DATABEHANDLERAFTALE

Mellem

CVR nummer:
(herefter "institutionen")

Og

MOBILIZE ME ApS
Åbogade 15
8200 Aarhus N
CVR. nr.: 34208077
(herefter "Leverandøren")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om Leverandørens behandling af personoplysninger på vegne af Institutionen:

1. Generelt

1.1 Omfang

Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav som fremgår af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen)

1.2 Krav

I Aftalen er indarbejdet de krav, som regler i Databeskyttelsesforordningen stiller til databehandleraftaler.

1.3 Principper

Principperne og anbefalingerne i ISO27001 med senere ændringer vil på alle relevante områder finde anvendelse, i det omfang andet ikke fremgår af denne aftale.

1.4 Forventning til leverandør

Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Institutionen.

Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Databeskyttelsesforordningen.

Leverandøren skal på opfordring fra Institutionen hjælpe med at opfylde Institutionens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Institutionens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, i medfør af Databeskyttelsesforordningen. Leverandøren skal hjælpe Institutionen med at efterleve dennes forpligtelser efter Databeskyttelsesforordningen.

Leverandøren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Institutionens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Institutionens personoplysninger opbevares. Leverandøren skal ajourføre oplysningerne over for Institutionen ved enhver ændring.

Leverandøren kan bede om godtgørelse af forbrugt tid og fakturere ud fra leverandørens aktuelle prisliste for aktuelle ydelser og konsulenttimer angivet/offentliggjort på leverandørens hjemmeside.

1.5 Formål

Formålet med aftalen er at understøtte brugen af leverandørens digitale værktøjer, men uden at leverandøren får betaling herfor. Derfor tager institutionen i stor udstrækning ansvar for forvaltning af data, og kan kun pålægge leverandøren at føre revision, tilsyn og følge institutionens processer/strategi ved nærmere aftale om leverance herfor.

Leverandøren vil bistå i rådgivning af best practices i forvaltning af data, og dermed være behjælpelig i at sikre Institutionen kommer til at overholde dataforordningens krav til behandling af data.

1.6 Begrænsning ift. hovedaftale

Leverandøren behandler i medfør af aftale med Institutionen personoplysninger for Institutionen, hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

1.7 Institutionens ansvar

Institutionen er dataansvarlig for de personoplysninger, som Institutionen instruerer Leverandøren om at behandle. Institutionen har ansvaret for, at de personoplysninger, som Institutionen instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Institutionens opgavevaretagelse.

Institutionen er forpligtet til at orientere Leverandøren i tilfælde af Institutionens eventuelle skærpede it-sikkerhedsregler og ved ændringer i Institutionens it-sikkerhedspolitik og it-sikkerhedsregulativ. Leverandøren kan ved skærpede eller ændrede it-sikkerhedsregler og politik omgående vælge at annullere aftalen ved skriftlig henvendelse eller afsendelse af e-mail til institutionen herom.

Leverandøren behandler alene de overladte personoplysninger efter instruks fra Institutionen og alene med henblik på opfyldelse af Hovedaftalen.

2. Underleverandør (underdatabehandler)

2.1 Definition

Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Institutionen.

2.2 ændring

Leverandøren må ikke uden udtrykkelig skriftlig godkendelse fra Institutionen anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Institutionen har overladt til Leverandøren i medfør af Hovedaftalen. Institutionen kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor.

2.3 Databehandling

Hvis Leverandøren overlader behandlingen af personoplysninger, som Institutionen er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underleverandøren.

2.4 Underdatabehandleraftaler

Underdatabehandleraftalen, skal pålægge underleverandøren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underleverandøren garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger

således, at underleverandørens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

Institutionen kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Institutionen.

Al kommunikation mellem Institutionen og underleverandøren sker via Leverandøren.

3. Instrukser

3.1 ansvar

Leverandørens behandling af personoplysninger på vegne af Institutionen sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er Leverandørens ansvar at sikre, at eventuelle underdatabehandlere, får tilsendt Institutionens instruks, jf. bilag 3.

Leverandøren giver omgående besked til Institutionen, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen.

4. Tekniske og organisatoriske sikkerhedsforanstaltninger

4.1 foranstaltninger

Leverandøren skal, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

Leverandøren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 7 samt bilag 1.

4.2 Ansatte

Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Institutionens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 6.

