UiO : Universitetet i Oslo
Universitetets senter for informasjonsteknologi

Notat

Til: Prosjektet digitalt læringsmiljø
v/ prosjektleder Svein Harald Kleivane

Fra:
Maren Magnus Jegersberg
Seniorrådgiver

Dato: 20. juni 2017

Vurdering av Læringsplattformene i UNINETTs rammeavtale

På bestilling fra prosjektet Digitalt læringsmiljø har de juridiske sidene ved de enkelte læringsplattformene i UNINETTs rammeavtale og kravsspesifikasjon med svar fra leverandører blitt gjennomgått. Målet var å identifisere mulige juridiske utfordringer ved avtalene og svarene til leverandørene i kravspesifikasjonen og hvilke konsekvenser disse eventuelt kan få. For alle tre leverandørene er det noen spørsmål som må besvares før avtale kan inngås og for et par tilfeller må det gjøres justeringer i avtaleverket, herunder særlig tillegg til avtalen som den ene leverandøren, Canvas, har lagt ved. Men det ingen av disse spørsmålene eller endringene som vi vil anta vil være store utfordringer eller sette en stopp for prosessen, og vi forventer at leverandøren ønsker dialog med oss på de relevante punktene.

Tilbakemeldingene er kun basert på de skriftlige svarene fra leverandørene og hva som fremkommer av avtalene, samt eventuelle tilleggsdokumenter leverandørene har lagt ved, og ikke en teknisk gjennomgang av læringsplattformene via en ROS-analyse.

Alle leverandørene gir gode og utfyllende svar. Overordnet fremstår NEO som noe uerfaren må de juridiske områdene sett ut i fra svarene deres, mens Brightspace fremstår veldig kundeorientert og legger opp til at mye skal løses i dialog med kunden og etter kundens krav. Canvas har som nevnt noen elementer i deres tillegg til avtalen som må justeres for å være i henhold til norsk lov og det må opprettes dialog med dem rundt disse punktene.

For alle tre leverandørene må det gjøres utsjekk i forhold til hva slags type data – herunder reelle kundedata eller testbase - de tester på i drift og utvikling. Sett i lys av nye personvernregler er leverandørene pliktige til å være kompatible med EUs personvernforordning både fordi de leverer tjenester til norske kunder, samt at UiO som kunde må sikre seg at leverandørene oppfyller de krav vi har som behandlingsansvarlig.

To av leverandørene beskriver at de bruker EUs standardkontrakt for overføring av personopplysninger. Denne må inngås uansett valg av leverandør ettersom leverandørene er henholdsvis fra USA og Canada og dermed regnet som tredjeland.

Under følger noen konkrete tilbakemeldinger og oppfølgingspunkter for de enkelte leverandørene (Her er det ikke henvist til de konkrete punktene i rammeavtalen):

NEO:
«Learning analytics tools»: Det angis at det er omfattende muligheter for «learning analytics tools». Det kommer ikke frem om det er mulig å velge hvilke rapporter vi kan bestille og om vi kan styre hvem som kan be om rapportene. Noen av rapportene fremstår som forholdsvis inngripende og UiO bør ha en gjennomgang på hvilke rapporter som er ønskelig og som er ihht. personopplysningslovverket sett opp mot.

Oppdateringer: Det kommer nye oppdateringer daglig som kunden selv velger å akseptere. Det er svært hyppige oppdateringer og noen av oppdateringene vil nok kunne utløse revisjoner av ROS, i alle tilfeller må dette vurderes av dem som godtar. Dette må utarbeides gode rutiner som hensyntar dette aspektet.

Logger. Det er to typer logger som blir beskrevet. Det kan være problematisk at det for den ene typen ikke kan gis innsyn. Loggene holdes heller ikke adskilt for hver kunde, noe det bør være. Her må det bes om en ytterligere beskrivelse og vi bør sette krav for håndteringen av loggene. typen ikke lar kunden få innsyn og at de ikke holder disse adskilt for hver kunde. Det er positivt at loggene slettes hyppig, men det bør gjøres en vurdering av om vi skal kreve ytterligere lagrinslengde.

For den andre typen logg går det frem at disse oppbevares for alltid. Her må vi gjøre en vurdering av hvor lenge vi mener disse skal oppbevares og kreve en tidsbegrensning.

Caching til memcache cluster: Det fremstår som noe omfattende hva de cacher og det fremkommer ikke et saklig behov for det. Dette må vurderes sammen med IT-sikkerhet og deretter eventuelt kreve mindre omfangsrik caching.

Leverandøren oppgir ingen informasjon om eventuelt andre underleverandører. Dette må fremskaffes og avtalereguleres i databehandleravtalen.

