

SKABELON FOR DATABEHANDLERAFTALER

MELLEM

[KUNDE]

OG

SUBIT APS

af [Indsæt dato]

DATABEHANDLERAFTALE

Mellem

[XXXX] Kunde

[adresse]

[postnr. og by]

CVR. nr.: [XXXX]

(herefter "Kunden")

og

Subit ApS

Dronning Olgas Vej 26 B

2000 Frederiksberg

CVR-nr. 39216736

(herefter "Leverandøren")

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

1. Generelt

- 1.1 Databehandleraftalen 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 I Databehandleraftalen er indarbejdet de krav, som Databeskyttelsesforordningen stiller til databehandleraftaler.

2. Formål

- 2.1 Leverandøren behandler, i medfør af aftale med Kunden om køb og drift af Subit's online vikarløsning (herefter "Hovedaftalen"), personoplysninger for Kunden, hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

3. Kundens rettigheder og forpligtelser

- 3.1 Kunden er dataansvarlig for de personoplysninger, som Kunden instruerer Leverandøren om at behandle. Kunden har ansvaret for, at de personoplysninger, som Kunden instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Kundens opgavevaretagelse.
- 3.2 Kunden har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Databehandleraftalens pkt. 1.1.
- 3.3 Der kan i Databehandleraftalens bilag 1 være opremset yderligere forpligtelser, som Kunden skal være opmærksom på.

4. Leverandørens forpligtelser

- 4.1 Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Kunden, jf. pkt. 6 og bilag 1. Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Databehandleraftalens pkt. 1.1.
- 4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Kunden, jf. pkt. 6 og bilag 1, og alene med henblik på opfyldelse af Hovedaftalen. Leverandøren kan behandle personoplysninger udenfor Kundens Instruks, i tilfælde hvor det kræves af EU-retten eller national ret, som Leverandøren er underlagt. Ved behandling af personoplysninger udenfor den fastsatte Instruks skal Leverandøren underrette Kunden om årsagen hertil. Underretningen skal ske, inden behandlingen foretages, og skal indeholde en

henvisning til de retlige krav, der ligger til grund for behandlingen. Underretning skal dog ikke ske, hvis underretning vil være i strid med EU-retten eller den nationale ret.

- 4.3** Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Databeskyttelsesforordningen, jf. bilag 1.
- 4.4** Leverandøren skal i overensstemmelse med Databeskyttelsesforordningen på opfordring fra Kunden bistå med at opfylde Kundens 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 Kundens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud i medfør af Databeskyttelsesforordningens kap. III samt artikel 34. Medmindre andet fremgår af Hovedaftalen er Leverandørens bistand særskilt betalbar.
- 4.5** Leverandøren skal i overensstemmelse med Databeskyttelsesforordningen bistå Kunden med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36. Medmindre andet fremgår af Hovedaftalen, er Leverandørens bistand særskilt betalbar.
- 4.6** Leverandøren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Kundens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 4.7** Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

5. Underleverandør (underdatabehandler)

- 5.1** Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Kunden.
- 5.2** Leverandøren må ikke uden udtrykkelig skriftlig godkendelse fra Kunden anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger,

som Kunden har overladt til Leverandøren i medfør af Hovedaftalen. Kunden kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor. En sådan indsigelse og begrundelse skal foreligge seneste 30 dage efter modtagelse af Leverandørens anmodning.

- 5.3** Hvis Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
- 5.4** Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Databehandleraftalen, herunder, at underdatabehandleren garanterer, at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 5.5** Når Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kunden ansvaret for underdatabehandlerens overholdelse af disses forpligtelser, jf. pkt. 5.3.
- 5.6** Kunden 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 Kunden.

