Aulas dataetiske regelsæt for leverandører

Aula vil få over to mio. brugere, herunder både børn, lærere og forældre. Informationerne om Aula vil ofte være af personlig art, og derfor er det ekstra vigtigt, at Aulas brugere trygt kan bruge Aula i forvisning om, at deres data er i sikre hænder.

Aula har naturligvis en privatlivspolitik og en Data Protection Officer (DPO), der sikrer at Aula efterlever EU's datalovgivning. Men derudover har Aula også et dataetisk ansvar, og da Aula også vil være indgangen til en lang række såkaldte widgets fra andre leverandører rækker dette ansvar også videre end til Aula selv. Derfor har Aula et dataetisk regelsæt, som leverandører skal tilslutte sig for at få adgang til Aula.

Det dataetiske regelsæt fremgår af dette dokument, og leverandørens besvarelse af de enkelte punkter i regelsættet vil blive anvendt til vurdering i Aulas Governance Board, når widgetleverandører søger om adgang til Aulas "widget store". Aulas Governance Board vil på baggrund af leverandørens besvarelse tildele adgang til Aulas widgetstore, nægte adgang eller bede om uddybning af leverandørens besvarelse til brug for fornyet behandling.

[Indsæt leverandørnavn] og datadeling

[Leverandørnavn] sælger ikke under nogen omstændigheder personoplysninger fra [løsningsnavn] videre.

[Leverandørnavn] deler ikke personoplysninger med 3-part og tillader ikke 3-parts cookies, herunder cookies, fra sociale medier.

[løsningsnavn] kan godt henvise til eksterne hjemmesider, der anvender cookies.

Brugerne af [løsningsnavn] kan selv vælge at eksportere personoplysninger og dele disse med andre.

Personhenførbare personoplysninger må ikke anvendes af widgetleverandør til at skabe yderligere forretning, end det der er aftalt med den pågældende kommune, skole eller daginstitution.

[Leverandørnavn] har en formuleret privatlivspolitik for [løsningsnavn].

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og datalagring

[Løsningsnavn]s personoplysninger lagres i fuld overensstemmelse med EU's datalovgivning. Alle personoplysninger er krypterede og slettes, når formålet med brugen er afsluttet. Det vil i praksis sige senest når barnet forlader skolen, eller hvis der er givet samtykke til andet.

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og dataadgang

Udover brugerne selv har kun sikkerhedsgodkendte systemadministratorer med tavshedspligt adgang til personoplysninger i [løsningsnavn], hvis dette er nødvendigt.

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og samtykke

[Løsningsnavn]s arkitektur har indbygget håndtering af samtykke, så ingen brugere afgiver personoplysninger uden først at blive spurgt.

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og databrug

[Løsningsnavn] indsamler kun de personoplysninger, der er absolut nødvendige, (jf. privatlivspolitikken) og efter gældende lovgivning.

[Løsningsnavn] bruger anonymiserede personoplysninger om brugeradfærd til fx at forbedre [Løsningsnavn]s funktionalitet.

[Løsningsnavn] foretager ikke profilering af børn eller andre brugere.

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og genanvendelse af data

[Løsningsnavn]s personoplysninger vil ikke kunne anvendes af andre end brugerne af [løsningsnavn] (dataejere).

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og algoritmer

[Leverandørnavn] anvender som udgangspunkt ikke kunstig intelligens i [løsningsnavn]. Såfremt kunstig intelligens tages i brug, skal dette forklares med udgangspunkt i at det sker til gavn for brugerne.

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og kommunikation

Kommunikation mellem mellem brugergrupperne i [løsningsnavn] er fortrolig

[Leverandørnavn]s kommentarer:

[Leverandørnavn] og overholdelse af dataetiske regelsæt

[Leverandørnavn] bedes beskrive, hvorledes vedlagte dataetiske regelsæt overholdes.

[Leverandørnavn]s kommentarer: