BRUGERPORTALSINITIATIVET

GENEREL KRAVSPECIFIKATION – TILLÆG

Læringsplatforme - Brugerportalsinitiativet

INFORMATIONSSIKKERHED OG SIKRING AF PERSONDATA

Krav til informationssikkerhed og sikring af persondata i læringsplatformene - BPI

Dette dokument udgør det resterende afsnit til ”Generel kravspecifikation – Læringsplatforme -Brugerportalsinitiativet”, der blev udgivet 1/8 2016. Dokumentet indeholder KL’s anbefalinger til krav, der stilles til leverandørerne under kommunernes anskaffelse af læringsplatforme under Brugerportalsinitiativet.

Indhold

1 Krav til datasikkerhed

Som led i arbejdet, med udbredelse af BPI og i lyset af blandt andet det generelt stigende fokus på digital sikkerhed i samfundet, det evigt foranderlige trusselsbillede samt den kommende databeskyttelsesforordning, anbefaler KL at der stilles krav til leverandører af læringsplatforme om datasikkerhed.

1.2 Databehandleraftale

Der skal indgås en databehandleraftale mellem kunden og leverandøren.

Kunden er som kommune ansvarlig for borgernes data, og er dermed også dataansvarlig for læringsplatformen. En dataansvarlig kan vælge at overlade det til en anden eller at udføre selve den praktiske behandling af personoplysninger på den dataansvarliges vegne.

Behandlingen ved en databehandler kræver, at der indgås en skriftlig aftale herom imellem den dataansvarlige og databehandleren (en såkaldt databehandleraftale).

Databehandleraftalen skal udformes efter retningslinjer fremsat af datatilsynet, som for eksempel ses i artiklen: ”Databehandler - Krav om skriftlig kontrakt med databehandler”, der kan findes på Datatilsynets hjemmeside.

Som en del af databehandleraftalen skal det præciseres, at Persondataloven (*Lov 429 af 31. maj 2000*) og Sikkerhedsbekendtgørelsen (*BEK nr 528 af 15/06/2000 - Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning*) efterleves.

Krav #1	**Databehandleraftale**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren skal underskrive databehandleraftale udarbejdet af kunden. Leverandøren skal indgå databehandleraftaler med eventuelle underdatabehandlere sådan, at der er de samme forpligtelser som dem leverandøren er pålagt i medfør af databehandleraftale med kunden. Endvidere skal kunden som dataansvarlig godkende de underdatabehandlere, som leverandøren ønsker at anvende i forbindelse med leverancen.		

1.3 Risiko og Konsekvensanalyse

Den 27. april 2016 blev der opnået enighed om indholdet i en ny EU Databeskyttelsesforordning med ikrafttrædelse den 25. maj 2018. Selvom der er et stykke tid til, at databeskyttelsesforordningen træder i kraft, er det relevant at gøre sig overvejelser omkring forordningens krav.

Krav #2	**Bidrag til konsekvensanalyse**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Databeskyttelsesforordningen lægger op til, at dataansvarlige gennemfører risiko- og konsekvensanalyse, der blandt andet skal indeholde en beskrivelse af planlagte behandlingsaktiviteter, en risikovurdering og beskrivelse af de sikringsforanstaltninger, der påtænkes gennemført til sikring af persondata. Herunder krav, der sikrer, at kunden kan foretage konsekvensanalyse af deres samlede systemlandskab. Leverandøren forpligtes til at medvirke til vurdering af beskyttelse mod trusler mod organisationen og fysiske personers data i læringsplatformen, sådan at der etableres og godkendes en konsekvensanalyse, der forholder sig til de aspekter, der fremgår af forordningens krav om konsekvensanalyse og vedrører læringsplatformen. I deltagelsen forpligtes leverandøren til at følge de standarder for konsekvensanalyse, der udstikkes af kunden, for eksempel ISO27005.		

1.3.1 Roller og rettigheder

For at kunne foretage konsekvensanalyse, er det nødvendigt med en beskrivelse af roller og rettigheder for identiteter og aktører i læringsplatformen.

Med identiteter menes brugeridentiteter – hvilke roller kan en identitet have og hvilke rettigheder er knyttet til en bestemt rolle?

