Databehandleraftale
mellem

(herefter Kommunen)
&
Mobilize Me
(herefter databehandleren)

Det er jf. licenskøb på skoler aftalt, at Mobilize Me skal udføre følgende opgave for Kommunen:

- Give adgang til anvendelse af servicerne Mobilize Me, PlaNet eller LiMo.

Indledning
På denne baggrund indgås denne databehandleraftale mellem Kommunen som dataansvarlig og med Mobilize Me (herefter databehandleren) som databehandler for Kommunen, idet der jf. Persondatalovens § 42, stk. 2, skal indgås en skriftlig aftale, når Kommunen overlader en behandling af personoplysninger til en databehandler.

Der gøres opmærksom på, at når Databeskyttelsesforordningen træder i kraft den 25. maj 2018, skal der indgås en ny databehandleraftale, som lever op til den nye lovgivning, jf. afsnit 2. Databeskyttelseslovgivning.

Der aftales herved følgende:

1. Efter instruks
Databehandleren handler alene efter instruks fra Kommunen i forbindelse med udførelse af de aftalte opgaver.

Oplysninger må ikke videregives til tredjepart eller behandles til andre formål, medmindre dette sker efter aftale med Kommunen.

2. Databeskyttelseslovgivning
Databehandleren overholder den til enhver tid gældende persondatalovgivning og herunder sikkerhedsbekendtgørelse nr. 528 af 15. juni 2000 og de sikkerhedsregler, der følger af sikkerhedsbekendtgørelsen.

2.1
Databehandleren sikrer herunder, at der er truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven eller Kommunens IT-sikkerhedspolitik[1] (som vedlægges som Bilag A) og herunder de basale retningslinier i den offentlige standard for informationssikkerhed DS 484:2005.

2.2
Databehandleren skal levere en oversigt over datacentre og backup centre med præcis adresse angivelse af, hvor Kommunens data behandles. Der sendes en ny oversigt til Kommunen ved ændringer. Der kan ikke uden forudgående aftale med Kommunen placeres data i et andet land.

[1] Bilag A – Kommunens IT-sikkerhedspolitik

2.3
Databehandleren er forpligtet til straks at give Kommunen (den kontraktansvarlige) meddelelse om driftsforstyrrelser, mistanke om brud på IT-sikkerhedsreglerne eller andre væsentlige uregelmæssigheder i forbindelse med udførelsen af opgaven.

3 Adgang til data
Ved adgang til sikrede lokaler i Kommunen, kan den enkelte kommunale afdeling udlevere et adgangskort med en personlig kode eller en nøgle mod kvittering.

Databehandleren har det ledelsesmæssige ansvar for, at databehandlerens medarbejdere overholder kommunens IT-sikkerhedsregler.

3.1
Databehandlerens medarbejdere må alene have adgang til data og/eller udføre jobs i det omfang, det er nødvendigt for udførelsen af arbejdet. Data må ikke lagres lokalt på medarbejderens udstyr.

Databehandleren garanterer, at nødvendig kopiering og backup af data sker under fuldt betryggende forhold.

Efter endt brug skal udleveret datamateriale enten returneres tilstrækkeligt sikkert til Kommunen eller destrueres forsvarligt, så det ikke er muligt at genskabe dem. Eventuel destruktion skal aftales nærmere med den dataansvarlige i Kommunen.

3.2
Databehandlerens medarbejdere, som har behov for adgang til Kommunens netværk skal forsynes med digital virksomhedssignatur (medarbejder NemID) af databehandleren. Medarbejderne skal være tilknyttet et sikkerhedsområde i Kommunens IT-sikkerhedsorganisation.

Medarbejdere tildeles en brugerident samt en personlig og fortrolig adgangskode i h.t. gældende standarder i Kommunen. Bestilling af ny kode - ved glemt kode - skal så vidt muligt ske via Kommunens IT-sikkerhedsorganisation.

4 Tavshedspligt
Databehandleren forpligter sig overfor uvedkommende til at hemmeligholde alle oplysninger modtaget fra og om Kommunen, som databehandleren får kendskab til i forbindelse med udførelsen af arbejdet for Kommunen.

4.1
Databehandleren sikrer, at deres medarbejdere, der får adgang til oplysninger fra Kommunen har underskrevet en tavshedserklæring om, at de har tavshedspligt over for uvedkommende med hensyn til deres adgang til kunders/samarbejdspartneres data. Tavshedspligten er gældende såvel under ansættelsen som efter ansættelsens ophør.