6. Instrukser

- 6.1** Leverandørens behandling af personoplysninger på vegne af Kunden sker udelukkende efter dokumenteret instruks, jf. bilag 1.
- 6.2** Leverandøren giver omgående besked til Kunden, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.1.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

- 7.1** Leverandøren skal jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:
 - (i) tilintetgøres, mistes, ændres eller forringes,

- (ii) kommer til uvedkommendes kendskab eller misbruges, eller
- (iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1

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

7.3 Leverandøren er forpligtet til straks at underrette Kunden om ethvert sikkerhedsbrud uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

8. Overførsler til andre lande

8.1 Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU/EØS (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Kundens instruks herfor, jf. bilag 1.

8.2 Hvis Kundens personoplysninger overføres til en EU-medlemsstat, er det Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

9. Tavshedspligt og fortrolighed

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

10. Kontroller og erklæringer

10.1 Leverandøren er forpligtet til uden ugrundet ophold at give Kunden nødvendige oplysninger til, at Kunden til enhver tid kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale. Leverandørens forpligtelse i henhold til dette punkt 10.1 er vederlagsfri i det omfang det følger af Hovedaftalens eller Databehandleraftalens bestemmelser, at disse oplysninger leveres uden yderligere vederlag.

10.2 Kunden, en repræsentant for Kunden eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision i rimeligt omfang hos Leverandøren, med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale. Leverandørens forpligtelse i henhold til dette punkt 10.2 er vederlagsfri, i det omfang det følger af Hovedaftalens eller

Databehandleraftalens bestemmelser, at Leverandøren medvirker uden yderligere vederlag i forbindelse med inspektion og revision.

- 10.3** Medmindre andet fremgår af Hovedaftalen, eller parterne særskilt aftaler udarbejdelse af anden revisorerklæring, skal Leverandøren alene udarbejde og fremsende revisionserklæringer som anført i bilag 1. Udarbejdelsen af revisionserklæringer som anført i bilag 1 sker vederlagsfrit.

11. Ændringer i Databehandleraftalen

- 11.1** Kunden kan til enhver tid, med et forudgående varsel på mindst 30 dage, foretage ændringer i Databehandleraftalen og instruksen, jf. bilag 1. Ændringsprocessen og omkostningerne aftales skriftligt mellem Kunden og Leverandøren i Hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.

- 11.2** I det omfang ændringer i lovgivningen, jf. pkt 1.1, eller tilhørende praksis, giver anledning til dette, er hver part med et varsel på 90 dage berettiget til at foretage ændringer i Databehandleraftalen. I det omfang ændringer i lovgivningen er dækket af et fast vederlag i medfør af Hovedaftalen, modtager Leverandøren ikke særskilt betaling herfor.

- 11.2.1** Ved ændringer i lovgivningen, jf. pkt 1.1 foretager Leverandøren de ændringer i Databehandleraftalen, som lovændringen giver anledning til, ens for alle Leverandørens kunder. Hvis Kunden ønsker yderligere ændringer af Databehandleraftalen, end dem Leverandøren foretager for Leverandørens øvrige kunder, vil Leverandørens bistand hertil være særskilt betalbar.

12. Sletning af data

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

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

13. Misligholdelse og tvistigheder

13.1 Misligholdelse og tvistigheder er reguleret i Hovedaftalen.

14. Erstatning og forsikring

14.1 Erstatnings- og forsikrings spørgsmål er reguleret i Hovedaftalen.

15. Ikrafttræden, varighed, og forrang

15.1 Databehandleraftalen indgås ved begge parter underskrift og løber indtil Leverandøren ikke længere behandler personoplysninger på vegne af Kunden.

15.2 Hvis der er uoverensstemmelse mellem Hovedaftalen og Databehandleraftalen, skal Databehandleraftalen have forrang.

16. Formkrav

16.1 Databehandleraftalen skal foreligge skriftligt, herunder elektronisk, hos Kunden og Leverandøren.

For Kunden

For Leverandøren

Dato

Dato

Bilag:

Bilag 1 – Instruks om behandling af oplysninger, tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse hermed samt øvrige forhold

Bilag 2 – Oplysninger om underdatabehandlere.

BILAG 1 – INSTRUKS OM BEHANDLING AF OPLYSNINGER, TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER I FORBINDELSE HERMED SAMT ØVRIGE FORHOLD.