Brugeridentiteter kommer fra UNI-Login, men det skal beskrives, om der sker yderligere rettighedstildelinger i læringsplatformen. Beskrivelsen skal være på et niveau, der beskriver, hvem der kan se hvad, hvem der kan ændre hvad, og hvem der kan slette hvad inden for de enkelte funktionsområder i læringsplatformen.

Krav #3	**Roller og rettigheder**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren skal beskrive, hvem der må hvad i læringsplatformen, og i besvarelsen skal der indsættes en oversigt over roller i læringsplatformen og rollens privilegier på funktionsniveau. Beskrivelsen kan være en tabel eller et diagram.		

Krav #4	**Adgangskontrol**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Adgangskontrol til læringsplatformen skal ske med UNI-Logins SAML-løsning		

Krav #5	**Brugeradministration**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren bedes beskrive, hvordan brugeradministration af brugerrettigheder foregår, og om der indgår en central eller decentral løsning til brugeradministration, eller om brugeradministrationen udelukkende sker via UNI-Logins roller.		

1.3.2 Dataflow

For at kunden kan foretage en samlet konsekvensanalyse, er det nødvendigt med en beskrivelse af dataflow i Læringsplatformen fra indsamling af data over behandling af data til sletning og destruktion.

Krav #6	**Dataflow**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren bedes beskrive Dataflow i læringsplatformen for eksempel som UML-diagram, user stories eller et andet for opgaven i relevant format, der giver overblik over behandlingen af data, der sker i systemet. Vedlægges i bilag.		

1.2 Reaktion ved sikkerhedsbrud

I Databeskyttelsesforordningen lægges op til, at den dataansvarlige ved sikkerhedsbrud uden unødvendig forsinkelse, og om muligt inden 72 timer efter bruddet, skal anmelde det til tilsynsmyndigheden.

Ved sikkerhedsbrud skal den registrerede, hvis data er blevet angrebet, underrettes uden unødig forsinkelse.

For at kunne dæmme op for sikkerhedsbrud, har kunden behov for at vide, hvordan, og i hvilken tidsramme sikkerhedsbrud rapporters.

Krav #7	**Sikkerhedsbrud**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Det er leverandørens ansvar at håndtere sikkerhedsbrud. Leverandøren bedes beskrive, hvordan systemet overvåges i forhold til sikkerhedsangreb og brud, og hvordan sikkerhedsbrud opdages og rapporteres.		

1.3 Placering af data

Persondataloven har krav om kontrol af at sikkerhedsforanstaltninger overholdes. For at kunne opfylde denne forpligtelse har kunden brug for at vide, hvor data fysik er placeret.

Krav #8	**Placering af data**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren bedes beskrive, hvor data fysisk er placeret inden for det Fælles Europæiske område, som beskrevet i Lov om behandling af personoplysninger §4		

1.4 Logning

Leverandøren skal foretage maskinel logning af alle anvendelser af personoplysninger.

I Sikkerhedsbekendtgørelsen (*BEK nr. 528 af 15/06/2000 - Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning*) §19 står:

Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Der lægges op til minimum tre typer af logs:

- Systemlogs
- Revisionsspor
- Verifikationslog

Krav #9	**Logninger opbevaring**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Systemlogs, revisionsspor og verifikationslog skal opbevares minimum 6 måneder, hvorefter de skal slettes.		

1.4.1 Systemlog

Krav #10	**Systemlog**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Der skal foretages systemlog i henhold til reglerne i sikkerhedsbekendtgørelsen. Som minimum skal følgende logges: Når data tilgås, så det kan dokumenteres: - Hvem der har tilgået data - Hvilke sammenhænge data er tilgået - Tidspunkt relateret til dataadgang - Aktør (bruger eller system), som har forsøgt at få adgang - Den person de anvendte oplysninger vedrørte		

Krav #11	**Systemlog – yderligere logning**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Hvis leverandøren logger flere handlinger i systemloggen end beskrevet ovenfor, bedes leverandøren beskrive disse.		

Krav #12	**Systemlog - beskyttelse**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Loggen skal beskyttes mod uautoriseret adgang, modifikation eller fabrikation.		

Krav #13	**Systemlog - beskyttelse**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren bedes beskrive, hvordan loggen beskyttes mod uautoriseret adgang, modifikation eller fabrikation		

1.5 Revisionsspor

Opsamling af, hvilke data er tilgået af hvilke brugere, der skal sikre mod uretmæssig adgang til personfølsomme data.

Krav #14	**Revisionsspor**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Der skal etableres revisionspor		

Krav #15	**Revisionsspor**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren bedes beskrive, hvilke data der logges til revisionsspor		

Krav #16	**Revisionsspor - beskyttelse**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren bedes beskrive, hvordan revisionsspor beskyttes mod uautoriseret adgang, modifikation eller fabrikation		

1.6 Revisionserklæring vedrørende sikkerhed

Dette afsnit beskriver krav i forhold til it-revision og auditaktiviteter, hvad enten der er tale om leverandørens interne auditaktiviteter eller kundens auditering af sikkerhedsforhold og forhold vedr. data og dokumentation.

Krav #17	**IT-revision og sikkerhedsaudits**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren skal leve op til lovgivningens krav vedrørende it-revision og sikkerhedsaudits.		

Krav #18	**Indledende IT-revision**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren skal inden overdragelse af læringsplatformen lade en ekstern statsautoriseret revisor, udpeget af Leverandøren, gennemføre it-revision af de generelle it-kontroller i relation til driften i overensstemmelse med Revisionsstandard ISAE 3000 eller tilsvarende med eventuelle nationale tilpasninger. Revisor skal udarbejde en IT-revisionserklæring efter både ISAE 3000 og ISAE 3402 type. Såfremt erklæringen påpeger alvorlige fejl eller mangler ved Leverandørens sikkerhedsydelser, skal disse udbedres, inden overtagelsen kan finde sted. Kunden kan udlevere erklæringen til de myndigheder, institutioner og virksomheder, som kunden distribuerer data på vegne af, til brug for disses kontrol af ISO/IEC 27001/2.		

Krav #19	**Løbende IT-revision**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	I hele kontraktperioden skal kunden én gang årligt modtage den ovenfor beskrevne erklæring vedrørende læringsplatformens sikkerhed, herunder driftssikkerhed. Kunden skal desuden på eget initiativ kunne modtage erklæringen. Kunden kan udlevere erklæringen til de myndigheder, institutioner og virksomheder, som kunden distribuerer data på vegne af, til brug for disses kontrol af ISO/IEC 27001.		

Krav #20	**Omkostninger til IT-revision**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Omkostninger afholdt til ovenstående årlige revisorerklæring, handlingsplaner, udbedringer og nye revisorerklæringer afholdes fuldt ud af Leverandøren. Yderlige IT-revision initieret af kunden, afholdes af kunden selv.		

2. Persondata

2.1 Sikringsforanstaltninger

Som beskrevet ovenfor i afsnittet om databehandleraftalen, skal Persondataloven (*Lov 429 af 31. maj 2000*) og Sikkerhedsbekendtgørelsen (*BEK nr. 528 af 15/06/2000 - Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning*) efterleves.

Krav #21	**Sikringsforanstaltninger**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren skal beskrive, hvilke sikringsforanstaltninger til sikring af fysiske personers persondata, der er anvendt i læringsplatformen.		

2.2 Forventede ændringer i anbefalinger til krav

Som led i arbejdet, og i lyset af blandt andet det generelt stigende fokus på digital sikkerhed i samfundet samt den kommende databeskyttelsesforordning, har det vist sig nødvendigt løbende at styrke sikkerheden i identifikation og autentifikation ved brug

af digitale løsninger. D. 13. maj 2016 blev en ny fællesoffentlig digitaliseringsstrategi aftalt, herunder et nyt initiativ om bedre sikkerhed i eID-løsninger for børn og unge. Det øgede fokus på digital sikkerhed har også betydning for brugerportalinitiativet, hvor der er behov for en nærmere afdækning af håndteringen af følsomme oplysninger.

Lovgivningen på området kan ændre sig, dels på baggrund af analyserne, men også af andre årsager, hvilket kan afstedkomme præceptive regler, der fremstilles i forordninger, bekendtgørelser og andre regulativer.

