4. Oktober 2019

KOMBIT
Kommunernes it-fællesskab

TILTAG I KOMMUNERNE TIL AT REDUCERE RISICI VED HÅNDTERING AF PERSONOPLYSINGER I AULA

Baggrund

KOMBIT har gennemført en risikovurdering af behandling af personoplysninger i Aula og dermed mulige konsekvenser for de registrerede (børn og forældre). Risikovurderingen er foretaget for de enkelte moduler i Aula (bl.a. besked, søgning, profil) og er sket med udgangspunkt i, at Databeskyttelses-forordningen og dermed Databeskyttelsesloven kræver, at en behandling af personoplysninger skal have et passende sikkerhedsniveau. Nogle risici er relateret til tekniske forhold vedrørende den fælles it-løsning til Aula og it-driftsafviklingen. Andre risici har sammenhæng med måden, som brugerne anvender Aula på, og kommunens setup i forhold til administration af brugere og rettigheder, samt kommunens it-infrastruktur til fx netværk og komme/gå-terminaler.

På baggrund af risikovurderingen har KOMBIT identificeret tiltag som KOMBIT forventer, at den enkelte kommune og/eller institution iværksætter for at reducere risikoen yderligere. Disse tiltag er beskrevet nærmer nedenfor.

Såfremt du er interesseret i at få de specifikke risikovurderinger for Aula tilsendt er du velkommen til at kontakte Aula projektet i KOMBIT. Risikovurderingerne kan bl.a. anvendes til kommunens eget arbejde med it-risikovurdering på skole- og børneområdet.

Organisatoriske tiltag målrettet brugerne af Aula

Disse tiltag kan sammenfattes til, at brugerne af Aula skal være i stand til at:

1. Undgå utilsigtet videregivelse af personoplysninger ved anvendelse af Aula
2. Korrekt at kunne klassificere almindelige og følsomme personoplysninger i beskeder og sikker fildeling i Aula
3. Korrekt at klassificere medier, så fx billeder eller videoer med genkendelige personer bliver opmærket i forhold til deling af medier
4. Bruge komme/gå-tavlen på en måde, som sikrer mod hændelige eller utilsigtede ændringer.

Kommuner, skoler og dagtilbud skal sørge for, at brugerne af Aula er uddannet i at ***undgå utilsigtet videregivelse af personoplysninger*** som de har adgang til i Aula. Det gælder, når de anvender Aula i forbindelse med

- Beskeder
- Sikker fildeling

- Medier (fx billeder) i galleriet
- Kalender
- Opslag
- Profiloplysning om brugerne, fx supplerende stamdata

Kommunerne skal have særligt fokus på betydningen og dermed konsekvenserne af, at utilsigtet videregivelse af personoplysninger kan blive forstærket afhængig af hvilken brugertype, der har adgang til personoplysninger i Aula. Fx vil en administrativ medarbejder med adgang til at søge data for alle kommunens skoler have adgang til flere data end pædagogisk personale på en enkelt institution, der kun har adgang til data om de grupper/klasser, som personalet til dagligt arbejder med.

Et andet eksempel vedrører at oprette dokumenter direkte i Sikker fildeling som "internt" dokument i Aula, fremfor at importere et eksisterende dokument. Hermed sikres det, at dokumentet ikke kan downloades og dermed minimeres risikoen for utilsigtet videregivelse.

Kommuner, skoler og dagtilbud skal sørge for, alle brugere er vejledt om, uddannet og/eller instrueret i dels, hvordan de håndterer og korrekt klassificerer almindelige og følsomme personoplysninger i Aula ved brug af **besked og sikker fildeling** (kun medarbejdere), og at de ikke må have følsomme personoplysninger i kalender og opslag.

I forhold **håndtering af medier i galleri** skal alle kommuner, skoler og dagtilbud sørge for, at alle brugere er vejledt om, uddannet og/eller instrueret i, hvordan de håndterer og *korrekt klassificerer medier*, så medier med genkendelige personer bliver opmærket. I den forbindelse skal der være en opmærksomhed på at vejlede børn og forældre om korrekt håndtering af medier.

I relation til **komme/gå-modulet** i Aula har kommunen som dataansvarlig en opgave med at *vejlede forældre og medarbejdere i brug af komme/gå-tavlen* for at forhindre hændelige eller utilsigtede ændringer, samt at instruere medarbejderne i, hvordan uvedkommende adgang til komme/gå-tavlen i institutionen undgås. Forældrene vælger selv om der ønskes et billede af barnet og om der skal benyttes et alias for barnets navn (kan tilvælges ifm. navne- og adressebeskyttelse af barnet). Kommunen skal som dataansvarlig *vejlede den registrerede og forældre om mulighederne*.

Organisatoriske og tekniske tiltag målrettet kommunen og dem, der administrerer brugere og Aula

Disse tiltag kan sammenfattes til, at kommunerne skal være i stand til:

1. Løbende at vedligeholde bruger- eller systemadgange til Aula

2. Løbende at praktisere brugeradministration i forhold til Aula med afsæt i en klar adgangspolitik
3. At håndtere brugerdata i de systemer, der forvalter oplysninger om brugere i Aula
4. At sikre sig tilstrækkelig overvågning og dokumentation af, at det ikke sker hackerangreb på de systemer, der forvalter oplysninger om brugere i Aula
5. At sikre sig mod udnyttelse af åben port eller service, eller åben systemkonfiguration i kommunens tekniske infrastruktur.

Kommunerne skal have et særligt fokus på *løbende at vedligeholde bruger- eller systemadgang*e, med særlig fokus på, når der sker ændringer som følge af ændret ansættelsesforhold og ændrede integrationer til Aula.

Alle kommuner, skoler og dagtilbud skal have en *klar adgangspolitik og praksis for løbende brugeradministration* for Aula, der minimerer forkerte bruger- eller systemadgange til personoplysninger i Aula. Kommunerne skal have særligt fokus på, at betydningen eller konsekvenserne ved denne risici kan blive forstærket afhængig af hvilke brugertypen, der har adgang til personoplysninger i Aula. Fx vil en administrativ medarbejder med adgang til at søge data for alle kommunens skoler have adgang til flere data end pædagogisk personale på en enkelt institution, der kun har adgang til data om de grupper/klasser, som personalet til dagligt arbejder med.

Kommunen er ansvarlig for processer, der håndterer brugerdata i de systemer[1], der *forvalter oplysninger om brugere i Aula*. I den forbindelse skal kommunen sikre sig *tilstrækkelig overvågning og dokumentation* af, at der ikke sker hackerangreb på disse systemer, der kan kompromittere brugerdata.

I forhold til kommunens tekniske infrastruktur (netværk og klientenheder) skal kommunen *sikre sig mod udnyttelse af åben port eller service, eller åben systemkonfiguration* (fx standardpasswords), som ikke er blevet deaktiveret gennem hærdning.

[1] Omfatter bl.a. brugeradministrative systemer fra KMD og Tabulex, Uni-Login hos STIL og kommunens IDP-systemer.