen tar ansvar når det foreligger ansvar og ikke minst for at institusjonen skal få en læringseffekt ut av hendelsen og forebygge nye hendelser. Deretter starter arbeidet med å finne ut hva som skal gjøres og av hvem, samt hvilket ansvar (erstatning, formelle feil etter uhl. § 5-2 ea.) som evt. foreligger for institusjonen.

4.3.1 Erstatning:

Problemstilling: Har institusjonen erstatningsansvar for skade på studentens utstyr/PC?

Erstatningsansvar for institusjonen forutsetter at tre vilkår er oppfylt; det må foreligge et ansvarsgrunnlag, et økonomisk tap og det må kunne etableres en årsakssammenheng mellom handlingen og studentens økonomiske tap. Samtlige vilkår må være oppfylt for at erstatningsansvar skal foreligge.

Sentrale ansvarsgrunnlag vil her være arbeidsgiveransvar etter lov om skadeserstatning (skl.) § 2-1 og ansvar på ulovfestet objektivt grunnlag.

Arbeidsgiveransvaret er et lovfestet ansvar der arbeidsgiver blir objektivt ansvarlig for ansattes uaktsomhet, dvs. selv om arbeidsgiver selv ikke kan bebreides for skaden. Det må likevel være utvist uaktsomhet eller forsett av noen innenfor virksomheten.

Arbeidsgiveransvaret er lovfestet i skl. § 2-1 nr. 1.

Arbeidsgiveransvaret omfatter både offentlige og private arbeidsgivere, jf. nr. 2: Med arbeidsgiver menes det offentlige og enhver annen som i eller utenfor ervervsvirksomhet har noen i sin tjeneste.

Det ulovfestede objektive ansvaret bygger på rettspraksis og går i hovedsak ut på at ansvar kan forekomme selv der det ikke er utvist skyld og det ikke finnes lover som regulerer et objektivt ansvar. Hovedprinsippet for det ulovfestede objektive ansvaret er at den som er nærmest til å bære ansvaret for en skade, vil måtte svare for det tapet som er inntruffet.

Bevisbyrden; Hvem har ansvaret for å bevise at det foreligger en skade og et økonomisk tap?

Hovedregelen er at den som krever å bli gitt en rett av motparten, har bevisbyrden. Krever studenten dekket sitt økonomiske tap for at PCen er skadet i eksamenssammenheng, vil i utgangspunktet studenten ha bevisbyrden.

Imidlertid kan det være gode grunner for at bevisbyrden skal legges på institusjonen, i alle fall dersom skaden har skjedd mens studentens utstyr var i universitetets varetekt. Begrunnelsen for dette er at det er institusjonen som har hatt de beste mulighetene for å sikre bevis i saken, slik at institusjonen må bevise at den ikke var ansvarlig for skaden.

For å oppfylle bevisbyrden i denne typen saker kreves det som utgangspunkt at det foreligger alminnelig sannsynlighetsovervekt, altså slik at det faktum som fremstår som mest sannsynlig legges til grunn.

I vurderingen av erstatningsansvar kan det tenkes at:

a) Institusjonen er ene og alene ansvarlig for skaden

b) Studenten er ene og alene ansvarlig for skaden

c) Medvirkende årsaker

Medvirkende årsaker skyldes både institusjonen og studenten (eksempelvis studentens PC hadde mangler som ikke ble oppdaget før skaden skjedde, studenten har ikke fulgt institusjonens instrukser ved forberedelse av maskinen til eksamen, i kombinasjon med skade fra institusjonens side)

Dersom det reises et erstatningskrav mot institusjonen, er dette vurderinger som det kan være relevant å gjøre alt etter hvordan sakens faktum er og hva som anses bevist og sannsynliggjort.

Det er vanskelig å legge generelle føringer og konklusjoner til grunn når det gjelder institusjonens erstatningsansvar, men generelt kan det legges til grunn som et utgangspunkt at dersom institusjonen er ansvarlig for skade skjedd på studentens utstyr, er institusjonen ansvarlig for å dekke tapet.

Hver sak her må imidlertid vurderes konkret både når det gjelder vurderingen av om vilkårene for erstatning er oppfylt og hva som legges til grunn som et økonomisk tap (hva er eksempelvis studentens PC verdt?). Utgangspunktet for vurderingen av tapet må være hva det koster å kjøpe/dekke en ny tilsvarende PC for studenten og ikke hva som helst av ny PC. En rettesnor her er at studenten skal stilles økonomisk som om skaden ikke var skjedd (forutsatt ansvar for institusjonen). Det følger av skadeserstatningsloven § 4-1 at erstatning for tingskade skal dekke den skadelidtes økonomiske tap.

Beregningen av det økonomiske tapet vil imidlertid avhenge av om skaden skyldes institusjonen alene eller om det er grunn til å legge noe av ansvaret også på studenten.

I henhold til det årlige tildelingsbrevet fra Kunnskapsdepartementet til institusjonene, har institusjonen fullmakt til selv å påta seg erstatningskrav opptil 250.000,- kr.

Konklusjon: Utgangspunktet er at institusjonen har et erstatningsansvar for skade på studentens utstyr/PC dersom institusjonen er ansvarlig for skaden.

4.3.2 Forsikring:

Institusjonen: Staten er selvassurandør, noe som innebærer at statlige utdanningsinstitusjoner ikke tegner forsikringer. Det ulovfestede selvassuranseprinsippet innebærer et forbud mot å tegne forsikring for virksomhetene som er en del av staten, og institusjonene tar derfor selv eventuelle erstatningsoppgjør. Dette gjelder med mindre det er uttrykkelig gitt samtykke til unntak fra selvassuranseprinsippet. Myndighet til å samtykke til unntak fra selvassuranseprinsippet, altså å gi adgang til å tegne forsikring i det private markedet, er lagt til Finansdepartementet.

Begrepsavklaring «Regress»:

I erstatnings- og forsikringsretten betyr regress at den som er ansvarlig for å betale for en skade, krever pengene tilbake fra den som er ansvarlig for at skaden oppstod. Dersom eksempelvis et forsikringsselskap har måttet betale for skade som institusjonen (skadevolder) er ansvarlig for, kan de på visse vilkår kreve pengene helt eller delvis tilbake fra skadevolderen.

Regler om erstatning for tingskade og annen formuesskade følger av skadeserstatningsloven kap. 4, spesielt relevant her er §§ 4-1, 4-2 og 4-3.

4.3.3 Dersom studenten bruker egen PC til gjennomføring av eksamen, kan da institusjon kreve:

1) At studenten går til anskaffelse av ett av alternative maskiner oppgitt av institusjonen?

Premisser for svaret:
Jeg legger til grunn for dette arbeidet at institusjonene må forholde seg til et gratisprinsipp når det gjelder spørsmål om det kan pålegges studentene å ha egen PC. I lys av dette, er det for digital eksamen i dag slik at dette er frivillig og at skriftlige eksamener også er et tilbud. Digital eksamen blir derfor et institusjonelt ressursspørsmål, hvor institusjonene kun kan avvikle digital eksamen dersom det kan lånes ut PCer til studentene som et alternativ til egen PC, eller dersom samtlige eksamenskandidater kan stille med egen PC. Dette er et ressursspørsmål som institusjonen må gjøre for den enkelte digitale eksamenen. Det kan således ikke planlegges for digital eksamen dersom det er et premiss at studenten selv har egen PC, hvis dette i realiteten ikke er gjennomførbart (jf. gratisprinsippet. Se mer under drøftelsen i kapittel 2).

Institusjonen kan derfor heller ikke pålegge studentene å kjøpe en bestemt maskin. Velger imidlertid studenten å avvikle eksamenen digitalt, må studenten forholde seg til de vilkår institusjonen setter for de tekniske løsningene. Det er institusjonen som garanterer for de tekniske løsningene, og studenten må forholde seg til det tilbudet som da gis. Ønsker studenten å avvikle eksamen på en PC som det ikke lar seg installere teknisk eksamensløsning på, så kan ikke studenten avvikle eksamen digitalt på egen PC, men må bruke institusjonens utstyr.

Konklusjon: Studentene må forholde seg til de vilkår institusjonen setter for de tekniske løsningene dersom de ønsker å gjennomføre eksamen på egen PC, men institusjonen kan

ikke kreve at studenten går til anskaffelse av ett av alternative maskiner oppgitt av institusjonen.

2) At studenten benytter spesifikk programvare?

Jf. svaret overfor.

Konklusjon: Studentene må forholde seg til de anbefalte tekniske løsningene og programvarene dersom de ønsker å bruke egen PC. Institusjonene kan ikke kreve at studenten benytter spesifikk programvare for å gjennomføre eksamen.

3) Må institusjonen holde programvaren for studentene eller kan institusjonen kreve at studentene kjøper lisenser selv?

Tilbud om digital eksamen, er et eksamensalternativ som institusjonen har ansvar for. Begrunnet i et gratisprinsipp og likhetsprinsipp (digitale eksamenskandidater skal likestilles med de som avvikler eksamen skriftlig), vil jeg i alle fall inntil videre mene at dette er det institusjonen som har ansvar for å tilby. Institusjonen kan ikke kreve at studentene kjøper lisenser selv. Skulle imidlertid gratisprinsippet bli gitt et annet innhold fremover i tid og forutsatt at alle eksamener blir avviklet digitalt i fremtiden, er det mulig at konklusjonen kan bli en annen.

Konklusjon: Institusjonen kan ikke kreve at studentene kjøper programvare eller lisenser selv.

4.3.4 Hvilket ansvar har institusjonen for PC og innholdet lagret på denne PCen?

1) Institusjonens eget utstyr?
Institusjonen har selv ansvar for skade som egne ansatte gjør på institusjonens utstyr. Imidlertid kan det tenkes at en student uaktsomt eller forsettlig påfører skade på universitetets utstyr. Denne situasjonen kan medføre at institusjonen får et erstatningskrav mot studenten. I så tilfelle kan de erstatningsrettslige utgangspunktene nevnt innledningsvis langt på vei brukes. Hovedregler om utmåling av det økonomiske tapet ved tingskade følger av skadeserstatningsloven § 4-1. Et annet og kanskje mer praktisk spørsmål er om institusjonen i det hele tatt ville reist et slikt krav mot en student. Sannsynligvis ikke. Institusjonens ansvar må også gjelde innholdet på PCen, og tilsvarende for innholdet som er knyttet til den digitale eksamen (studentens arbeid). Dersom PCen (institusjonens eiendom) bryter sammen grunnet tekniske årsaker under eksamen og studentens innhold forsvinner,

må nok institusjonen som ansvarlig kompensere tapet for eksamen, eksempelvis at studentens gis ytterligere tid, eventuelt ny eksamen.

Konklusjon: Hvilket erstatningsansvar institusjonen har for PC og innhold på PCen må vurderes i hvert enkelt tilfelle ut i fra faktum i saken.

2) Studentens utstyr?
Her må det gjøres en presisering hvor det skilles mellom institusjonens ansvar for utstyret og ansvar for innholdet på utstyret/PCen.

Når det gjelder institusjonens ansvar for utstyret, kan utgangspunktene som er nevnt innledningsvis legges til grunn. I slike tilfeller må det reises spørsmål om årsaken til skaden, ligger dette innenfor eller utenfor det som institusjonen er ansvarlig for, er det flere årsaker til at skaden inntraff mm.

Når det gjelder ansvaret for hva som er lagret på PCen må det gjøres en ytterligere presisering. Institusjonen har ikke noe ansvar for privat innhold som sådan. Dersom det imidlertid oppdages ulovlig innhold, må det være opp til den enkelte institusjon å ha egen policy på hvordan dette skal håndteres (anmeldelse/utestenging fra institusjonens brukerkonto ea.). Dette er policyspørsmål som hver enkelt institusjon selv må ta stilling til. Dersom skaden skyldes systemnedlastninger i forbindelse med avviklingen av eksamen, må resonnementet være som nevnt innledningsvis her. Det innebærer også at institusjonen kan komme i erstatningsansvar for studentens private innhold på PCen dersom vilkårene for erstatning er oppfylt.

Konklusjon: Institusjonen kan ha erstatningsansvar for studentens PC og innhold på denne dersom vilkårene for erstatning er oppfylt – dette må avgjøres etter en konkret vurdering.

3) På institusjonen vs. under hjemmeeksamen

Hvorvidt studenten bruker institusjonens utstyr eller eget utstyr på institusjonen eller hjemme, endrer ikke de rettslige utgangspunktetene. Spørsmålet vil derfor kunne løses slik det er beskrevet under a) og b) her.

a) Hva gjør institusjonen om de ved klargjøring av students maskin skader denne eller innholdet?

Konklusjon: Se gjennomgangen under innledningen. Oversikt over erstatnings- og forsikringsrettslige utgangspunkt.

b) Hva gjør institusjonen om de ved klargjøring av students maskin finner piratkopiert maskinvare eller annet ulovlig innhold?

Ulovligheter utover ulovlig kopiert programvare, film og musikk oppleves svært sjeldent (jf. erfaring fra både UiB og UiO). Vurderingen av om programvare, film og musikk er ulovlig og hvilken beredskap institusjonen skal ha på dette, må det være opp til den enkelte institusjon å ha planer for (den enkelte institusjons autonomi). Imidlertid skal institusjonene være oppmerksomme på handlinger her som er straffbare og som bør/skal politianmeldes.

Dette resonnementet må også gjelde for ulovlig bruk av institusjonens nettverk.

Konklusjon: Hver enkelt institusjon må ha beredskap for sånne tilfeller, og må være særskilt oppmerksomme på handlinger som bør eller skal politianmeldes.