Krav #22	**Præceptive regler**		
Kategori:	Minimumskrav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren skal indestå for, at leverede leverancer og ydelser opfylder relevante præceptive regler, herunder love, bekendtgørelser og forordninger, således som disse foreligger ved kontraktens indgåelse, herunder f.eks., men ikke begrænset, til Databeskyttelsesforordningen, Persondataloven og Sikkerhedsbekendtgørelsen udstedt i medfør heraf. Det samme gælder for leverancer efter kontraktens indgåelse, idet leverandøren dog i så fald vil være berettiget til et rimeligt vederlag for udførelsen af opgaven, som udgangspunkt efter medgået tid eller efter en anden betalingsmodel, der aftales i forbindelse med opgavens udførelse, og hvor proceduren for gennemførelse af leverancen i alle tilfælde sker efter kontraktens bestemmelser om ændringshåndtering.		

2.2.1 Sikkerhedsanalyse

Som følge af, at den nye Databeskyttelsesforordning der blev vedtaget den 27. april 2016 til ikrafttrædelse maj 2018, er der, i foråret 2016 indledt en analyse under BPI-programmet for at vurdere sikkerhed for data i BPI-programmet. Analysen har fokus på de tekniske løsninger i BPI-programmet og relevante umiddelbart tilgrænsende systemer, men også for processer og arbejdsgange, når løsningerne anvendes og er i drift.

Arbejdet er et samarbejde mellem Styrelsen for IT og Læring, KOMBIT og KL.

Som en del af arbejdet, vil leverandører blive inviteret til at deltage i relevante dele af analysearbejdet.

Analysearbejdet vil ligge til grund for en udvidet sikkerhedsarkitektur, vejledninger og anbefalinger til krav i forhold til de eventuelle sikringsforanstaltninger, der vil blive udviklet som følge af analysens resultater.

Sikkerhedsarkitekturen og sikringsforanstaltningerne vil også omfatte læringsplatforme, da der i et vist omfang vil kunne forekomme følsomme oplysninger i læringsplatformene. Det er derfor forventningen, at der vil komme anbefalinger til skærpede krav til læringsplatformene fremadrettet. Dels som følge af arbejdet med sikkerhedsarkitekturen men også som følge af det stadigt ændrede trusselsbillede, der generelt er på IT.

På nuværende tidspunkt forventes anbefalinger til yderligere specificerede krav på følgende områder:

2.2.2 Opdatering af UNI-Login

Styrelsen for IT og Læring (STIL) har igangsat en plan for opdatering og udvidelse af UNI-Login. Dette arbejde kan betyde ændringer i anbefalinger til krav til læringsplatformene.

2.2.3 Rolle- og rettighedsstruktur

STIL, KL og KOMBIT har i sommeren 2016 igangsat et projekt om at etablere en mere detaljeret og uddybet fælles rolle- og rettighedsstruktur til BPI-programmet. Udfaldet af dette arbejde vil være en rolle- rettighedsstruktur, der har været efterspurgt af både kommuner og leverandører af BPI-programmets dele og vil betyde ændringer i anbefalinger til krav til læringsplatformene.

2.2.4 Sikring af forskellige sikringsniveauer

Der vil i forbindelse med arbejdet med sikkerhedsarkitekturen udkomme anbefalinger til krav om håndtering af forskellige typer af personoplysninger på forskellige sikringsniveauer i forhold til ISO 29115 i læringsplatformene.

2.2.5 2-faktorlogin til børn

Som en del af den fællesoffentlige digitaliseringsstrategi vil der blive igangsat en analyse af behov for en 2-faktor login til børn, og dette arbejde kan medføre ændringer i krav til loginkomponenter.

2.2.6 Publicering af ændringer i krav

Vejledninger til yderligere specificerede krav vil kunne udkomme fire gang om året, og kommunerne vil for eksempel kunne stille krav til leverandøren efterleve dem 12 måneder efter udgivelsen.

Vejledninger til præciserede krav vil blive udgivet på www.kl.dk/BPI/laeringsplatform/krav på følgende tidspunkter:

Dato	Forslag til efterlevelse
1-1-2017	1-1-2018
1-4-2017	1-4-2018
1-7-2018	1-7-2018

Krav #23	**Omkostningsmodel**		
Kategori:	Krav	Type:	Ikke- funktionelt
Beskrivelse:	Leverandøren bedes beskrive omkostningsmodel og vilkår for opfyldelse af skærpede krav, der udgives på www.kl.dk/BPI/laeringsplatform/krav fremadrettet, og hvor proceduren for gennemførelse af leverancen i alle tilfælde sker efter kontraktens bestemmelser om ændringshåndtering.		