Databehandler skal levere en kopi af disse erklæringer efter anmodning fra Kommunen.

4.2
Ved indgåelse af aftalen vedlægges et bilag B med en oversigt over de tilknyttede medarbejdere[2], der skal have adgang til Kommunens lokaliteter/netværk. Leverandøren er forpligtet til at løbende at

[2] Bilag B – Oversigt over tilknyttede medarbejdere

tilmelde nye medarbejdere og afmelde medarbejdere, der ikke længere har behov for adgang, til kontraktholder hos Kommunen.

5. Underdatabehandlere (underleverandører)
Hvis databehandleren anvender underdatabehandlere er det databehandlerens ansvar, at underdatabehandleren efterlever databehandleraftalen, idet aftalen også gælder for disse.
Databehandleren skal informere Kommunen om evt. underdatabehandlere samt sikre, at også deres underdatabehandleres medarbejdere har underskrevet en tavshedserklæring.
Efter anmodning fra Kommunen skal databehandler levere en kopi af underdatabehandleraftalen.

6 Tilsyn
Kommunen fører tilsyn med, at databehandleren har truffet de fornødne sikkerhedsforanstaltninger. Dette kan ske ved et besøg hos databehandleren og/eller hos evt. underdatabehandlere. Kommunen kan også lade andre (f.eks. revisor) gennemføre tilsyn.

Kommunen er til enhver tid berettiget til at gennemføre yderligere kontrolforanstaltninger, herunder at begrænse databehandlers adgangsmuligheder til Kommunens netværk og data.

Databehandleren skal på Kommunens anmodning, give Kommunen tilstrækkelige oplysninger til, at denne kan påse, at de krævede tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

6.1
Hvis det fremgår af kontrakten, skal der ved underskrift af databehandleraftalen leveres den seneste revisorerklæring, og herunder evt. baggrundsmateriale til erklæringen. Herefter leveres en årlig revisorerklæring, der er udarbejdet i overensstemmelse med de gældende branchestandarder på området (f.eks. ISAE 3000 vedrørende overholdelse af persondataloven). Dette gælder også for evt. underdatabehandlere.

7. Øvrige forhold
Hvis Kommunen oplyser, at der foretages videoovervågning i de lokaliteter, hvor databehandlerens medarbejdere færdes hos Kommunen, skal databehandleren sikre, at deres medarbejdere samt underdatabehandleres medarbejdere gøres bekendt med dette.

Databehandleren skal endvidere informere de pågældende medarbejdere om, at der sker registrering (logning) af alle anvendelser af fortrolige personoplysninger samt registrering af afviste adgangsforsøg i kommunens IT-systemer. De pågældende medarbejdere skal herunder gøres bekendt med, at der foretages kontrol med alle anvendelser af systemer med fortrolige personoplysninger. Loggen gemmes i 6 måneder, hvorefter den slettes.

8. Overtrædelse af databehandleraftalen
Parternes erstatningspligt efter dansk rets almindelige regler skal være reguleret i kontrakten.

9. Databehandleraftalens ophør
Aftalen kan genforhandles, hvis der sker ændring af det i punkt 2 anførte juridiske grundlag for aftalen.

9.1
Databehandleraftalen træder ud af funktion, når det samarbejde, der er en forudsætning for aftalen, ikke længere er gældende.

9.2

Tavshedspligten for databehandleren/underdatabehandlere og deres medarbejdere ophører ikke, selv om databehandleraftalen træder ud af kraft.

9.3.
Databehandleren må kun behandle personoplysninger, som Kommunen er ansvarlig for, så længe det er nødvendigt for udførelse af den aftalte opgave.

9.4.
Ved ophør skal det aftales med Kommunen, at data skal leveres tilbage til Kommunen eller der skal ske uoprettelig sletning punkt 3.1.

For Mobilize Me	Kommunen,
Dato: / - 201_	Dato: / - 201_
_____	_____
(Underskrift)	(Underskrift)

Bilagsoversigt:
Bilag A – Kommunens IT-sikkerhedspolitik
Bilag B – Krav til databehandlere
Bilag C – Kvitteringsbilag
Bilag D – Oversigt over tilknyttede medarbejdere