4.3.5 Hvilket ansvar har institusjonen dersom studentens PC crasher under eksamen?

Digitale eksamener må være godt planlagt og risikovurderinger må være gjort i forkant. Risikoen for at noe kan gå galt i forkant eller underveis i eksamen er tilstede, og institusjonen må derfor ha etablert tiltak som kan begrense potensielle problem når de oppstår. Institusjonene bør tilby at:

- Institusjonens egne maskiner på datalaber blir reservert og kandidater kan flyttes dit på kort varsel for å fullføre eksamen
- IT-personell er tilgjengelig under hele eksamen
- Brukerstøtte fra leverandør er tilgjengelig under hele eksamen
- Rutiner for å gi ekstra tid ved tekniske problemer
- Kandidatene vil kunne gjennomføre/fullføre eksamen på papir etter ordinære prosedyrer samme dag, eventuelt med tillegg i tid, alternativt på en senere angitt dato (enten skriftlig på pair eller digitalt)

Digital skoleeksamen er underlagt de samme regler som en ordinær papirbasert skoleeksamen. Arbeidsgruppen har lagt til grunn at digital eksamen er en alternativ måte å avvikle eksamen på, men ikke en annen vurderingsform.

Institusjonens ansvar vil kunne være både et praktisk, men også et rettslig ansvar, alt etter hva som har skjedd. Forutsatt at studentens PC crasher under eksamen, men lar seg ordne i

ettertid, vil det i alle fall være et praktisk spørsmål hvilke tilbud studenten gis for å få avlagt eller fullført sin eksamen. Institusjonene vil nok legge dette ulikt opp, slik at noe blir avhjulpet samme dag og noe i etterkant. Dersom institusjonen ikke klarer å avhjelpe samme dag, er det viktig at nytt tilbud blir gitt raskt og dette bør det også ha vært informert om i forkant av den digitale eksamen.

Forutsatt at studentens PC ikke lar seg reparere av institusjonen, så vil dette også bli et rettslig spørsmål i form av eventuell erstatning til studenten. Det blir da et spørsmål om bl.a. årsaken til at PCen crashet, om årsaken ligger innenfor eller utenfor det som institusjonen er ansvarlig for, og/eller om det foreligger samvirkende årsaker (se nevnt under innledningen), og om de tre vilkårene for erstatning er oppfylt m.m. Vurdering av erstatningsansvaret er nevnt innledningsvis.

Dersom studenten ikke blir tilbudt ny eksamen på en tilfredsstillende måte, og følgende er at studenten ikke oppfyller krav til progresjon (kommer forsinket ut i arbeidslivet, får ikke lenger støtte fra Lånekassen ol), vil det potensielt kunne bli reist et erstatningskrav mot institusjonen. For dette se mer under pkt. 4.6 og oversikt gitt innledningsvis om vilkårene for erstatning.

Konklusjon: Institusjonen må ha gode rutiner for hva som skal tilbys dersom noe skjer med studentenes PC under eksamen, både under eksamen og i etterkant dersom det får påfølgende konsekvenser.

4.3.6 Ansvar for eksamensbesvarelsen?

For generelle vilkår se gjennomgangen under innledningen, pkt. 4.5 om «Oversikt over erstatnings- og forsikringsrettslige utgangspunkt». Studenten har ansvar for å levere besvarelsen innen angitt tidsfrist. Institusjonen er ansvarlig for å gi denne typen opplysninger til studenten når eksamen starter.

Dersom besvarelsen av tekniske årsaker ikke kan leveres eller forsvinner (før/under/etter levering), vil institusjonen kunne komme i ansvar. Det er institusjonen som er ansvarlig for programvaren, og annet teknisk utstyr, som tilbys for gjennomføringen av digital eksamen. Dersom denne svikter under eksamen slik at eksamensbesvarelsen forsvinner ea, må utgangspunktet være at institusjonen er ansvarlig (både praktisk og rettslig). Dette forutsetter imidlertid at studenten har fulgt de instrukser institusjonen har satt for klargjøring av PCen i forkant av eksamen og underveis i eksamen. Hver sak må vurderes konkret, årsaksforklares og bevises.

Konklusjon: Institusjonen har ansvaret for eksamensbesvarelsen, forutsatt at studenten har fulgt de instrukser som gjelder for den enkelte eksamen.

4.4 Hvem er økonomisk ansvarlig for hva knyttet til maskinen? Må lærestedet ha forsikringer knyttet til gjennomføring?

For spørsmålet om forsikringer, gjelder selvassuranseprinsippet. Dette innebærer i denne sammenheng at institusjonen ikke har forsikret egne PCer eller studentens. Som nevnt tidligere kan studenten ha egen forsikring, i så tilfelle kan det bli aktuelt med regress fra forsikringsselskapet (forutsatt ansvar for institusjonen).

Institusjonen kan som følge av selvassuranseprinsippet ikke inngå forsikringsordninger.

4.4.1 Bruk av eget utstyr på eget ansvar?

Konklusjon: Institusjonen kan ikke legge dette til grunn som et prinsipp her. En slik ansvarsfraskrivelse, vil nok ikke holde rettslig dersom skade inntreffer på studentens utstyr. Det må som nevnt innledningsvis vurderes konkret i hver sak hva som er årsak til skaden (innenfor eller utenfor institusjonenes ansvar), var studenten helt/delvis skyld i skaden selv osv.

4.5 Eksamen på institusjonen på institusjonens PC

4.5.1 Hvilket ansvar har institusjonen for fysiske lokaler / infrastruktur / strømtilførsel / nettkapasitet/ Ventilasjon / støy

Det legges til grunn at det er institusjonens ansvar å legge optimale forhold til rette ved gjennomføring av enhver eksamen. I motsatt tilfelle kan studenten/e klage over formelle feil, jf. uhl. § 5-2.

Manglende strøm og nettkapasitet, er feil som nok faller innenfor bestemmelsens anvendelsesområde. I denne sammenheng vil nok konsekvensen være at det holdes ny eksamen, fordi feilen ikke kan rettes opp ved ny sensur. Sensurvedtaket skal oppheves både når det holdes ny eksamen og ved ny sensur, jf. uhl. § 5-2 (2). Feilen kan ikke tolkes til ugunst for studentene, slik at det er frivillig for hver enkelt student om den velger å avlegge ny eksamen her eller beholde opprinnelig karakter (forutsetter da at eksamenen lot seg gjennomføre, men med strøm/nettkapasitetsproblemer underveis, slik at det foreligger en eksamen som kan bli gjenstand for sensur).

Forutsatt at eksamen må avbrytes som følge av nevnte årsaker (se problemformuleringen) og at institusjonen ikke klarer å gi et nytt tilbud til studentene uten at det medfører forsinkelse, kan erstatningsansvar også tenkes å bli aktuelt for institusjonen. Særlig praktisk og aktuelt er vel dette egentlig ikke, idet institusjonene har et slikt back-up system for alle eksamener (gjentak av eksamen innen rimelig tid) uavhengig av om eksamen er digital eller skrives med penn og papir.

Konklusjon: Institusjonen har ansvaret for at alt rundt fysiske lokaler /infrastruktur / strømtilførsel / nettkapasitet / ventilasjon / støy fungerer optimalt under gjennomføring av enhver eksamen.

4.5.2 Hvilket ansvar har institusjonen der eksamen blir avlyst pga. tekniske feil ved løsningen?

Relevante ansvarsgrunnlag her vil kunne være institusjonens ansvar for formelle feil etter uhl. § 5-2. Institusjonens ansvar for å kunne gi et fullgodt alternativ til studentene, eksempelvis ved å tilby ny eksamen innen kort tid. Erstatningsansvar for forsinkelse/manglende progresjon, forsinkelse ut i arbeidslivet, manglende videre støtte fra Lånekassen osv. (Jeg er usikker på hvor praktisk og aktuelt dette i realiteten er, fordi slike saker vil være unntaksvise saker som nok vil søkes løst av institusjonen før det blir et spørsmål om erstatningsansvar.)

1) Dersom eksamensbesvarelsen ikke kan gjenfinnes i den tekniske løsning som institusjonen har valgt, har da institusjonen ansvar for å holde ny eksamen for denne kandidaten?

Konklusjon: For slike saker vil det bli et spørsmål om det foreligger formelle feil etter uhl. § 5-2.

2) Dersom ja, har institusjonen erstatningsansvar for forsinket studieløp og det som følger av det?

Dette forutsetter at det er institusjonens tekniske løsninger som er brukt og institusjonens nettverk. Motsetningsvis vil institusjonen neppe bli ansvarlig dersom studenten har valgt å bruke eksternt nettverk for gjennomføring av eksamen og teknisk svikt i dette medfører at studenten ikke får levert i tide og derav manglende progresjon.

Normalt vil nok institusjonen finne løsninger for studenten/e slik at denne/disse i realiteten ikke opplever å få et forsinket studieløp.

Skulle imidlertid dette inntreffe for studenten/e, vil det måtte bero på en konkret vurdering av hver sak hvilket ansvar institusjonen har for å dekke et økonomisk tap for studenten (erstatningsansvar). Vilkårene nevnt innledningsvis i dette kapitlet vil måtte være oppfylt; Erstatningsansvar for institusjonen forutsetter at tre kumulative vilkår er oppfylt; det må foreligge et ansvarsgrunnlag, et økonomisk tap og en årsakssammenheng mellom handlingen og studentens økonomiske tap. Sentrale ansvarsgrunnlag vil her være arbeidsgiveransvar og ansvar på objektivt grunnlag. Det vil også måtte vurderes om studenten/e selv har ansvar for skaden.

Konklusjon: Krav om erstatning fra studenten/e i denne sammenheng er ikke upåregnelig, men ikke særlig praktisk idet institusjonen nok vil strekke seg langt for å avhjelpe denne typen av skade. Skulle det imidlertid bli aktuelt, må hver sak vurderes konkret i forhold til de nevnte vilkår og ansvarsgrunnlag.

4.6 Økonomisk ansvar: hva har det enkelte universitet faktisk ansvar for?

Institusjonen har ansvar for tekniske løsninger, infrastruktur, fullgode løsninger for at eksamen blir avviklet på en forsvarlig måte m.m. Premissene for institusjonens ansvar vil følge av lisensavtaler, tekniske løsninger, om hva og hvordan studentene informeres i forhold til digital eksamen, universitets- og høyskolelovens regler og egne institusjonelle regler.

Konklusjon: Det er ikke mulig å gi en uttømmende angivelse her. Veldig enkelt sagt er institusjonen ansvarlig for digital eksamen, herunder valg av tekniske løsninger osv., egne PCer og innhold samt studentens PC og innhold, men på gitte premisser.

4.7 Eksamen utenfor institusjons område på studentens eget utstyr:

Det forutsettes her at institusjonen godkjenner at det holdes eksamen utenfor institusjonens område (det kan tenkes her hjemmeeksamener, studenten befinner seg i et annet land, ved ambassade osv.).

Spørsmålet er hvilket ansvar institusjonen har i slike situasjoner?

Premiss for vurderingen her: Institusjonen gir regler om eksamen og det forutsettes også at studentene holder seg oppdatert på de til enhver tid gjeldende regler for eksamen samt hvilke premisser institusjonene eventuelt setter for å avvikle eksamen utenfor institusjonens område på egen PC.

Konklusjon: Forutsatt premissene nevnt over er det studenten som løper risikoen dersom han/hun ikke får levert eksamen elektronisk og i tide. Et annet spørsmål er jo i hvilken grad institusjonen mener seg forpliktet eller av servicehensyn ønsker å avhjelpe studentens problemer/for sen innlevering ol. Dette vil nok variere mellom institusjonene.

4.8 Kan en institusjon kreve at en student bruker eget internett ved gjennomføring av eksamen?

Dette avhenger av hvilke eksamensformer hver institusjon har. Dersom det avholdes hjemmeeksamen, vil studenten bruke eget nettverk, universitetets nettverk (forutsatt at studenten befinner seg på institusjonenes nettverksområde) eller tredjemanns nettverk.

Det ligger således i dette at institusjonene ikke kan kreve at studenten bruker eget nettverk. Jeg tror svaret må snus rundt; Velger studenten å bruke et nettverk utenfor institusjonens nettverk løper studenten selv risikoen for tekniske problemer som kan oppstå underveis i eksamen og i innleveringsfasen. Dette ligger utenfor institusjonens ansvar, men som nevnt kan det bli et spørsmål om i hvilken grad institusjonen mener seg forpliktet eller av servicehensyn ønsker å avhjelpe studentens problemer. Mister studenten innholdet på PCen ved bruk av nettverk utenfor institusjonene eller ikke får levert i tide, er dette nok studentens eget ansvar. Denne typen risiko for studenten fremstår også som nærliggende og påregnelig og studenten må selv ta ansvar for å minimere risikoen.

Ved teknisk svikt på institusjonens nettverk ved gjennomføringen av eksamen, må institusjonen selv ta ansvar overfor studenten/e.

Konklusjon: Institusjonen kan ikke kreve at en student bruker eget internett ved gjennomføring av eksamen, men dersom studenten selv velger å bruke eget internett har studenten selv ansvaret for å gjennomføre og levere eksamen.

4.9 Kan en institusjon godta at en student sitter på nettverk de ikke selv har ansvar for, f.eks. offentlig bibliotek?

Dette avhenger av hvilke eksamensformer hver institusjon har og hvilket handlingsrom dette gir for institusjonen og ikke minst studenten i valg av sted for gjennomføring av eksamen (på institusjonens område og utenfor).

Konklusjon: Forutsatt at det ligger innenfor institusjonens regler at eksamen kan avvikles utenfor institusjonens område, så kan institusjonen godta at en student avvikler eksamen på et nettverk utenfor institusjonens. Som nevnt tidligere løper studenten en viss risiko selv for

teknisk svikt på slike eksterne nettverk, som studenten som utgangspunkt må bære risikoen for selv.

5 Krav til autentisering

Kapittelet er skrevet av May Liz Bjørnevik Tho, NTNU.

5.1 Problemstillinger

Hvordan kan undervisningsinstitusjoner sjekke at det er rette vedkommende som leverer eksamen når innlevering skjer elektronisk?

Hvordan kan undervisningsinstitusjoner sjekke at det er rette sensor som gir karakter til rett kandidat?

5.2 Innledning

For at en student skal kunne gå opp til eksamen må studenten være registrert som student ved undervisningsinstitusjonen, og ha betalt semesteravgift, jf. Lov om studentsamskipnader[30]§ 10 og oppfylle kravene etter § 3-10 i uhl. I enkelte emner kan det også være andre tilleggskrav for å kunne avlegge eksamen. Ved avlegging av eksamen vil undervisningsinstitusjonen ha behov for å sjekke om studenten har rett til å gå opp til eksamen, og om det er rette vedkommende som avlegger eksamen. Ved avleggelse av eksamen på tradisjonell måte der studenten møter i eksamenslokale skjer en slik sjekk ved at studenten identifiserer seg ved å vise legitimasjon

Avleggelse av eksamen digitalt vil by på nye utfordringer i forhold til autentisering av eksamenskandidaten.