Dette bilag er en integreret del af Databehandleraftalen.

1 INSTRUKS

1.1 Beskrivelse og formålet med behandlingen

Leverandøren behandler data i forbindelse med drift, support og vedligeholdelse af Subit's online vikarløsning som Kunden har indgået aftale om i Hovedaftalen.

1.2 Kategorier af registrerede personer

Der behandles personoplysninger om følgende kategorier af personer:

1. Lærer
2. Vikar
3. Skolemedarbejder (ansvarlig for vikardækning)

1.3 Kategorier af personoplysninger:

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier.

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6)

Almindelige personoplysninger

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

- Racemæssig eller etnisk baggrund
- Politisk overbevisning
- Religiøs overbevisning
- Filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
- Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9):

- Strafbare forhold
 - Væsentlige sociale problemer
 - Andre rent private forhold, som ikke er nævnt ovenfor:
-
-

Oplysninger om cpr-nummer jf. Databeskyttelsesforordningens artikel 87

CPR-numre

1.3.1 Typer af personoplysninger

Leverandøren behandler persondata, der indsendes, lagres, importeres, sendes eller modtages via Subit's online vikarløsning, af den dataansvarlige (eller efter hans instrukser) og af dennes autoriserede brugere.

Dataene omfatter følgende kategorier:

- Kontaktoplysninger (navn, e-mail, telefonnr., initial, brugernavn osv.)
- Fravær og årsag (Lærer) (fx akut sygdom, kursus)
- Kalender (Vikar) med tilgængelighed og aftalte lektioner
- Skolens lektionspræferencer (Vikar) (fx engelsk, fysik)
- Login oplysninger (fx tidspunkt, IP-adresse, login metode)

Der behandles ikke særlige kategorier af personoplysninger eller personoplysninger vedrørende straffedomme og lovovertrædelser.

2 TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

- 2.1 Leverandøren træffer de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysningerne beskrevet i dette bilag.
- 2.2 Leverandøren behandler personoplysningerne i overensstemmelse med nærværende Databehandleraftale og de bestemmelser i henholdsvis persondataloven og databeskyttelsesforordningen, der er gældende for databehandlere.
- 2.3 Ansatte hos Leverandøren, der er beskæftiget med behandling af personoplysninger under Databehandleraftalen, er underlagt tavshedspligt. Alene personale, som autoriseres hertil, må have adgang til de personoplysninger, der behandles under Databehandleraftalen. Såfremt det følger af Databehandleraftalen, at særlige sikkerhedsgodkendelser er påkrævet for personale, der er beskæftiget med behandling af Kundens personoplysninger, skal Leverandøren sikre, at disse godkendelser tilvejebringes.
- 2.4 Leverandøren skal sikre, at Leverandørens medarbejdere modtager tilstrækkelig uddannelse og instruktioner.