Leverandøren er forpligtet til straks at underrette Institutionen om ethvert sikkerhedsbrud, samt ved

(i)

Enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed, medmindre orienteringen af Institutionen er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,

(ii)

Anden manglende overholdelse af Leverandørens, samt eventuelle underdatabehandleres forpligtelser] uanset, om dette sker hos Leverandøren eller hos en underdatabehandler. Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, uden forudgående skriftlig aftale med Institutionen om indholdet af en sådan kommunikation, medmindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

5. Overførsler til andre lande

5.1 Overførsel til et ikke EU medlemsland

Leverandørens må og kan kun gennemføre overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloud løsning eller en underdatabehandler, når der foreligger en instruks fra institutionen herfor, jf. bilag 3.

Ved overførsel til tredjelande er alene Institutionen ansvarlig for, at der foreligger et gyldigt overførsels grundlag.

6. Tavshedspligt og fortrolighed

6.1 varighed

Leverandøren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet.

6.2 underdatabehandlere og tredjeparter

Leverandøren skal sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

7. Kontroller og erklæringer

7.1 Institutionens forpligtelser ift. kontroller og erklæringer

Institutionen, en repræsentant for Institutionen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, eksempelvis få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne aftale.

Institutionen kan til enhver tid bede leverandøren om udarbejdelse og fremsendelse af erklæring om overholdelse af denne aftale. Omfanget af disse erklæring rammesættes af institutionen, som leverandøren skal prioritere at gennemføre, producere og fremsende uden forsinkelse.

Leverandøren er forpligtet til uden ugrundet ophold at behandle institutionens henvendelser og bistå Institutionen med alle nødvendige oplysninger til, at Institutionen til enhver tid kan sikre sig, at Leverandøren overholder de krav, der følger af denne aftale.

Leverandøren kan bede om godtgørelse af forbrugt tid ved bistående af disse kontroller og udarbejdelse af erklæringer, og fakturere ud fra leverandørens aktuelle prisliste for konsulenttimer angivet/offentliggjort på leverandørens hjemmeside.

7.2 Datatilsyn

I tilfælde af, at Institutionen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Leverandøren og Leverandørens underleverandører sig til uden yderligere omkostninger for Institutionen at stille tid og ressourcer til rådighed herfor.

8. Ændringer i Aftalen

8.1 Varsel

Institutionen kan til enhver tid, med et forudgående varsel på mindst 30 dage, foretage ændringer i Aftalen og instruksen, jf. bilag 3. Ændringsprocessen og omkostningerne aftales skriftligt mellem institutionen og Leverandøren i Hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.

9. Sletning af data

9.1 Institutionens beslutning

Institutionen træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.

9.2 Behandling

Institutionen skal senest 30 dage inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Institutionen. I det tilfælde, hvor personoplysningerne tilbageleveres til Institutionen, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Institutionens meddelelse.

10. Misligholdelse og tvistigheder

10.1 Misligholdelse og tvistigheder er reguleret i Hovedaftalen.

11. Erstatning og forsikring

11.1 Hovedaftalen

I tilfælde af, at Hovedaftalen ikke tager stilling hertil, skal dansk rets almindelige regler finde anvendelse i forhold til erstatnings- og forsikringsspørgsmål.

12. Ikrafttræden og varighed

12.1 Varighed

Aftalen indgås ved begge parters underskrift og løber indtil ophør af Hovedaftalen.

13. Formkrav

Aftalen skal foreligge skriftligt, herunder elektronisk, hos Institutionen og Leverandøren

Dato:	Dato:
For Institutionen	For Leverandøren
_____	_____

Bilag 1 – Sikkerhed

1. Leverandørens ansvar

Leverandøren må alene handle efter denne instruks fra den dataansvarlige og kun vedrørende de opgaver,
leverandøren har i henhold til databehandleraftalen og hovedaftalen.

2. Tekniske og organisatoriske sikkerhedsforanstaltninger

Leverandøren skal som minimum træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysninger på vegne af den dataansvarlige.

Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger er nødvendige for at sikre efterlevelse af databehandleraftalens afsnit, skal sådanne mere omfattende foranstaltninger altid træffes i samråd med institutionen.

2.1 Kontaktpunkt

Leverandøren kan indenfor normal arbejdstid kontaktes på følgende kontaktoplysninger:

- tlf: 70707437
- e-mail: support@mobilize-me.com

2.2 Risici for sikkerhed

Leverandøren skal hjælpe institutionen med at træffe de nødvendige skridt til at identificere, vurdere og begrænse enhver, med rimelighed forudsigelig, intern og ekstern risiko for tilgængeligheden, fortroligheden, og/eller integriteten af alle personoplysninger omfattet af databehandleraftalen.

Institutionen kan forvente at leverandøren har passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang, og at der eksisterer en løbende proces for at evaluere og forbedre effektiviteten af sådanne forholdsregler.

Leverandøren skal have formelle processer for håndtering af sikkerhedshændelser.