Sensurprotokoller oversendes vanligvis undervisningsinstitusjonen fra sensor(ene) når endelig karakter er satt. Denne er da signert av sensor(ene) som bekreftelse på gjennomført sensur. Dersom karakter kun skal dokumenteres i et digitalt system byr det på utfordringer knyttet til autentisering av sensoren. Undervisningssituasjonen vil ha et klart behov for å kvalitetssikre en sensur ved bruk av digitale systemer.

5.3 Begrepsforklaring

Nedenfor gis noen begrepsforklaringer som er relevant i forbindelse med krav til autentisering av eksamenskandidat og sensor ved avleggelse og sensur ved digital eksamen.

[30] LOV-2007-12-14-116

- *Oppmøteprotokoll*
  En oppmøteprotokoll er betegnelsen for oversikten over de eksamenskandidatene (kandidaten) som er meldt opp og kvalifisert til den konkrete eksamen. Etter endt eksamen blir informasjon fra oppmøteprotokollen vanligvis registrerer i FS.

- *Sensurprotokoll*
  Utarbeides på bakgrunn av oppmøteprotokollen. Den sendes til sensor, og returneres signert og påført kandidatens karakter. Karakter blir ført inn i den enkelte kandidats eksamensprotokoll/vurderingsprotokoll i FS.
  Eksamensprotokollen/vurderingsprotokollen i FS bevares for evig tid.

- *Autentisering*
  Autentisering er å verifisere en påstått identitet.[31]
  De som skal autentisere seg må inneha noe som kan bekrefte deres identitet. Dette kalles autentiseringsfaktorer. En bruker kan ha en eller flere av disse avhengig av sikkerheten i den valgte løsningen. Det finnes tre forskjellige typer autentiseringsfaktorer:

  - Noe personen vet - for eksempel et passord
  - Noe personen har - for eksempel en passordkalkulator
  - Noe personen er - for eksempel et fingeravtrykk

  Autentiseringsfaktoren(e) må knyttes til studenten eller sensorens identitet. Denne administrasjonen av brukere kan gjøres av en tredjepart eller av undervisningsinstitusjonen selv.

  FEIDE står for Felles Elektronisk IDEntitet. FEIDE skal sørge for autentisering, autorisasjon og forvaltning av brukernes identitet i universitets- og høyskolesektoren skjer uavhengig av de datasystemer som studentene benytter.[32]

- *Elektronisk signatur*
  Data i elektronisk form som brukes som autentiseringsmetode, jf esignaturloven § 3[33].

[31] http://www.regjeringen.no/nb/dep/kmd/dok/lover_regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/4.html?id=505929
[32] http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Utkast_eIDstrategi_13.03.07.pdf#search=esignatur&regj_oss=1
[33] LOV-2001-06-15-81, Lov om elektronisk signatur

5.4 Hvilke krav stilles til autentisering av eksamenskandidaten ved avleggelse av digital eksamen?

Ved avvikling av digital eksamen er det behov for løsninger der innlevering av eksamen sikrer autentisering av eksamenskandidaten.

Det er ingen entydig regulering i lov eller annet regelverk som presiserer krav til autentisering av en eksamenskandidat. Imidlertid har undervisningsinstitusjonene lokale regler for hvordan de sikrer at det er rette vedkommende som har avlagt eksamen. Fremleggelse av legitimasjon og signering av oppmøteprotokoll er vanlige måter å bekrefte ens identitet på.

Ved digital eksamen kan autentisering skje ved FEIDE-pålogging og ved elektronisk signatur. Dog vil en slik løsning kunne åpne for at studenten fusker ved å sende en annen til å avlegge eksamen utstyrt med studentens brukernavn og passord, eventuelt passordkalkulator e.l. En løsning med kun FEIDE-pålogging eller lignende vil altså neppe sikre tilstrekkelig autentisering av eksamenskandidaten.

Ved innlogging i nettbank har man vanligvis en løsning med både brukernavn og passord samt kodebrikke e.I. Altså stilles det strenge krav i forhold til autentisering. Dette er for å sikre at uvedkommende ikke skal få tilgang til ens bankkonto. Ved avleggelse av eksamen må undervisningsinstitusjonen i sin risikovurdering ta høyde for at eksamenskandidaten selv gir fra seg sine autentiseringsfaktorer for å la en annen møte opp og avlegge eksamen på ens vegne - altså fuske. Dersom kandidaten ønsker å fuske, vil kandidaten, her som eier av identiteten, ikke ha det samme ønsket om å sikre identiteten som ved for eksempel tilgang til nettbank. Behov for autentisering vil for innlevering av eksamen være for å kvalitetssikre at det er rette vedkommende som leverer eksamen, herunder å avdekke fusk.

Det vil være mulig å sikre seg mot slik fusk ved å avkreve legitimasjon ved utlevering av for eksempel unikt og ukjent kandidatnummer, slik det også noen steder gjøres ved avleggelse av tradisjonell skoleeksamen. Sammen med en digital løsning der innlevering av eksamen digitalt krever brukernavn, passord for f.eks. FEIDE-pålogging samt det unike kandidatnummeret. En annen løsning som kanskje ligger noe lenger frem i tid, er fingeravtrykkscanning eller annen autentiseringsløsning som er knyttet til hvem personen er.

Konklusjon

Ved digital eksamen som skal skje som en erstatning for tradisjonelle skoleeksamen, vil det være behov for legitimering eller annen autentiseringsfaktor knyttet til noe personen “er” i tillegg til de autentiseringsmetoder som kan benyttes via FEIDE eller eSignatur dersom

undervisningsinstitusjonen mener det er behov for å stille tilsvarende krav til autentisering som ved dagens system. Bakgrunnen for dette er at en ren digital løsning ikke vil være tilstrekkelig i forhold til å sikre at det er eksamenskandidaten som avlegger eksamen.

Ved hjemmeeksamen der undervisningsinstitusjonen krever identifisering som ved skoleeksamen er det behov for en løsning som sikrer autentisering ut over brukernavn og passord på tilsvarende måte. En løsning da vil også være å bruke identifisering med kandidatnummer.

5.5 Hvilke krav stilles til autentisering av sensor ved sensur av eksamen?

Ved avvikling av digital eksamen er det behov for løsninger som sikrer autentisering av sensor.

Det er som for autentisering av eksamenskandidater heller ingen entydig regulering i lov eller annet regelverk som presiserer krav til autentisering av sensor. Imidlertid har undervisningsinstitusjonene også for disse lokale regler for hvordan de sikrer at det er rette vedkommende som sensurerer. Dette skjer vanligvis ved signering av sensurprotokoll.

Risiko for at sensor gir fra seg brukernavn og passord for å la andre gjøre oppgavene for seg er klart tilstede. Det er en kjensgjerning også etter dagens system at sensorer lar andre (konsulenter ved ens enhet evt. andre ansatte) gjøre skrivearbeidet for seg. Imidlertid er ikke motivasjonen for å gi fra seg arbeidet her fusk, slik det vil kunne være for eksamenskandidatene. Dog har undervisningsinstitusjonen behov for å sikre at det er rette vedkommende som avleverer sensur. Under henvisning til at motivasjonen for eventuelt "lekking" av autentiseringsfaktorer til andre vil være å søke hjelp til praktisk avlastning og ikke fusk, må det antas at det vil være tilstrekkelig med brukernavn og passord for innlogging for oversendelse av sensur, sammen med en eventuell kode for den aktuelle eksamen. I tillegg kan det i avtale med sensor presiseres at brukernavn og passord er personlig og skal ikke overleveres andre.

Konklusjon
Ved avleggelse av sensur ved bruk av digitale hjelpemidler vil det være tilstrekkelig med autentisering med brukernavn og passord.

5.6 Signeringskravet på klager

En eksamenskarakter er et enkeltvedtak som kan påklages av studenten jf. forvaltningsloven § 2b, samt § 28.

§ 11 i eForvaltningsforskriften omhandler klage. Paragrafen lyder:

§ 11. Klage

I forbindelse med underretning om enkeltvedtak skal forvaltningsorganet informere om hvorvidt det har lagt til rette for mottak av klage i elektronisk form, og hva som er rette elektroniske adresse. Det skal også informeres om at parten bør kontrollere at han mottar bekreftelse når klage leveres i elektronisk form.

Klagefristen etter forvaltningsloven § 29 begynner å løpe fra det tidspunktet enkeltvedtaket er gjort tilgjengelig for parten, og varsel om dette er sendt, jf. § 8 tredje ledd.

Klage over enkeltvedtak kan fremsettes ved bruk av elektronisk kommunikasjon dersom det forvaltningsorganet som skal motta klagen har lagt til rette for det, jf. § 3 og § 4.

Hvis klager ikke mottar bekreftelse etter § 6, skal klagen sendes på nytt.

Klage er rettidig framsatt dersom den er kommet fram til den elektroniske adressen som forvaltningsorganet har oppgitt for mottak av elektroniske klager innen klagefristens utløp.

Utdrag fra veileder til eForvaltningsforskriften[34] (Kommunal- og moderniseringsdepartementet), kap. 3.8 Klage over enkeltvedtak:

Klage over enkeltvedtak kan fremsettes ved bruk av elektronisk kommunikasjon dersom det forvaltningsorganet som skal motta klagen har lagt til rette for det, se fvl § 32 siste ledd og efvf. § 9. Etter forvaltningsloven skal en klage være undertegnet eller "autentisert som fastsatt i forskrift, eller i medhold av forskrift". Formuleringen trekket i retning av at det først og fremst er bekreftelse på klagerens identitet eller fullmakter man er ute etter. Hvordan klagen skal fremsettes og hvilke sikkerhetskrav som stilles, bestemmer forvaltningsorganet i henhold til efvf. §§ 3 og 4. Det kan for eksempel dreie seg om å bruke et spesielt klageskjema og autentisering ved hjelp av elektronisk signatur.

Det er etter forvaltningsloven ingen klare krav til autentisering ved klage på enkeltvedtak. Undervisningsinstitusjonen vil imidlertid ha behov for å sikre at det er rette vedkommende som klager på sin egen karakter. Det er dog sannsynligvis ikke det samme behovet for å sikre autentisering som ved avleggelse av eksamen all den tid risiko for fusk ikke er tilstede.

[34] http://www.regjeringen.no/nb/dep/kmd/dok/veiledninger_brosjyrer/2007/veileder-til-eforvaltningsforskriften.html?id=476581

En løsning for klage der studenten oppgir brukernavn, passord og kandidatnummer for registrering av klagen vil kunne være en sikker autentisering av studenten.

Konklusjon

Ved en digital klage vil en løsning med brukernavn og passord være tilstrekkelig for autentisering av klager.

5.7 Hvilke krav stilles det til autentisering av studenten ved gjennomføring av hjemmeeksamen?

Autentisering ved hjemmeeksamen vil kunne skje ved FEIDE-pålogging eller ved esignatur på tilsvarende måte som ved digital eksamen i felles eksamenslokale. Dette er som nevnt over ikke en tilstrekkelig autentisering i forhold til å sikre at det er rette vedkommende som har skrevet teksten. Imidlertid har institusjonene ved avleggelse av hjemmeeksamen på tradisjonell måte tatt høyde for at alle hjelpemidler er tillatt, slik at bekymring i forhold til fusk ikke er tilstede på samme måte som for tradisjonelle skoleeksamener. Da vil en sikring i forhold til autentisering være mer av hensyn til at andre ikke har tilgang til brukernavn og passord til studenten. Dersom det også for skoleeksamen legges opp til en løsning for å gi ut kandidatnummer som en tredje autentiseringskomponent vil dette kunne være en tilstrekkelig løsning for autentisering ved digital hjemmeeksamen.

Konklusjon

Ved digital hjemmeeksamen bør autentisering skje ved brukernavn, passord og utdelt kandidatnummer på samme måte som nevnt i pkt. 5.4.

6 Behandlinger av personopplysninger relatert til gjennomføring av digital eksamen

Kapittelet er skrevet av Märtha Felton og Maren Magnus Jegersberg.

Punkt 6.6 om skytjenester er skrevet av May Liz Bjørnevik Tho, Märtha Felton og Maren Magnus Jegersberg.

6.1 Innledning

Personopplysninger som behandles i en eksamenssituasjon er opplysninger som er knyttet til de studentene som gjennomfører eksamen, og vil for eksempel være studentens navn og øvrige personalia, eventuelt vedtak om tilrettelegging ved eksamen eller andre særlige forhold. Når en eksamen gjennomføres vil studentenes personopplysninger behandles på forskjellig måte ut i fra de ulike systemer som brukes og eksamensformen.

Behandlinger av personopplysninger reguleres av Lov om behandling av personopplysninger[35] (pol.) og forskrift om behandling av personopplysninger (pof). Regelverket definerer hvilke roller det knyttes rettigheter og plikter til.

Personopplysningslovens formål er å beskytte den enkelte mot at *personvernet blir krenket* ved behandling av deres personopplysninger, jf. § 1,1.ledd. For å oppnå dette formålet skal loven bidra til at behandlinger av personopplysninger skjer i samsvar med grunnleggende personvernhensyn, som behovet for nødvendig kvalitet på opplysningene, privatlivets fred og personlig integritet. Disse hensynene materialiseres gjennom de oppsatte kravene ved at de som skal bruke opplysningene aller først må ha en rett, hjemmel eller annet rettsgrunnlag, for å behandle personopplysningene. Det er viktig at alle som har en rolle hvor de bruker andre personers personopplysninger har i bakhodet at det er studenten selv som eier sine egne opplysninger. Vi, som en utdanningsinstitusjon, har bare en tillatelse ved at personen er student hos oss til å forvalte disse opplysningene, og med denne tillatelsen ligger det et stort og viktig ansvar for å behandle personopplysningene til hvert enkelt individ med forsiktighet.