Leverandøren beskriver heller ingenting om deres policy rundt innsyn og utlevering av opplysninger til myndigheter og andre aktører, noe vi bør kreve å få en uttalelse på. Det kan også vurderes om dette bør inn i avtalen.

Brightspace:
Det er positivt at leverandøren fremhever tilgangskontrollen og at den skal ligge på organisasjonsnivå og ikke følge hvem som har inngått rammeavtalen.

«Learning analytics tools»: Det angis at det er omfattende muligheter for «learning analytics tools». Det kommer ikke frem om det er mulig å velge hvilke rapporter vi kan bestille og om vi kan styre hvem som kan be om rapportene. Noen av rapportene fremstår som forholdsvis inngripende og UiO bør ha en gjennomgang på hvilke rapporter som er ønskelig og som er ihht. personopplysningslovverket sett opp mot.

Det er positivt at leverandøren fremhever at kunden i dialog med leverandør kan velge hvilke funksjoner vi vil ha og lovlig kan bruke.

Logger: Logghåndteringen er i overensstemmelse med våre krav og vi kan få utlevert det som tilhører oss. Det fremstår som at vi kan sette lengden på lagring av logger selv, men det må avklares. Automatikk vil her være å foretrekke.

«The Data Purge Pool»: Noe uklart hva dette er og det ser ut som at de samler og oppbevarer mye data, herunder også personopplysninger. Det må bes om en nærmere beskrivelse av hva det er og hva det skal brukes til.

Leverandøren oppgir ingen informasjon om eventuelt andre underleverandører. Dette må fremskaffes og avtalereguleres i databehandleravtalen.

Leverandøren beskriver heller ingenting om deres policy rundt innsyn og utlevering av opplysninger til myndigheter og andre aktører, noe vi bør kreve å få en uttalelse på. Det kan også vurderes om dette bør inn i avtalen.

Leverandøren fremhever at de er villige til å gå dialog rundt ulike problemstillinger som kunden ønsker å ta opp og anerkjenner at Uninett og institusjonene har fokus på personvern og datahåndtering. Leverandøren fremhever også at de er villige til å gjøre endringer i kontrakten som er tilpasset kunden.

Canvas:
«Learning analytics tools»: Det angis at det er omfattende muligheter for «learning analytics tools». Det kommer ikke frem om det er mulig å velge hvilke rapporter vi kan bestille og om vi kan styre hvem som kan be om rapportene. Noen av rapportene fremstår som forholdsvis inngripende og UiO bør ha en gjennomgang på hvilke rapporter som er ønskelig og som er ihht. personopplysningslovverket sett opp mot.

Konto: her kan vi velge egen konto eller sub-konto under UNINETT. Her bør UiO opprette egen konto for å ha det separat fra UNINETT og øvrige institusjoner.

Integrasjon med Flicr: Leverandøren beskriver at de har en integrasjon med Flicr. Det fremgår ikke hva slags informasjon de overfører dit. Dette må beskrives og vurdert ihht. tilbakemeldingene vi får.

Sletting av innhold i studentkonto: Innholdet i en studentkonto blir aldri slettet så lenge det er en aktiv ID. Det må rettes en bestilling til Avdeling for Fagstøtte for å vurdere hvor lenge vi kan/skal oppbevare det ihht. regler rundt oppbevaring av besvarelser. Deretter må det gis tilbakemelding til leverandør dersom det må foretas endringer i oppbevaringsperioden.

Aktivitet og brukerinfo: Denne informasjonen er tilgjengelig for UiO i 30 dager og slettes fra konto etter det. Men Canvas kan sammenstille utover det og tilbake hele kontraktsperioden. Dette er ikke i henhold til norske personvernregler. Her må vi kunne stille krav til at alt blir slettet ved et visst tidspunkt hvor vi leverer parameter.

Instructure Data Processing Addendum: Leverandøren har et eget bilag med til avtalen som heter Instructure Data Processing Addendum. Der står det blant annet at hele avtalen er konfidensiell og at den kun kan gis ut til tilsynsmyndigheter og andre myndigheter. Dette er problematisk for oss fordi vi offentleglova ikke gir mulighet til å hele avtalene etter signering, kun deler av dem. Dette må vi ha en dialog med Canvas på og vi må ha på plass en endring i avtalen/eventuelt et tillegg før avtalen kan signeres.

Taushetsplikt: Ved gjennomføring av ROS-analyse i forbindelse med anskaffelsesprosessen ble alle deltakere bedt om å signere på taushetserklæring som i altfor stor grad omfattende og ikke i henhold til norsk personvernlovgivning. Ved en gjennomføring av ROS for UiO for denne læringsplattformen og andre lignende tilfeller må det passes på at ingen signerer slike taushetserklæringer uten at de er kvalitetssikret og eventuelt endret i samråd med leverandøren.