Leverandøren skal ved hændelser, hvor person oplysningers fortrolighed, integritet eller tilgængelighed kan være eller have været negativt påvirket, underrette institutionen uden ugrundet ophold.

2.3 Autorisation og adgangskontrol

Leverandøren skal især iagttage følgende vedrørende autorisation og adgangskontrol:

1. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.
2. Leverandøren skal sikre, at der foretages et efter omstændighederne passende baggrundstjek for alt personale, der i forbindelse med deres ansættelse vil have adgang til personoplysninger omfattet af databehandleraftalen, uanset i hvilket format personoplysninger måtte være tilgængelige.
3. Kun de personer, som autoriseres dertil, må have adgang til personoplysninger, der behandles.
4. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.
5. Der må endvidere autoriseres personer, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.
6. Den autoriserede bruger udstyres med en personligt brugeridentifikation og et password, der skal anvendes hver gang, der logges på systemet. Leverandøren skal være sikre at leverandørens medarbejdere modtager tilstrækkelig uddannelse og instruktioner, inklusiv – men ikke begrænset til – uddannelse der tilsigter mod at øge medarbejdernes generelle sikkerhedsbevidsthed, introduktion af relevante sikkerhedspolitikker og procedurer, samt adgang til og uddannelse i dokumenterede processer og arbejdsbeskrivelser særligt vedrørende behandling af personoplysninger. Uddannelse og instruktioner skal omfatte de emner, der er relevante for at sikre, at personoplysninger behandles i overensstemmelse med såvel lovgivningen som leverandørens og den dataansvarliges relevante politikker og procedurer.
7. Autorisation gives til den dataansvarliges systemer af den dataansvarlige efter den dataansvarliges indstilling.
8. Der skal træffes foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, og at brugeren kun kan få adgang til de personoplysninger og anvendelser (behandlinger), som den pågældende er autoriseret til.
9. Leverandøren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

2.4 Kontrol

Leverandøren skal iagttage følgende vedrørende kontrol med afviste adgangsforsøg og logning:

1. Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger omfattet af lov om behandling af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium. Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode, dog højest 5 år, af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

2. Sikkerhedskopier
   Leverandøren skal sikre, at systemer og personoplysninger sikkerhedskopieres regelmæssigt. Sikkerhedskopierne skal opbevares betryggende, og således at sikkerhedskopier ikke fortabes ved hændelser, der medfører tab af originale personoplysninger eller uautoriseret adgang til oplysningerne. Leverandøren skal regelmæssigt kontrollere, at sikkerhedskopier er læsbare.

3. Opdateringer og ændringer
   Leverandøren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid. Leverandøren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.

4. Beskyttelse mod ondsindet software
   Leverandøren skal have formelle procedurer til sikring af udstyr er beskyttet mod ondsindet koder og programmer. Med dette menes at man har en antivirus løsning som er opdateret og periodisk scanner udstyr for virus samt at der udføres "patchning" af programmer og operativsystemer i henhold til "best practice".

5. Transmission af data
   Leverandøren skal sikre at persondata ikke sendes ubeskyttet over det åbne net. Data skal således sendes i krypteret form når det sendes via internettet.

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen

- Arosii a/s, Åbrogade 15, 8200 Aarhus N.
- Cloud.dk, Højvangen 4, 8660 Skanderborg

2. Underdatabehandlere

- Arosii a/s, Åbrogade 15, 8200 Aarhus N. Cvr. 34352569
- Cloud.dk, Højvangen 4, 8660 Skanderborg. Cvr. 29139555

Bilag 3 – Instruks

Institutionen instruerer hermed Leverandøren om at foretage behandling af Institutionens oplysninger til brug af leverandørens serviceydelser Mobilize Me, PlaNet og LIMO.

Leverandøren er ansvarlig for, at Institutionens instruks fremsendes til eventuelle underdatabehandlere.

1.1 Behandlingens formål

Behandling af Institutionens oplysninger sker i henhold til formålet i Hovedaftalen.
Leverandøren må ikke anvende oplysningerne til andre formål.
Oplysningerne må ikke behandles efter instruks fra andre end Institutionen.

1.2 Generel beskrivelse af behandlingen

Mobilize Me vil levere serviceydelser til at hjælpe brugere til en mere selvstændig og selvhjulpen hverdag. Mobilize Me vil yde drift af disse, samt rådgivning, support og hosting.

1.3 Typen af personoplysninger

Behandlingerne indeholder almindelige personoplysninger

1.4 Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede f.eks. borgere, elever, udsatte borgere.

1.5 Tredjelande (ikke EU-medlemslande)

Leverandøren må ikke overføre personoplysninger til følgende tredjelande