6.2 Definisjoner knyttet til behandling av personopplysninger

- *Personopplysninger* er alle opplysninger og vurderinger som kan knyttes til en enkeltperson, for eksempel navn, adresse, lønn, studenters besvarelser, kandidatnummer, jf. pol. § 2, nr.1. Definisjonen tolkes vidt, og både direkte og

[35] LOV-2000-04-14-31

indirekte tilknytning omfattes. Det er kun opplysninger som kan knyttes til fysiske personer som omfattes.

- *Sensitive personopplysninger* er opplysninger som krever ekstra beskyttelse, som rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger, jf. § 2, 8 a-e. Legg også merke til at man kan komme til å behandle personopplysninger som på grunn av sin natur, sitt innhold eller sammenhengen de står i kan ha behov for samme beskyttelse som sensitive personopplysninger til tross for at de ikke faller inn under lovens definisjon. Det er institusjonens ansvar å fange dette opp.

  Personopplysningsloven krav til behandlingen av sensitive personopplysninger er når det gjelder sikkerhet og kontroll strengere enn de krav som stilles til behandling av «alminnelige» personopplysninger. En direkte konsekvens av dette, som er relevant for vurderinger i dette kapittel, er at sensitive personopplysninger iht. EU's artikkel-29 arbeidsgruppe eller Datatilsynet, ***ikke*** kan behandles i skytjenester. Det er fordi de aller fleste leverandører av skytjenester ikke kan (eller vil) bistå behandlingsansvarlige med å sikre at kravene i personopplysningsloven er overhold når det gjelder behandlinger av sensitive personopplysninger. Det kan for eksempel bety at de ikke har full kontroll over hvor data lagres, data kan være lagret i et land som ikke har tilstrekkelig beskyttelse i nasjonal lovgivning eller de kan bruke underleverandører som i sin behandling ikke kan oppfylle loven. Se mer under punkt 6.6.3.

- *Anonymiserte personopplysninger* er personopplysninger der navn, personnummer og andre direkte personidentifiserbare kjennetegn er fjernet. Når personidentifikasjon er fjernet kan opplysningene i prinsipp ikke knyttes til en bestemt person og da er dataene heller ikke definert som personopplysninger. Det betyr også at bestemmelsene i personopplysningsloven ikke kommer til anvendelse på opplysningene. Merk her at personopplysninger bare er anonyme der det ikke foreligger mulighet til å re-identifisere en bestemt person eller personer.

- *Avidentifiserte personopplysninger* ligner noe på anonyme opplysninger fordi direkte personidentifiserbare kjennetegn tilsynelatende er fjernet. Det finnes imidlertid en «nøkkel» som gjør det mulig å finne ut hvem opplysningene peker tilbake til. For den

som ikke har tilgang til nøkkelregisteret, er opplysningene anonyme. Fordi de teknisk sett kan re-identifiseres, regnes de som avidentifiserte. Avidentifiserte personopplysninger skal behandles som personopplysninger iht. bestemmelsene i personopplysningsloven.

- *Den registrerte* er den personen som opplysningene kan knyttes til, og er den som eier opplysningene, jf. § 2, nr. 6. Reglene i personopplysningloven med forskrift er gitt for å sikre at opplysninger om den registrerte ikke behandles unødig, at den som eier opplysningene i størst grad skal ha kontroll over egne opplysninger og hindre misbruk. Studentene på våre institusjoner, som i denne sammenhengen er de registrerte, kan vi til en viss grad si er tvunget til å gi oss deres personopplysninger for å kunne studere.

- *Behandling av personopplysninger* – er enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf.§ 2, nr. 2. Ved gjennomføring av eksamen vil for eksempel behandling av personopplysninger være lagring, overføring eller utlevering til en ekstern leverandør av eksamensløsning (som kan være en skytjeneste) eller sensor.

- *Behandlingsansvarlig* er den som er ansvarlig for behandling av opplysningene, og den som bestemmer formålet med behandlingen av personopplysninger og *hvilke hjelpemidler som skal brukes under behandlingen*, jf. § 2, nr. 4. For institusjoner i UH-sektoren er dette enten universitets- eller høyskoledirektør, eller rektor. Dette ansvaret er knyttet til stillingen og er derfor personlig, noe som betyr at den som sitter i stillingen er juridisk ansvarlig. Videre i dette kapittelet vil vi omtale hele institusjonen som behandlingsansvarlig.

- *Databehandler* er den som etter avtale behandler personopplysninger på vegne av den behandlingsansvarlige, jf. § 2, nr. 5. Databehandler kan ikke behandle personopplysningene på annen måte enn det som er avtalt. En databehandler i vår sektor kan f.eks. være FS eller Ephorus. Ofte vil databehandler være en *leverandør* av en tjeneste som institusjonen kjøper.

- *Databehandleravtale* er en avtale som regulerer rammene for hvordan en databehandler kan behandle personopplysninger på vegne av den behandlingsansvarlige, jf. § 13, jf. § 15. Når behandlingsansvarlig velger å sette bort hele eller deler av databehandlingen av personopplysninger, skal forholdet reguleres

av en databehandleravtale. Databehandleravtalen skal til enhver tid angi hvor og hvordan personopplysningene blir behandlet. I praksis innebærer dette informasjon om hvilken leverandør som fysisk besitter de aktuelle opplysningene i det aktuelle landet. Dette kan også omfatte underleverandør til den som selve tjenesten er levert av.

Vi legger til grunn Datatilsynets oppfatning[36] som innebærer at leverandør av skytjenester behandler personopplysninger på vegne av behandlingsansvarlig (som her er den aktuelle institusjon), og *leverandøren derfor er databehandler*.

Noen tjenester som tilbyr eksamensløsninger trenger kun kandidatnummer og emnekode. Disse opplysningene er koblet mot personen gjennom FS og andre lister med oversikt over hvem som tilhører hvilket kandidatnummer. Denne informasjonen er tilgjengelig for blant annet eksamensadministrasjonen. Eksamensbesvarelsene inneholder derfor personopplysninger fordi opplysningene kan knyttes til den enkelte personen. Opplysningene er fjernet og erstattet med en koblingsnøkkel, her kandidatnummeret, som er kandidatens identitet under eksamen og ved sensuren. Personopplysningene er det som kalles *avidentifiserte*. Det skiller seg fra opplysninger som er *anonymiserte* ved at koblingsnøkkelen finnes, noe den ikke gjør for anonymiserte data og som derfor ikke karakteriseres som personopplysninger.

6.3 Kan institusjonene monitorere[37] studentens aktivitet på PC under eksamen

6.3.1 Monitorering av tekniske hensyn

Loggføring av datasystem (EDB-system, inkludert maskiner) av tekniske hensyn har hjemmel i bl.a. pol. § 13, og pof. kapittel 2 og § 7-11.

Behandling av personopplysninger som ikke er sensitive er ikke konsesjonspliktige, jf. bestemmelsen i pol. § 33. Denne type behandling er heller ikke meldepliktig jf. bestemmelsen i pof. § 7-11.

Institusjonen har alltid lov til å loggføre aktivitet i sine IT-ressurser av rent tekniske hensyn. Dette betyr også at det er tillatt å loggføre for å kunne undersøke og dokumentere hva som

[36] Artikkel på Datatilsynet sine nettsider: http://www.datatilsynet.no/Teknologi/Nettsky---Cloud-Computing/Cloud-Computing/

[37] Med monotorering menes her en mer passiv form for overvåkning. Institusjonen holder ikke øye med en bestemt student, men detekterer all aktivitet. Dersom pre-definert adferd oppdages vil den bli undersøkt, slik som surfing på internett under gjennomføring av eksamen der det ikke er tillatt med hjelpemidler.

har skjedd dersom for eksempel en besvarelse «forsvinner i systemet»[38] nettopp fordi en slik «forsvinning» skyldes en feil i det tekniske. Denne dokumentasjonen vil så institusjonen kunne anvende dersom det oppstår en sak om den «forvunnede besvarelsen».

Konklusjon: En institusjon har alltid lov til å logge aktivitet i sine IT-ressurser av tekniske hensyn, og så lenge disse loggene brukes til å avdekke tekniske feil og mangler oppstått under eksamen vil det helt klart falle under bestemmelsen i pol. § 13 og pof. Kapittel 2 og § 7-11.

Merk! Logger innhentet til dette formål kan ikke brukes til å avdekke f.eks. fusk fordi formålet med monitoreringen med påfølgende logger er en annen enn å fange fusk.

6.3.2 Monitorering av studentenes aktivitet på PC for å fange fusk

Hva er fusk?

Hvis man finner det bevist at en student har «forsøkt å fuske eller forsettlig eller grovt uaktsomt har fusket ved avleggelsen av, eller forut for endelig sensur av, vedkommende eksamen eller prøve, eller under gjennomføringen av vedkommende kurs», kan klagenemnden annullere eksamen eller godkjenning av kurs, og studenten kan utestenges, jf. universitets- og høyskoleloven(uhl.)[39] § 4-7, 1 b og § 4-8, 2.[40]

Den alminnelige definisjonen av fusk i utdanningsøyemed er «*når en student har ulovlige hjelpemidler tilgjengelige under en eksamen eller på andre måter handler i strid med eksamensreglementet eller regler om kildebruk*».[41] Fusk kan karakteriseres som et brudd på akademisk troverdighet ved at man blant annet ikke oppgir kilder man har anvendt, gir inntrykk av at et svar er mer selvstendig enn det faktisk er og at man bruker hjelpemidler som ikke er tillatt.[42] I tillegg vil det innen enkelte fagområder være så alvorlig at studenten påberoper seg kunnskap han eller hun ikke har, at liv og helse blir satt i fare. Dette gjelder fag som for eksempel medisin og farmasi.

---

[38] Dette har vært tilfelle ved UiO, og vi har ved hjelp av logger kunnet finne ut hvor besvarelsen var blitt lagt.
[39] Lov om universiteter og høyskoler, LOV-2005-04-01-15.
[40] Det bemerkes at forslag til endringer i universitets- og høyskoleloven har vært på høring og at saken er under behandling. Kunnskapsdepartementet har blant annet foreslått endring i § 4-7, første ledd, bokstav b som medfører en presisering av at også tilfeller *før* eksamensoppgaven omfattes av hjemmelen. Videre er det foreslått en utvidelse av § 4-8, tredje ledd til også å omfatte studenter som har medvirket til fusk. Se høringsnotat: http://www.regjeringen.no/pages/38394044/Hoeringsnotat.pdf.
[41] Ot.prp.nr.40 (2001-2002) s. 55.
[42] Den 15. februar 2008, sist endret 10. juni 2008, fastsatte Universitetsdirektøren "Rutiner for behandling av mistanke om fusk/forsøk på fusk ved Universitetet i Oslo". I rutinens pkt. 3 angis det nærmere hva fusk er og når man anser at fusk forekommer ved UiO. http://www.uio.no/studier/admin/eksamen/fusk/

1) Kan institusjonen monitorere studentenes PC under eksamen for å fange fusk?

Personopplysninger er i henhold til personopplysningsloven § 2 nr. 1, opplysninger og vurderinger som kan knyttes til en enkeltperson. ”Behandling av personopplysninger omfatter enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter”, se pol § 2 nr. 2.

Ved monitorering av aktivitet på en students PC under digital eksamen vil systemet blant annet lagre studentens brukernavn og aktivitet under eksamen. Hva systemet lagrer vil variere fra system til system, men det må uansett anses som behandling av den enkelte students personopplysninger.

(i) Samtykke som behandlingsgrunnlag

Utgangspunktet er at det må foreligge et behandlingsgrunnlag i henhold til pol. § 8. Dersom det foreligger samtykke fra den registrerte, her studentene, vil institusjonene ha tilstrekkelig behandlingsgrunnlag, jf. § 8, første ledd.

Utdanningsinstitusjonene i Norge varierer mye i størrelse og antall studenter. For de som er mindre institusjoner, kan det være aktuelt å innhente samtykke fra hver enkelt student. For institusjoner som for eksempel UiO, vil det være uaktuelt å innhente samtykke fra hver enkelt student som skal gjennomføre digital eksamen på grunn av volumet av studenter som hvert semester tar eksamen og fordi studentmassen er så sammensatt. For en mindre institusjon kan samtykke som behandlingsgrunnlag med fordel vurderes.

Når en slik vurdering skal foretas er det viktig å inkludere tanken om et eventuelt samtykke ville vært reelt. Det er fordi det ligger et snev av tvang i innhentingen av det: «dersom du ikke samtykker så får du ikke avlegge eksamen». Når det er sagt så har studentene allerede måtte akseptere monitorering under eksamen ved at det brukes eksamensvakter under eksamen. Monitorering av PC under eksamen kan sees på som en naturlig konsekvens av den teknologiske utvikling.

Det er vanskelig å gi en generell konklusjon på hvorvidt samtykke er et gyldig behandlingsgrunnlag for å monitorere studentenes aktivitet under digital eksamen. Dette må avklares av den enkelte institusjon.

Det er vår oppfatning at samtykke nok i de fleste tilfeller ikke er tilstrekkelig som behandlingsgrunnlag. Det betyr at man må ha hjemmel i lov for å kunne monitorere aktivitet på students PC under eksamen.

(ii) Hjemmel fastsatt i lov som behandlingsgrunnlag

Det foreligger så langt vi har sett ingen klare hjemler i norsk lov som sier at behandling av personopplysninger, der formålet er å fange opp fusk, kan finne sted. Det betyr at klar lovhjemmel ikke er et alternativ som behandlingsgrunnlag.

Merk! Bestemmelsen i uhl. § 4-7, 1 b og § 4-8, 2 sier kun at fusk ikke er lov. Bestemmelsene kan ikke, så langt vi kan forstå, benyttes som hjemmel for måter å fange fusk på.

(iil) Hjemmel i en av unntaksbestemmelsene i pol. § 8 a) – f)

Dersom en ønsket behandling verken kan baseres på de registrertes samtykke eller på hjemmel i lov, må minst ett av vilkårene i pol. § 8 a) – f) oppfylles for at de skal foreligge grunnlag for å kunne sette i gang med behandlingen, her monitorere for å fange evt. fusk.

Her anser vi unntaksbestemmelsen i § 8, bokstav f som den mest relevante hjemmel. Denne bestemmelsen er en snever unntaksbestemmelse noe som betyr at den skal anvendes restriktivt og at den ikke kan tolkes utvidende. Det betyr også at hensynet til den registrerte, her studenten, vil veie tungt. Etter denne bestemmelsen kan en behandling av personopplysninger skje dersom behandlingen er nødvendig for at den behandlingsansvarlige kan ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Hver enkelt institusjon må foreta en selvstendig vurdering av hvorvidt denne unntaksbestemmelsen vil kunne gjøre seg gjeldende for deres digitale eksamen og det systemet de velger å bruke.

Vi vil her skissere opp vurderingsmomenter som det er viktig å ha med i en vurdering av om den aktuelle monitoreringen kan skje med hjemmel i § 8, bokstav f.

Foreligger det en berettiget interesse?
Vurderingsmomenter i en slik vurdering:

- Foreligger det en berettiget interesse? Dette kan for eksempel knyttes opp mot samfunnets og institusjonens interesse i å ha tiltak som har som formål å hindre og oppdage fusk under eksamen.

- Er monitoreringen nødvendig for at institusjonen kan ivareta den berettigede interessen? Momenter i denne vurderingen kan være at skoleeksamen allerede i dag gjennomføres med tilsyn av eksamensvakter. Eksamensvaktene har oversikt over lokalet til enhver tid, følger kandidatene til pause og på toalettet, mobiltelefoner er ikke tillatt og eventuelle tillatte hjelpemidler blir kontrollert. Disse tiltakene er innført for én grunn, for å hindre og oppdage forsøk på fusk /fullbyrdet fusk. Disse tiltakene vil også være nødvendige ved digital skoleeksamen, men på grunn av innføring av PC fremfor bruk av penn og papir, oppstår det et behov for å iverksette ytterligere tiltak for å sikre at kandidaten ikke urettmessig får tilgang til ikke godkjente hjelpemidler. Spørsmålet institusjonen må stille seg er derfor om det finnes andre måter å ha tilsyn med aktiviteten til studentene på PC under eksamen enn monitorering av aktiviteten på PC.

Overstiger denne interessen (institusjonens og samfunnets interesse i å oppdage fusk) den enkelte kandidats personverninteresser?
Vurderingsmomenter i en slik vurdering:

- Overstiger hensynet til den enkelte students personvern hensynet til den berettigede interessen? Her vil momenter være om samfunnets og institusjonens interesse i å hindre, samt å oppdage fusk overstiger den integritetskrenkelsen en monitorering av en PC innebærer for den enkelte student. I denne vurderingen må det legges særlig vekt på hensynet til å ivareta en berettiget interesse og at overvåkningssystemet anvendes på en slik måte at det i minst mulig grad krenker den enkelte students integritet ut over de tilsynsordninger som allerede eksisterer.

Disse vurderingspunktene er kun en anbefaling for hvordan man kan gripe an problemstillingen og hvilke vurderingsmomenter som er viktige.

Konklusjon: Kun der man kommer til at 1) det foreligger en berettiget interesse for å overvåke studentens aktivitet på PC under eksamen og 2) denne interessen overstiger

kandidatens/den registrertes personverninteresser så kan man igangsette monotirering av studentens aktivitet på PC under eksamen med hjemmel i pol. § 8 f).

6.3.3 Bruk av kamera i eksamenslokalet

Har institusjonen rett til å monitorere eksamenslokalet med video under gjennomføring av digital eksamen?

Personopplysningsloven med forskrift regulerer hvordan personopplysninger skal samles inn og hvordan de skal behandles. Utgangspunktet for en vurdering av hvorvidt institusjonen kan bruke kamera i et eksamenslokale fremkommer av lovens kapittel 7 og forskriftens kapittel 8.

Definisjonen av kameraovervåkning etter personopplysningsloven er "vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert. Som kameraovervåking anses både overvåking med og uten mulighet for opptak av lyd- og bildemateriale. Det samme gjelder utstyr som lett kan forveksles med en ekte kameraløsning.", jf. § 36.

Kameraovervåkning av personer vil kunne være et inngrep i personvernet til den enkelte og derfor strengt lovregulert. Datatilsynet har laget en veiledning om regelverket [43], og følgende er det som må vurderes og følges før en eventuell kameraovervåkning kan tas i bruk:

- Det må defineres hvorvidt det er kameraovervåkning i lovens forstand, jf. pol. § 36.
- Institusjonen må stille seg spørsmålet om hvorvidt kameraovervåkningen er nødvendig. Foreligger det et saklig behov for å bruke denne typen overvåkning, herunder hva ønsker man å oppnå og vil kameraovervåkningen hjelpe? Er det andre alternativer som eventuelt kan vurderes? Vil det for eksempel være tilstrekkelig å bruke personer som eksamensvakter i lokalet?
- Hvilke områder kan overvåkes? Selv om institusjonen konkluderer med at overvåkningen er nødvendig medfører ikke det naturlig at det aktuelle området kan overvåkes. Grensene for hvilke områder som kan tillates å overvåke er uklare, men det skal i utgangspunktet mye til. Institusjonen må selv vurdere om områdene vil være lovlige å overvåke.
- Institusjonen er selv ansvarlig for å sette seg inn i pliktene som medfører kameraovervåkningen. Dersom man ikke kjenner til og / eller følger pliktene i

[43] http://www.datatilsynet.no/Teknologi/Kameraovervaking/

tilstrekkelig grad, kan det medføre både straffe- og erstatningsansvar. Pliktene som medfører i et slikt ansvar er blant annet:

- Varsling og informasjon. All videoovervåkning skal varsles tydelig gjerne i form av varslings- og informasjonsskilt, samt for eksempel informasjon utdelt ved oppmelding til eksamen.
- Melding til Datatilsynet *eller* konsesjonsplikt.
- Informasjonssikkerhet, herunder sikring av opptakene
- Sletting av opptakene når det ikke lenger foreligger saklig grunn for oppbevaring.
- Utlevering til politi- og påtalemyndighet.
- Innsyn må gis til de personer som er avbildet i opptaket, men innsyn kan kun gis i de delene hvor den aktuelle personen faktisk er med.
- Internkontroll
- Evaluering og revisjon. Kameraovervåkning av lokalet må vurderes jevnlig. Er fortsatt de forutsetningene som gjorde at man satte i gang kameraovervåkning til stede? Institusjonen må foreta kontroll av utstyret de bruker til kameraovervåkningen og rutinene rundt ofte.

Datatilsynet har utarbeidet en veileder for hva som er lov når det kommer til kameraovervåkning.[44] For de institusjonene spørsmålet om overvåkning er aktuelt, anbefales det å sette seg grundig inn i denne veiledningen før man foretar vurderingen.

Konklusjon: Det kan ikke konkluderes på spørsmålet om institusjonene har hjemmel til å overvåke eksamenslokalet. Dette må hver institusjon selv vurdere, og dokumentere, for hvert enkelt lokale og eksamen de ønsker å overvåke. Det stilles svært strenge krav som må vurderes i hvert enkelt tilfelle på hver enkelt institusjon, og her må det vektlegges at kameraovervåkning i seg selv kan fremstå som et stort inngrep i den enkelte students personvern fordi kameraet fanger opp så mye mer enn det man er ute etter å fange opp. I tillegg er misbrukspotensialet større for denne type informasjon enn det som fanges opp når man bruker en person til å monitorere et eksamenslokale under eksamen som jo i realiteten ikke er mye annet enn det den enkelte vakt ser. Det oppfordres derfor til å utvise forsiktighet

[44] http://www.datatilsynet.no/Global/04_veiledere/Kameraoverv%c3%a5king_veileder_nett.pdf

dersom man kommer frem til at vilkårene for å overvåke en eksamenssituasjon med kamera er oppfylt etter en grundig vurdering.

6.4 Plagiatkontroll

6.4.1 Hvordan kommer hensynet til studentens personvern inn ved plagiatkontroll?

Fusk er som nevnt tidligere et brudd på akademisk troverdighet og vi anser det som et samfunnsproblem fordi ingen ønsker at de som fusker skal få en karakter og grad de ikke fortjener. Plagiatkontroll gjennomføres for eksempel på digitalt innleverte hjemmeeksamener og masteroppgaver, og det vil også være naturlig å kontrollere eksamensbesvarelser som er blitt levert inn i en digital eksamensløsning. Plagiering omfattes av definisjonen av fusk, se punkt 6.3.2

En eksamensbesvarelse inneholder blant annet kandidatnummer og emnekode. Kandidatnummeret er koblet mot personen gjennom FS og på andre lister med oversikt over hvem som tilhører hvilket kandidatnummer. Et kandidatnummer er personidentifiserende og er derfor en personopplysning, jf. pol. § 2, 1. Fordi eksamensbesvarelsen derfor kan knyttes til den enkelte studenten, inneholder den personopplysninger. Disse opplysningene er imidlertid erstattet med en koblingsnøkkel, kandidatnummeret, og oppgaven er derfor å anse som avidentifiserte[45]. Det vil ikke være mulig å finne ut hvem opplysningene tilhører uten koblingsnøkkelen som her er kandidatnummeret. Leg merke til at dette i noen tilfeller ikke er helt korrekt. Det er fordi noen fag har svært få studenter, og det kan derfor tenkes at opplysningene likevel ikke er avidentifisert fordi det vil være mulig å lese ut i fra besvarelsen hvem studenten er. Dette er en konkret vurdering hver institusjon må foreta ved behov.

Stadig flere utdanningsinstitusjoner tar i bruk verktøy for plagiatkontroll, slik som for eksempel Ephorus[46]. Verktøyet som blir brukt er eid og driftet av en leverandør som institusjonene må inngå en avtale med før det blir tatt i bruk. Ved bruk av slike verktøy overfører institusjonen personopplysninger sammen med besvarelsen eller oppgaven som skal kontrolleres for fusk til databehandler (den som behandler personopplysninger på vegne av institusjonen) som her er leverandøren. I de tilfellene hvor mistanke om fusk oppstår, vil besvarelsen gå fra å inneholde personopplysninger til å inneholde *sensitive* personopplysninger[47]. Dette medfører at kravene til sikkerheten må heves. Dette skyldes at

[45] Se nærmere om dette under definisjon av begreper punkt 6.2.
[46] https://www.ephorus.com/
[47] Se nærmere om hvorfor disse opplysningene i punkt.6.6.2.

disse opplysningene potensielt kan være svært skadelig for den registrerte, studenten, dersom de misbrukes.

Hver institusjon har et selvstendig ansvar for å sikre at den sensitive informasjon om studenten overføres i henhold til personopplysningslovens bestemmelser med forskrift. Den enkelte institusjon er pliktig, iht. personopplysningsloven, til å sikre at det er inngått gyldig databehandleravtale med leverandør og at dette inkluderer en risikovurdering av plagiatkontrollverktøyet. Se punkt 6.6.3. for hva som skal inngå i en databehandleravtale og risikovurdering.

Vi understreker at når det i et system behandles sensitive personopplysninger, krever det en mer detaljert avtale som sikrer at opplysningene blir behandlet på en riktig og sikker måte. Fordi nivået for sikkerheten som skal ytes legges etter de sensitive data som behandles så vil kravet til sikkerhet for all kommunikasjon i et plagiatkontrollverktøy være høyd selv om man normalt ikke får mange treff i kontrollen. På grunn av dette er det svært viktig at institusjonen, før de tar verktøyet for plagiatkontroll i bruk, foretar en grundig vurdering og eventuelt innhenter ekstern hjelp til dette dersom det er behov for det.

Konklusjon: Hensynet til studentens personvern skal ha en større rolle i vurderingen av hvilket plagiatkontrollverktøy institusjonen skal bruke. Institusjonene må derfor sette seg godt inn i den tekniske oppbygningen til verktøyet og se det opp mot i hvilken grad hensynet til studentens personvern kan ivaretas gjennom gjeldende avtaler, og lovverk dersom leverandør er utenlandsk.

6.5 Kommunikasjon med sensor

6.5.1 Kan institusjonen sende eksamensbesvarelser til sensor via epost?

Under dette punktet har vi valgt å inkludere bachelor- og masteroppgaver fordi det også for mange institusjoner enten er eller vil bli aktuelt å sende besvarelser og oppgaver digitalt til sensor.

Følgende prosess legges til grunn for vurderingen:

- Studenter leverer besvarelsen i den løsningen institusjonen har for innlevering digitalt.
- Eksamenskonsulent henter ut besvarelsene fra løsningen.

- Besvarelsen sendes til sensor via ordinær e-post
- Retur av sensurvedtak, inkludert vurdering av besvarelsen, til administrasjon.

Det forutsettes en toveiskommunikasjon der institusjonene sender besvarelsen, med kandidatnummer som eneste identifikator, og sensor sender karakter inkludert kommentarer tilbake til institusjonen.

Den kommunikasjonen som skjer mellom student og veileder under prosessen med å skrive bachelor-/masteroppgave faller ikke innunder denne vurderingen fordi denne kommunikasjonen baserer seg på frivillighet og samtykke fra de to partene i kommunikasjonen.

Det er viktig å være klar over at hvordan institusjonen kommuniserer med en sensor ikke kan sammenlignes med situasjonen veileder/student. Det er fordi institusjonens(behandlingsansvarlig) kommunikasjon med sensor (databehandler) er en del av en forvaltningssak knyttet til vurderingen av det studenten (den registrerte) har skapt som en del av sin tilknytning til universitet. Studenten er ikke en del av denne kommunikasjonen, noe som stiller strengere krav til partene. Vi mener derfor at den enkelte institusjon bør vurdere om de må inngå databehandleravtale med hver enkelt sensor dersom de velger å bruke en slik løsning. Hver institusjon er ansvarlig for å sikre at den enkelte sensor har den nødvendige sikring av de opplysningene han eller hun behandler for institusjonen.

For å kunne foreta en nærmere vurdering av om institusjonen kan sende en eksamensbesvarelse med epost til sensor, må vi først foreta en vurdering av e-post som kommunikasjonsverktøy.

E-post som teknologi ble utviklet og tatt i bruk i en tid med et helt annet trusselbilde enn dagens. Når vi bruker epost til å sende et ”brev” til noen vil det ikke gå direkte fra A (avsender) til B (mottaker). Ordinær (ukryptert) e-postutveksling mellom to adresser sendes i klartekst via flere instanser (ekstern eposttjener). Institusjonen, som ansvarlig for utsendelsen, har ingen kontroll på denne transporten eller de eksterne eposttjenerne som en sensor bruker, og vi kan dermed hverken garantere at eposten kommer frem til mottaker eller

si noe om og eventuelt hvem og hvor mange som kan ha tilgang til informasjonen på vei til mottaker[48] . Vi har heller ikke mulig til å spore eposten fra utsendelse til mottak.

I ordinær korrespondanse (altså der vi eksempelvis sender en uformell henvendelse) har vi vanligvis redusert behov for sporing. Så lenge meldingene når motparten og dialogen opprettholdes, er hensikten oppnådd. I en mer formell sammenheng, som i en forvaltningssak, kan det derimot være kritisk å kunne vise til nøyaktig når en gitt informasjon kom motparten i hende og sannsynliggjøre hvem som har aksessert informasjonen. Et eksempel på dette er prosesser som sensur av eksamensbesvarelser eller bachelor-/masteroppgaver.

Utsendelse av besvarelse:
Eposten sensor mottar inneholder besvarelsen, emnekode og kandidatnummeret. Kandidatnummeret er koblet mot personen gjennom FS og lister med oversikt over hvem som tilhører hvilket kandidatnummer. Denne informasjonen er tilgjengelig for eksamensadministrasjonen. Oppgaven anses på bakgrunn av dette å inneholde personopplysninger som er avidentifiserte. Her viser vi til nærmere redegjørelse om personopplysninger i eksamensbesvarelser under punkt 6.4 og 6.6.2.

Sensors innsendelse av karakter, inkludert kommentarer:

Når sensor vurderer besvarelsen og setter en karakter, vil vurderingen fort kunne gå fra å inneholde ”alminnelige” personopplysninger til opplysninger som kan være sensitive – og i det minste opplysninger som krever ekstra beskyttelse. Dette fordi sensurering ikke skjer iht. til en gitt standard, noe som igjen åpner for at sensors egen «stil» skinner igjennom. Et resultat av dette er at sensorkommentarer og vurderingene kan inneholde informasjon som det ikke er ønskelig skal komme på avveie (kommentarer som grenser mot personkarakteristikk). I tillegg vil en besvarelse som er innlevert til sensurering bli underlagt plagiatkontroll. Dersom det viser seg at kandidaten har fusket vil den automatisk inneholde sensitive personopplysninger jf. personopplysningsloven § 2 nr. 8 b) noe som gjør at kravene til informasjonssikkerhet heves ytterligere, se nærmere om dette under punkt 6.6.2.

Vi mener ut i fra dette at kommunikasjon av denne type innhold fra institusjonen til sensor aldri bør skje direkte via epost, men gjennom tilgangsbeskyttede løsninger. En

[48] Informasjonen kan være lekket fra kildens lagringsløsning, eller motpartens lagringsløsning. For de systemer der det ikke er mulig å lagre lokal kopi kan fremdeles informasjonen likevel komme på avveie ved bilde/screenshot, manuell avskrift, enten av mottaker selv, vet at noen har holdt øye med mottakers skjerm eller at noen har skaffet seg tilgang til nødvendig tilgangsinformasjon for å utgi seg som mottaker.

eksamensbesvarelse eller bachelor-/masteroppgave er en viktig, og i mange tilfeller avgjørende del av studiet, og det bør derfor ikke formidles til sensor for vurdering gjennom et system man ikke kan garantere for at kommer frem til mottaker, samt sikre sporbarhet for. Det samme vil gjelde for sensur og eventuelle kommentarer/vurderinger institusjonene skal ha i tilbake.

Konklusjon: Institusjonen kan ikke sende eksamensbesvarelse til sensor via epost.

6.6 Bruk av skytjenester ved digital eksamen

6.6.1 Hva er skytjenester

Skytjenester eller såkalt ”Cloud Computing/Cloud Storage” er en samlebetegnelse for datalagring og bruk av programvare på servere som er tilgjengelig i eksterne serverparker tilknyttet internett. Skytjenester tilbyr fleksible løsninger ved at datakraften kan tilpasses behovet til brukeren, og kunden har mulighet til å betale for faktisk bruk. Fordelen ligger i at leverandør har større fleksibilitet og dermed kan tilby billigere tjenester. En av flere utfordringen med skytjenester er at innholdseier ofte ikke har kontroll med hvor innholdet lagres. En annen ulemp ligger i større sikkerhetsrisiko blant annet ved at innhold fra forskjellige eiere kan blandes sammen, en eier kan komme til å få tilgang til en annens innhold og innhold kan forsvinne Dette er en type tjeneste som har blitt svært utbredt de siste årene. Som eksempler på skytjenester kan vi nevne Dropbox, Google-mail, Icloud, Jottacloud og Inspera.

6.6.2 Skytjenester og digital eksamen

Leveranse av skytjenester gir fordeler sammenlignet med leveranser av tradisjonelle servertjenester, som for eksempel lagring av egne data på server lokalt på institusjon, ved at tjenestene kan gi mer fleksible og integrerte løsninger. Skytjenestene fremstår også som tilsynelatende kostnadsbesparende. Disse fordelene medfører imidlertid utfordrende problemstillinger.

Datatilsynet har skissert spesielle problemstillinger som virksomheten må ta stilling til dersom det vurderes å ta i bruk skytjenester, i tillegg til disse ser vi enda flere utfordringer som er mer spesielle for gjennomføring av eksamen. Alle vil ikke drøftes inngående, men de viktigste og mest prinsipielle vil gjennomgås i dette kapittelet.

Vi ser at det er i hovedsak to deler av gjennomføringsprosessen hvor skytjenester vil være aktuelle:

- Midlertidig lagring[49] av eksamensoppgaver, besvarelser og sensurnotater. Det kan også være lagt til rette for at sensorene kan hente ut besvarelsene fra skytjenesten.

- Gjennomføring av selve eksamen. Her kan det være lagt til rette for at studentene både henter ut oppgavene og skriver besvarelsen i selve tjenesten, samt leveringsfunksjon.

Institusjoner som velger å ta i bruk skytjenester har et selvstendig juridisk ansvarlig for at de personopplysninger de er ansvarlige for og som de velger å legge i skyen blir behandlet i tråd med gjeldende regelverk.

Som nevnt tidligere i kapittelet inneholder en eksamensbesvarelse personopplysninger, se bl.a. punkt 6.4.1. Dette betyr at institusjoner i UH-sektoren som vil ta i bruk skytjenester må gjennomføre personvernrelaterte vurderinger – sikre at deres ønsker er i tråd med loven – før de tar i bruk tjenestene. Dette innebærer en klassifisering av innholdet/opplysningene, risikovurdering av tjenesten og inngåelse av en databehandleravtale.

Dersom den aktuelle skytjenesten også tilbyr løsninger for plagiatkontroll, vil det være et ytterligere forhold som medfører at vurderingen av tjenesten må være mer dyptgående – og i de fleste tilfeller bør medføre at man ikke tar i bruk tjenesten. Begrunnelsen for dette er at når mistanke om fusk oppstår, vil besvarelsen gå fra å inneholde *personopplysninger* til å inneholde *sensitive personopplysninger*. Dette medfører at kravene til sikkerhet må heves både når det gjelder overføring av opplysningene samt behandlingene hos databehandler.

En besvarelse som mistenkes for fusk inneholder sensitive opplysninger fordi når fusk, eller forsøk på fusk, anses bevist foreligger det en straffbar handling i den forstand at bestemmelser i universitets- og høgskoleloven er krenket. Forutsetningen er at klagenemnden finner det bevist at en student har «forsøkt å fuske eller forsettlig eller grovt uaktsomt har fusket ved avleggelsen av, eller forut for endelig sensur av, vedkommende eksamen eller prøve, eller under gjennomføringen av vedkommende kurs», jf. uhl. § 4-7, 1 b og § 4-8, 2. Konsekvensen ved fusk er at eksamen kan annulleres og studenten kan utestenges.

[49] Vi forutsetter her en midlertidig lagring og at arkivverdig materiale blir flyttet til godkjent arkiv. I kapittel 3.5 blir det utredet mer om arkivering og lagring.

Det er vår klare oppfatning at besvarelsen derfor omfatter opplysninger om at kandidaten har vært «mistenkt, siktet, tiltalt eller dømt for en straffbar handling», jf. pol. § 2, 8 b.

Sensitive personopplysninger er informasjon som krever en ekstra beskyttelse. Vi tolker ordlyden i personopplysningsloven § 2, nr.8 b "straffbar handling" utvidende i denne sammenhengen. Dersom ordlyden leses i snever forstand er det lett å tolke bestemmelsen dithen at det kun siktes til straffbare forhold etter straffeloven. I ordlyden "straffbar handling" vil det i utvidende forstand være slik vi ser det helt selvsagt at man kan tolke inn sanksjoner som blir ilagt også etter annen lovgivning enn straffelovgivningen, og som derfor er opplysninger som krever ekstra beskyttelse. Vi legger derfor ikke til grunn en analogisk tolkning, men en direkte, utvidende tolkning. Dette støttes av hensynet bak personopplysningsloven, samt Datatilsynets holdning. I forbindelse med arbeidet med RUST - Register for utestengte studenter[50], som ble bestilt av KD og utviklet av UiO, var Datatilsynet klare på at innholdet i dette registeret skulle gis samme beskyttelse som alt innhold i strafferegisteret. RUST muliggjør utveksling av informasjon om vedtak om utestengning i henhold til uhl. blant annet på grunn av fusk.

I tillegg til dette, som etter vår vurdering i seg selv viser klart at informasjon om en mulig fuskesak skal anses som sensitive personopplysninger, taler bestemmelsen i uhl. som omhandler fusk, for at det å fuske må kunne tolkes på lik linje med et straffbart forhold - dette fordi bestemmelsen anvender skyldkravene forsøk på fusk, forsettlig eller grovt uaktsomt har fusket. I en vurdering av hvorvidt det foreligger forsøk på eller fullbyrdet fusk, må det derfor foretas en skyldvurdering på lik linje med vurdering som foretas etter straffelovgivningen.

Dersom det kommer ut til allmenheten at en person er mistenkt for eller faktisk tatt i å fuske så vil dette være informasjon som er svært skadelig for den det gjelder. Jo mer skadelig innholdet i informasjon er for den enkelte (registrerte) desto større beskyttelse skal den gis.

Per i dag er det de færreste leverandørene av skyløsningstjenester som er i stand til å overholder personopplysningsloven når det gjelder behandlinger av sensitive personopplysninger. Merk! Dette må selvfølgelig vurderes konkret ved hver institusjon for hver leverandør. Vurderingen må dokumenteres – blant annet for å dokumentere vurdering ved et evt. tilsyn av Datatilsynet.

[50] http://www.fellesstudentsystem.no/applikasjoner/rust/

6.6.3 Hva skal til for å kunne ta i bruk en skytjeneste?

6.6.3.1 Databehandleravtale – er det mulig å inngå en tilfredsstillende databehandleravtale med leverandør av skytjenester?

Dersom en institusjon velger å bruke en skyleverandør knyttet til gjennomføring av eksamen, så vil denne behandle personopplysninger på vegne av institusjonen og med det være databehandler. Det er et krav i personopplysningsloven at det inngås en skriftlig databehandleravtale mellom behandlingsansvarlige og databehandleren, jf. § 13, jf. 15. Hver enkelt institusjon må selv vurdere om det er mulig å inngå databehandleravtale med den eller de leverandørene av skytjenester som er aktuelle for dem. En slik vurdering vil blant annet inkludere vurdering av de opplysninger som skal behandles. Datatilsynet har per publiseringstidspunkt for dette notat konkludert med at man kan behandle de mer "enkle" personopplysninger, som navn, adresse og mobilnummer i skyen - etter en nøye vurdering. Det man ikke kan er å behandle sensitive eller beskyttelsesverdige opplysninger i skyen. Til dette er tjenestene per i dag ikke egnet[51].

Vi vil gi en oversikt over punkter som bør være inkludert i slik vurdering. Det kan ikke gis en felles konklusjon på om institusjonene kan inngå databehandleravtale med leverandør av skytjenester fordi hver konklusjon institusjonen kommer til er avhengig av den aktuelle leverandøren og deres evne/vilje til å inngå en lovlig databehandleravtale, hva selve tjenesten tilbyr, tjenestens innhold og innholdets (personopplysningenes) behov for beskyttelse.

Delkonklusjon: Hver institusjon må foreta en selvstendig vurdering av hver tjeneste og leverandør, og dersom kravene etter loven og forskrift er oppfylt, kan databehandleravtale inngås.

Datatilsynet har utarbeidet egne veiledere med minimumskrav til en databehandleravtale samt utarbeidet maler for slike avtaler som det anbefales å se nærmere på ved inngåelse av databehandleravtale for hver enkelt institusjon.[52]

6.6.3.2 Hva må være på plass ved inngåelse av en databehandleravtale

Her vil vi kort gå gjennom de punktene som må være oppfylt som minimumskrav.

- Formålet med behandlingen – I henhold til pol. § 11, 1.ledd, bokstav b, jf. § 13, jf. § 15 må institusjonen ha en databehandleravtale for hvert formål. Dersom institusjonen skal

[51] Se mer om skytjenester og vurderinger hos Datatilsynet.
[52] http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/

behandle de samme personopplysningene for to forskjellige formål må det inngås to databehandleravtaler. Det er viktig at formålet er formulert så klart og presisert som mulig. Formålet med behandlingen kan ikke endres underveis uten at databehandleravtalen oppdateres.

- Angivelse av hvilke personopplysninger det er som behandles av databehandler: Det er et krav at man gir en så detaljert angivelse av hvilke personopplysninger som skal behandles som mulig. Det betyr at det for eksempel ikke holder å skrive «relevante personopplysninger» eller «studentdata» dersom man faktisk behandler «navn, adresse, telefonnummer og studentnummer». Dette er viktig blant annet fordi det er et vilkår at man fornyer databehandleravtalen inkludert gjennomfører en ny risikovurdering dersom man i løpet av samarbeidet legger til en eller flere nye personopplysninger til behandlingen.

    - Merk! Dersom databehandler skal behandle sensitive personopplysninger eller personopplysninger som har et ekstra beskyttelsesbehov[53] for institusjonen, så heves kravene til sikkerhet både når det gjelder overføring av opplysningene samt behandlingene hos databehandler. Det kan medføre at man i en risikovurdering kan komme til at man (institusjonen) allikevel ikke kan ta i bruk databehandlers tjenester fordi denne ikke kan oppfylle kravene knyttet til sikkerhet.

- Rutiner for behandling av personopplysningene: Det er viktig at databehandler kan dokumentere at de har etablert gode interne rutiner for den behandling av de opplysningene som skal behandles for institusjonen (behandlingsansvarlig). Det innebærer blant annet at de sjekker om databehandlers rutiner faktisk har tatt inn i seg de krav som stilles i avtalen. Det er institusjonen som har ansvar for å sikre at dette er på plass.

- Regler for utlevering av opplysningene. Det er her snakk om utlevering av data fra databehandler til institusjonen. Det skal være etablert rutiner for hvordan dette skal gjennomføres på en sikkermåte. «Sikker måte» avgjøres i henhold til type opplysninger som behandles. Merk her at overføring på epost er en meget usikker måte, mens overføring på for eksempel en kryptert minnepinne kan være mer sikkert.

[53] Dette er opplysninger som ikke kan defineres som sensitive personopplysninger i lovens forsand, men som av sin art eller i den konkrete sammenheng vil gjøre den registrerte «sårbar» dersom de kommer på avveie.

- Regulere bruk av underleverandører: For at databehandler skal kunne bruke en underleverandør i sin behandling av data/opplysninger for institusjonen må dette være angitt i databehandleravtalen. Merk her at databehandler forplikter seg til å sikre at underleverandøren overholder pliktene i databehandleravtalen. Med andre ord – institusjonen trenger ikke å inngå en egen databehandleravtale med databehandlers underleverandør. Imidlertid må institusjonen være klar over at underleverandøren og dennes forhold må inngå i risikovurderingen.

- Innsyn, retting og sletting: Den registrerte, altså studenten, har en selvstendig rett til å få hvite hva institusjonen har av opplysninger om den enkelte. Institusjonen skal ha etablert rutiner for å håndtere begjæring om innsyn. Denne formen for innsyn må ikke forveksles med innsyn ihht. offentleglova. Dersom studenten krever det har institusjonen plikt til både å rette de opplysninger de har registrert og slette alle opplysninger dersom studenten krever det. Dette følger av bestemmelsene i pol. §§ 18, 27-28

- Risikovurdering: Målet med risikovurdering er å identifisere hendelser som kan få betydning for sikring av personvernet, og uttrykke en hypotese om konsekvenser av hendelsene og sannsynligheten for at de inntreffer. En viktig del av oppgaven er kartlegging av de data som må sikres, og å kartlegge det miljø disse befinner seg i. Risikovurderingen skal i tillegg identifisere behov for risikoreduserende tiltak – ved å sammenligne avdekket risiko med akseptabelt risikonivå. I forlengelsen av dette er det naturlig å gi anbefalinger om sikkerhetstiltak – for å understreke resultater av vurderingen, og til hjelp i videre arbeid. Sikkerhetstiltakene skal stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd.

  En institusjon må både gjøre en risikovurdering før avtalen om databehandling inngås, og gjennomføre jevnlige revisjoner (Kunnskapsdepartementet har i tildelingsbrev angitt en forventning om at dette skal gjøres hvert annet år) av risikovurderinger. Det man her skal legge vekt på er om det har skjedd endringer i situasjonen rund behandlingen – foreligger det svakere eller sterkere risiko for avvikende behandling enn på avtaleinngåelsestidspunktet. Husk at institusjonen også er forpliktet til å gjennomføre en risikorevisjon dersom man legger til nye typer personopplysninger til de data som skal behandles av databehandler.

- Informasjonssikkerhet: Avtalen må inneholde krav til informasjonssikkerhet. Med informasjonssikkerhet i denne sammenhengen menes det at databehandler må ha

rutiner og sikringstiltak på plass for å ivareta konfidensialitet, integritet og tilgjengelighet, jf. forskriftens kap. 2. Nivået for sikkerheten fastsettes etter en godt gjennomført risikovurdering I disse tre nøkkelbegrepene ligger det at informasjonen kun skal være tilgjengelig for *de som skal ha tilgang og motsatt – ikke er tilgjengelig for andre*, at personopplysningene ikke endres uten at det er *autorisert* og *tilsiktet* og at tilgangen til personopplysningene er *tilgjengelig* når det er nødvendig.

- Avvikshåndtering: Databehandler må ha etablert rutiner for håndtering av en avvikssituasjon. Med avvik mener vi en situasjon der opplysningene av en eller annen grunn behandles i strid med databehandleravtalen eller personopplysningsloven med forskrift. Det kan for eksempel være at data fra flere institusjoner blandes, at personopplysninger kommer uvedkommende i hende eller at data ved en feil slettes. I disse rutinene må det være avklart hvordan og når institusjonen og Datatilsynet skal varsles.

- Avtalens varighet og opphør: Avtalen må inneholde et punkt som regulerer hvor lenge avtalen skal gjelde, om den kan fornyes og hva som skal skje med institusjonens data når avtalen opphører. Her er det veldig viktig at man er tydelig på om dataene skal slettes, og da hvordan dette skal foregå. Dersom deler eller alle opplysninger er sensitive, så er kravene til måten data slettes på strengere enn om det kun er snakk om vanlige personopplysninger. Noen ganger er det tilstrekkelig at data overskrives andre ganger må lagringsenheter destrueres.

- Bruk av leverandørs mal for databehandleravtale: Store leverandører har ofte godt innarbeidede standardbetingelser som legges til grunn for avtalen, og forhandlingsrommet kan derfor være litt begrenset. Dette kan føre til utfordrende vurderinger for oss som institusjon siden vi har krav og plikter som vi må følge. Dette var en sentral problemstilling i saken om Narvik og Moss kommunes bruk av Googles tjenester[54] som Datatilsynet vurderte. Datatilsynet var klare i sin vurdering og mener at selv om leverandøren har betingelser som ikke stemmer overens med det norske regelverket, vil ikke det frita behandlingsansvarlig (institusjonen) fra sine plikter. Det er institusjonens ansvar å inngå en lovlig databehandleravtale, og vi kan ikke gi tilgang til studentenes personopplysninger uten at en tilfredsstillende databehandleravtale er på plass.

[54] http://www.datatilsynet.no/Regelverk/Tilsynsrapporter/2012/Bruk-av-nettskytjenester/

6.6.3.3 Risikovurdering

Institusjonen (behandlingsansvarlig) må gjennomføre en risikovurdering jf. pol. § 13, jf. forskriftens kap. 2. Det er en forutsetning for at en databehandleravtale skal være gyldig at en reell risikovurdering er gjennomført, jf. pof. § 2-4. En risikovurdering skal definere uønskede situasjoner og risikoen for at disse kan skje. For å kunne gjennomføre denne vurderingen må det bestemmes for hvert enkelt forhold hva som er en akseptabel risiko forbundet med behandling av personopplysninger i den aktuelle skytjenesten. Kjernen i behandlingen er å vurdere typen personopplysninger opp mot den behandling databehandler vil gi den. Sensitive personopplysninger vil kreve en helt annen type – og adskillig strengere – sikkerhet enn «alminnelige personopplysninger» som navn og telefonnummer.

Det må også skisseres opp hvordan en situasjon skal håndteres og hvilke sikkerhetstiltak som skal iverksettes både før en situasjon oppstår og i etterkant. Disse tiltakene skal stå i forhold til sannsynligheten og konsekvensen av sikkerhetsbrudd, jf. forskriften § 2-1. Selve arbeidet med risikovurderingen må ikke være mer omfattende enn nødvendig, og det er en vurdering de ansvarlige ved institusjonen selv må foreta. Videre heter det i merknaden til § 2-4 om risikovurdering at arbeidet med å avdekke risiko ikke bør være mer omfattende eller formalisert enn strengt tatt nødvendig.

En risikovurdering skal gjøres i forkant av en inngåelse av databehandleravtale. Senere skal ny risikovurdering gjennomføres dersom det oppstår endringer som har betydning for sikkerheten av tjenesten og/eller opplysningene til studentene, jf. forskriften § 2-4, 2.ledd, 2. setning. I tildelingsbrevet til Universitetet i Oslo fra Kunnskapsdepartementet i 2013 ble det påpekt under punktet om Sikkerhet og Beredskap at ROS-analyser (risiko- og sårbarhetsanalyser) skal revideres minst annet hvert år.[55] Risikovurdering av en skytjeneste som institusjonen avholder digitale eksamen i, vil kunne omfattes av en ROS-analyse. Her må det avgjøres hos hver enkelt institusjon hvilke systemer og tjenester som omfattes av dette. I alle tilfeller ser vi det slik at institusjonene bør ha en gjennomgang av risikovurderingen for skytjenesten forholdsvis ofte.

Datatilsynet har utarbeidet egen veiledning for risikovurdering av informasjonssystem som vi anbefaler å sette seg godt inn i forkant av et slikt arbeide.[56]

[55] http://www.uio.no/for-ansatte/arbeidsstotte/okonomi/Fordeling/Enhetenes%20disponeringsskriv%202010/tildelingsbrev-2013-kd-med-vedlegg.pdf

[56] https://www.datatilsynet.no/Global/04_veiledere/Risikoveileder_pdf.pdf

Resultatet av en risikovurdering kan være at institusjonen finner at sikkerhetsnivået ikke er akseptabelt og at skytjenesten dermed ikke kan benyttes. Det kan imidlertid også være at sikkerhetsnivået som er etablert i skyen er høyere enn det institusjonen selv har definert som akseptabel risiko. Det er derfor viktig å ta hensyn til at sikkerhetstiltakene skal stå i forhold til sannsynligheten for og konsekvensene av sikkerhetsbrudd. Det skal altså være forholdsmessighet. Dette innebærer at institusjonen må legge seg på et høyere sikkerhetsnivå når det er opplysninger som krever ekstra beskyttelse enn når mer alminnelige personopplysninger behandles.

6.6.3.4. Revisjon av risikovurdering

Vi definerer sikkerhetsrevisjon som en etterprøving av sikkerhetsarbeidet for å bekrefte at de sikkerhetstiltakene som ble besluttet iverksatt er i faktisk bruk og fungerer. Den faktiske bruken av skytjenesten skal samsvare med de retningslinjene som ble skissert i planleggingsfasen, og da særlig i risikovurderingen. Sikkerhetsrevisjon er hjemlet i personopplysningsforskriftens § 2-5.

En av de viktigste delene av kravene til informasjonssikkerhet er at det foreligger en forpliktelse til å gjennomføre jevnlige sikkerhetsrevisjoner, jf. forskriftens § 2-5, 1. ledd. Institusjonen (behandlingsansvarlig) må jevnlig kontrollere bruken av skytjenestene og at de besluttede sikkerhetstiltakene fungerer. (Dette må gjerne gjøres av databehandler, og blir ofte det. Men det ligger likevel et ansvar på institusjonen som behandlingsansvarlig å etterprøve sikkerhetsrevisjonen for å sikre at bruken og tjenesten er forsvarlig.)

For at en sikkerhetsrevisjon skal ha en hensikt er det avgjørende at leverandøren (databehandleren) kan legge frem dokumentasjon for utformingen av tjenesten og hvilke sikkerhetsløsninger de tilbyr. Dette må være på plass for at institusjonen kan være sikker på at tjenesten tilfredsstiller de krav de har. Leverandøren kan heller ikke endre sikkerhetstiltak uten at institusjonen er blitt tilstrekkelig informert og har godkjent endringen. Dette bør være med i avtalen som inngås mellom institusjonen og leverandør. Disse punktene er også presisert av Datatilsynet i artikkel om «Bruk av nettskytjenester».[57]

Et spørsmål som ble vurdert av Datatilsynet i Narvikkommunesaken, var om tredjepartsrevisjoner er tilstrekkelig for å oppfylle kravet etter forskriften § 2-5. Google hadde forpliktet seg overfor sine kunder til jevnlig å foreta sikkerhetsrevisjoner, og gi kundene tilgang til revisjonsrapportene. Google benyttet en tredjepart til å utføre slike sikkerhetsrevisjoner. Datatilsynet anså dette tilstrekkelig, men presiserte at kommunen

[57] http://www.datatilsynet.no/Teknologi/Nettsky---Cloud-Computing/Cloud-Computing/

jevnlig måtte følge opp at revisjonen ble gjennomført og selv gjennomgå revisjonsrapportene. Vi ser det som mulig problematisk at dersom institusjonen velger å godta tredjepartsrevisjon, vil ikke hver enkelt leverandør selv gå inn og foreta revisjonene, noe som i seg selv i våre øyne kan utgjøre en sikkerhetsrisiko fordi kontrollen over at alt blir gjennomgått blir delegert til en utenforstående tredjepart.

Det er også viktig at sikkerhetstiltakene dokumenteres, jf. forskriften kap.2. Dokumentasjonen skal være tilgjengelig for utvalgte medarbeidere hos begge parter, samt for Datatilsynet og Personvernnemnda dersom det blir aktuelt.

6.6.4 Forholdet til databehandler (leverandør av skytjenester)

Leverandør i denne sammenhengen er den/de selskapene/institusjonene institusjonen kjøper en tjeneste av, altså de som leverer skytjenester institusjonen ønsker å bruke til å gjennomføre digital eksamen. Leverandør behandler studentenes personopplysninger på vegne av institusjonen. Institusjonen er behandlingsansvar og leverandør er databehandler. Forholdet til leverandør som databehandler vil være ulikt ut i fra hvilket lands lovgivning leverandøren må forholde seg til. Disse forholdene kan deles inn i tre ulike deler; underlagt norsk lovgivning, innenfor EU/EØS og tredjeland.

1) Leverandør av skytjenester i Norge
Dersom leverandør har serverparken (lagringsenheter) i Norge og selskapet er norskeid, vil leverandør på lik linje med institusjonene være underlagt norsk lovgivning. Forutsetningen for å inngå en gyldig databehandleravtale, samt muligheten for å oppfylle de andre kravene loven stiller til behandlingsansvarlig for at denne skal kunne ta i bruk skytjenester på en riktig måte, vil absolutt være god. Vi vil likevel understreke at selv om leverandør er underlagt norsk lovgivning er institusjonen også i disse tilfellene selv ansvarlig for å foreta en konkret vurdering for den enkelte tjeneste, jf. vurderingspunktene som er skissert over i dette kapittelet.

Konklusjon:
Utgangspunktet for å foreta en vurdering av om en avtale kan inngås med norsk leverandør, vil være at begge parter er underlagt norsk lovgivning og derfor har samme regelverk de må forholde seg til. Det gjør prosessen for å komme frem til et sikkert og godt avtalegrunnlag bedre.

2) Leverandør av skytjenester i Norge bruker underleverandør
I et partsforhold mellom to avtaleparter vil i vår sammenheng en tredjepart være for

eksempel en underleverandør som ikke i utgangspunktet er en del av avtalen, eller myndighetene i det land som den ene parten hører innunder.

Det kan være problematisk at underleverandør kan være underlagt et annet regelsett enn behandlingsansvarlig, og det kan få konsekvenser for hvordan databehandler behandler opplysningene. Dette illustrerer problemet: Her siterer vi Datatilsynet fra deres svar til Moss Kommune av 21. september 2012: " I tillegg er det opplyst at Microsoft vil kunne bli nødt til å utlevere opplysninger til "*law enforcement [authorities]*". Vi antar at det siktes til krav om utlevering av persondata som skriver seg fra andre jurisdiksjoner enn den norske, for eksempel i forbindelse med etterforskning av straffbare forhold. Så fremt det enkelte kravet er rettslig bindende overfor tjenesteleverandøren, og en påfølgende utlevering ikke er i strid med øvrige bestemmelser i norsk lov, vil utleveringer fra tjenesteleverandøren til nevnte behandlingsformål kunne finne sted. Behandlingsansvarlig bør imidlertid også forsikre seg om at databehandleren kan garantere at ingen personopplysninger vil bli utlevert til noe annet lands justismyndigheter, med mindre de ovennevnte kriteriene er oppfylt.»[58]

Dersom det er spørsmål om personopplysninger kan overføres til en tredjepart som er underleverandør til hovedleverandøren av skytjenesten, må dette avtales særskilt i både hovedavtalen og databehandleravtalen. Her er bestemmelsen i pof. § 2-15 utfyllende for hva som kreves av sikkerhet hos andre virksomheter enn kontraktsparten.

Konklusjon:
Utlevering av data til en tredjepart kan skje dersom det 1) foreligger et rettslig grunnlag i det aktuelle tredjelandet og 2) utlevering ikke krenker norsk lov – noe som også kan forekomme i Norge.

3) Leverandør av skytjenester i EU/EØS?
Institusjoner som vurderer å inngå avtale med en leverandør som har lagringsenheter/servere i utlandet må forholde seg til personopplysningsloven kapittel 5 og forskriften kapittel 6.

Det grunnleggende vilkåret etter pol.§ 29 er at personopplysninger kun kan overføres til land som «sikrer en forsvarlig behandling av opplysningen». De landene som har innført Personverndirektivet[59] som handler om beskyttelse av personer under behandling av personopplysninger og fri utveksling av disse opplysningene, oppfyller automatisk kravet til en forsvarlig behandling.

[58] http://www.datatilsynet.no/Sektor/Overfoering/Safe-Harbor-prinsippene/
[59] http://www.lovdata.no/pro/#document/DLX3/eu/31995l0046

EU- og EØS-land har alle innført dette direktivet og oppfyller derfor det grunnleggende kravet til overføring av personopplysninger til land utenfor Norge.

Konklusjon:
Så lenge leverandøren kan oppfylle de kravene som stilles til å behandle personopplysninger, som er skissert over i kapittelet, vil det være trygt og lovlig å overføre personopplysninger og med det inngå avtale om kjøp av skytjeneste.

Merk at innholdet i punkt 6.6.4, 2) om de tilfeller der skyleverandør bruker underleverandør også kommer til anvendelse her.

4) Leverandør av skytjenester i et tredjeland
Personopplysninger kan ikke uten videre overføres til land utenfor EØS/EU-sonen. Reguleringen i det som kalles tredjeland kan være en helt annen enn i Norge og dermed kreve helt andre forholdsregler fra behandlingsansvarlig.

Det første vilkåret som må være oppfylt er at kravet til forsvarlig behandling etter pol. § 29 er tilfredsstilt. I praksis betyr det at overføring av persondata til andre land enn medlemsstatene i EU og EØS-landene, i utgangspunkt er utelukket. Imidlertid er det etablert løsninger som åpner for unntak fra hovedregelen. Dataeksportøren, her institusjonen, kan for eksempel gi egne individuelle og tilstrekkelige garantier, eller EU-kommisjonen kan ha besluttet at visse enkeltstater er trygge mottakerstater.

Dersom eksempelvis tjenesteleverandøren er sertifisert under Safe Harbor-prinsippene[60] [61], kan personopplysninger overføres fra et EØS-/EU-land til foretaket i USA iht. nærmere angitte regler. Disse reglene vil vi ikke drøfte nærmere da det ikke er en del av bestillingen.

Blant annet kan skytjenesteleverandøren være forpliktet til å gi myndighetene i det landet serveren er fysisk plassert tilgang til våre data. Lovverket i dette landet kan også være atskillig svakere når det gjelder bl.a. krav til sikring av data, noe som vi også ser som bekymringsverdig. Det er også enkelte skytjenesteleverandører som ikke påtar seg ansvar for tap av data. De krever i tjenesteavtalene at kunden selv tar backup. Dette er en forutsetning vi ser kan være veldig problematisk å godta ettersom det er leverandør som sitter på oppbygningen og sikringen av tjenesten.

[60] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DA:PDF

[61] Datatilsynet om Safe Harbour-prinsippene: http://www.datatilsynet.no/Sektor/Overfoering/Safe-Harbor-prinsippene/

Det å ha tilstrekkelig kontroll over data og sikkerhet for at det ikke skal kompromitteres av tredjepart, er en utfordring for leverandørene av skybaserte tjenester. Leverandørene må kunne dokumentere for kundene at de gjennom programvare og virtualisering kan etablere sikre skiller mellom virksomhetene i skyen, samt at de er i stand til implementere brukerstyring og adgangskontroll som fungerer optimalt. For brukerne må tjenesten i skyen være trygt og oversiktlig før den kan tas i bruk.

Konklusjon:
Vi ser flere vanskelige utfordringer med å forholde seg til leverandører som ikke forholder seg til personvernlovgivning tilsvarende den som gjelder i Norge. Det er derfor viktig at institusjonen, dersom den vurderer å ta i bruk en tjeneste i skyen, forsikrer seg om at studentenes personopplysninger er tilstrekkelig trygge og at behandlingen oppfyller kravet etter bestemmelsen i pol. § 29.

Merk at innholdet i punkt 6.6.4, 2) om de tilfeller der skyleverandør bruker underleverandør også kommer til anvendelse her.

6.7 Hva skal til for å kunne ta i bruk skytjenester?

Som vi har skissert over, er det mange og viktige vilkår og forutsetninger som må være vurdert og avklart før institusjonen kan ta i bruk skytjenester for å gjennomføre digital eksamen.

Datatilsynet har satt opp avgjørende punkter[62] sett ut i fra de krav personopplysningsloven med forskrifter stiller, og i tillegg til disse ser vi at det vil være enda flere forutsetninger og utfordringer som vi kan se fra blant annet et sikkerhetsmessig og opphavsrettslig syn. Disse problemstillingene må også sånn vi ser det vurderes og avklares i forkant av en igangsettelse av skytjenester for gjennomføring av digital eksamen.

Vi vil nå kort fremstille de ulike punktene som må være vurdert og avklart før institusjonen kan ta i bruk skytjenester. Deler av punktene er utredet tidligere i kapittelet og repeteres her.

- Grundige risiko- og sårbarhetsanalyser må gjennomføres i forkant. Institusjonen må stille seg spørsmålet om hva som kan gå galt, sannsynligheten for at det gjør det og hvilke følger det eventuelt kan få, både for den enkelte registrerte studenten og institusjonen.

Dette er punkter som bør vurderes i en risikovurdering:

[62] http://www.datatilsynet.no/Regelverk/Tilsynsrapporter/2012/Bruk-av-nettskytjenester/

1. Hva er faren for at sensitive data kommer på avveie som følge av datainnbrudd og påfølgende datatap? Sensitive data tilsier høy sikkerhet!

2. Hva er faren for at data blir tilgjengeliggjort, enten ved en glipp fra leverandørs side eller fordi myndighetene i leverandørens opphavsland ber om innsyn.

3. Hvilken kontroll har institusjonen over forvaltningen av data som lagres i skyen?

4. Hvem har tilgang til hva av data hos leverandør?

5. Hva er faren for at skytjenesteleverandøren mister kontroll med brukers data, noe som igjen kan resultere i at data ikke kan gjenfinnes? – Dette anser vi som særlig avgjørende for en tjeneste for bruk under eksamen.

6. Hva er faren for at data er utilgjengelig fordi tjenesten er utilgjengelig. – Dette anser vi også som avgjørende for en tjeneste for bruk under eksamen.

7. Hva er skytjenestens yteevne/tilgjengelighet, herunder hvorvidt tilgang til egne data er konstant og holder akseptabel leveringskvalitet?

8. Tar løsningen høyde for registrering av autorisert og uautorisert bruk?

9. Hva slags rett til innsyn i løsningen har institusjonen som kunde?

10. Hvilken kontroll har institusjonen når det kommer til krav til rutiner for sletting / oppbevaring / arkivering?

- Det må ved tjenesteoppstart foreligge en tilfredsstillende og gyldig inngått databehandleravtale, jf. pol. § 13, jf. § 15 og en godt gjennomført risikovurdering av tjenesten som er i tråd med norsk regelverk. Institusjonen er selv ansvarlig for å forsikre seg om at 1) avtalen oppfyller personopplysningslovens krav og 2) databehandler (skytjenesteleverandøren) faktisk oppfyller de vilkår som er angitt i avtalen. Vi understreker igjen at det er den enkelte institusjon som har ansvar for at lovens krav følges.

- Institusjonen må være garantert at databehandleravtalen er den som gjelder og at leverandørens generelle personvernerklæring ikke går utover avtalen.

- Det må sikres at databehandleravtalen mellom partene ved motstrid har rang foran databehandler/tjenesteleverandørens generelle personvernerklæring.

- Jevnlig sikkerhetsrevisjon må gjennomføres for å sikre at databehandleravtalen følges.

- Institusjonene må ha med seg inn i vurderingen av sikkerhetsløsningene ved skytjenesten at dersom det er svakheter i løsningen som gjør at oppgaver og besvarelser blir gjort tilgjengelige for allmenheten, kan dette skje uten at opphavsmannen (her studentene) er klar over det.

Konklusjon: Skytjenesteløsninger er slik vi ser det utfordrende juridisk sett og det krever mye forarbeid av institusjonen før det kan vedtas å ta i bruk slike løsninger. På den andre siden ser vi at behovet og etterspørselen er stor etter denne type løsninger, og det er derfor et arbeid hver enkelt institusjon er nødt til å gjennomføre på et visst punkt i fremtiden dersom det ikke allerede er gjort.

Vi har i dette kapittelet forsøkt å skissere opp de kravene som stilles opp etter personopplysningsloven med forskrifter i tillegg til de ekstra utfordringene vi ser vil dukke opp med en eksamensløsning i skyen.

Konklusjonen er derfor at hver institusjon må selv foreta en vurdering av om den aktuelle løsningen tilfredsstiller de kravene institusjonen selv har og de kravene som vi er nødt til å følge etter det gjeldende regelverket.

7 Avslutning

Målet med denne utredningen var å identifisere, systematisere og vurdere juridiske problemstillinger knyttet til digital vurdering og eksamen.

Dette er et stort fagområde med mange ulike problemstillinger og innfallsvinkler. Arbeidsgruppen har valgt den struktur vi anså som mest oversiktlig og praktisk, både for å få frem alle relevante problemstillinger og vurderinger, samtidig som vi ønsket at vurderingene skulle være så mottakervennlig som mulig.

Vi er fem jurister som har ført utredningen «i pennen», og det vises naturlig nok i de enkelte delene at hver person har sin fremstillingsmåte og skrivestil. Hver av juristene står ansvarlig for hver sin del, derav jeg-formen, men alle i arbeidsgruppen har jobbet sammen om å identifisere problemstillinger, vi har lest vurderingene og kommet med innspill og kommentarer. I de delene hvor flere har skrevet brukes vi-form i teksten.

Dokumentet er, som nevnt innledningsvis, en utredning som tar opp de problemstillingene vi ser som aktuelle for digital vurdering og eksamen på nåværende tidspunkt – sommeren 2014. Selv om den digitale utviklingen går fort, og på noen områder går så raskt at det er vanskelig å holde tritt blant annet når det gjelder de juridiske implikasjonene, må vi alle forholde oss til de lovene og reglene vi har i dag. Vi forventer at det vil være behov for en revidering av utredningen, når institusjonene har fått mer erfaring med gjennomføring av digital eksamen. Vi har derfor kalt vurderingen versjon 1.0.

Deltakerne i arbeidsgruppen har selv lært mye underveis i denne prosessen, og vi håper at utredningen vil være et godt utgangspunkt og arbeidsverktøy for sektoren.

Vedlegg

Vedlegg 1: Oversikt eksamensprosessen, laget ved NTNU.

Vedlegg 2: Vedtak om bevaring og kassasjon av eksamensbesvarelser m.m. i universitetssektoren og de vitenskapelige høgskolene fra Riksarkivaren – 2005/13708 ELFU

Vedlegg 3: Vedtak om bevaring og kassasjon av eksamensbesvarelser i høgskolesektoren fra Riksarkivaren – 2007/9563 ANNMAL

Vedlegg 4: Brev fra Kunnskapsdepartementet til Politihøgskolen, datert 05.05.2006.