- 2.5 Leverandøren har restriktioner for fysisk adgang. Områder, hvor der sker behandling af personoplysninger - hvad enten dette er manuelt eller elektronisk – er ved adgangskontrolmekanismer adskilt fra områder, hvortil der er generel adgang. Sådanne adgangskontrolmekanismer kan eksempelvis omfatte systemer til fysisk adgangskontrol, låse, personsluser, sikkerhedspersonale og overvågningsudstyr.
- 2.6 Leverandøren har begrænsninger på adgangsrettigheder til personoplysninger og et system til adgangskontrol. Adgang til personoplysninger er begrænset til medarbejdere, og hvor det er relevant, andre leverandører, med et arbejdsbetinget behov og tildes efter forudgående godkendelse fra Leverandøren. Adgang tilbagekaldes, når brugeren ikke længere opfylder kriterierne for at have adgang. Leverandøren varetager autorisation for Leverandørens medarbejdere og, i det omfang det er særskilt aftalt i Databehandleraftalen eller i Hovedaftalen, for Kundens medarbejdere.
- 2.6.1 Adgangsrettigheder gennemgås periodisk.
- 2.6.2 Leverandøren anvender passende logiske autentifikationsmekanismer, eksempelvis adgangskoder, biometri eller lignende. De anvendte autentifikationsmekanismer lever op til, hvad der kan opfattes som god skik på området (eksempelvis krav til adgangskoders længde og kompleksitet).
- 2.7 Leverandøren har passende tekniske foranstaltninger til at begrænse risikoen for uautoriseret adgang og/eller installation af skadelig kode. Sådanne foranstaltninger kan omfatte, firewalls, anti-virus software og malware-beskyttelse. Leverandøren har formelle procedurer til sikring af, at sikkerhedssystemerne holdes opdaterede.
- 2.8 Leverandøren har formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren understøttes af en effektiv funktionsadskillelse og/eller ledelsesopfølgning for at sikre, at ingen enkeltpersoner kan kontrollere en ændring alene.
- 2.9 I det omfang det er et krav i medfør af gældende lovgivning eller i øvrigt er omfattet af Databehandleraftalen med Kunden, anvender Leverandøren relevante krypteringsteknologier og andre tilsvarende foranstaltninger. I det omfang, at det følger af Hovedaftalen, skal Leverandøren foranstalte, at systemer og data sikkerhedskopieres, samt at sikkerhedskopier opbevares betryggende og i overensstemmelse med det i Databehandleraftalen anførte.
- 2.10 Leverandøren foretager logning af personoplysninger i overensstemmelse med det i Databehandleraftalen indeholdte. Kunden er ansvarlig for selv at kontrollere Kundens adgang til og behandling af personoplysninger.
- 2.11 Leverandøren foretager i overensstemmelse med det i Databehandleraftalen indeholdte, registrering af afviste adgangsforsøg og blokering for yderligere forsøg efter et nærmere antal på hinanden følgende afviste adgangsforsøg.

- 2.12 Produktion og test foregår i adskilte miljøer.
- 2.13 Leverandøren har processer for håndtering af brud på datasikkerheden.
- 2.14 Leverandøren sikrer, at der sker sletning af data inden udstyr overgives til tredjepart eller i øvrigt bortskaffes
- 2.15 Leverandøren efterlever anbefalinger og principper i ISO27001.
- 2.16 Leverandøren skal én gang årligt (første gang i maj 2019) foranledige udarbejdet en erklæring fra en uafhængig, sagkyndig tredjepart om Leverandørens overholdelse af nærværende databehandleraftale. Erklæringen gøres årligt tilængelig for Kunden. Leverandøren sender en advisering til Kundens øverste sikkerhedsansvarlige, som Kunden har indberettet jf. punkt 3.4 i dette bilag, når den årlige erklæring foreligger. Udarbejdelsen af erklæringen er vederlagsfri, jf. pkt. 10.3.

3 ØVRIGE FORHOLD

3.1 Gældende lovgivning

Leverandørens behandling af personoplysninger er underlagt persondatalovgivningen i Danmark. Såfremt den persondataretlige regulering for andre lande end Danmark vil være gældende for behandlingen, påhviler det Kunden at oplyse Leverandøren herom samt hvilke yderligere foranstaltninger, dette måtte medføre. Eventuelle omkostninger, som Leverandøren måtte blive påført som følge heraf, skal afholdes af Kunden.

3.2 Overførsler til tredjelande

Leverandøren overfører ikke Kundens personoplysninger til tredjelande, udover i forbindelse med anvendelsen af de anførte Underdatabehandlere i bilag 2, og med det anførte overførselsgrundlag (fx EU Standard Contractual Clauses, BCR og EU-U.S. Privacy Shield certificering).

3.3 Test

Kunden kan ved specifik instruks give Leverandøren ret til at behandle alle relevante personoplysninger i det omfang det er nødvendigt for, at Leverandøren kan opfylde de i Hovedaftalen fastsatte forpligtelser og andre relaterede opgaver, herunder i nødvendigt omfang test i forbindelse med udvikling og vedligeholdelse inden for persondatarettens rammer.

Leverandøren skal godtgøre hvilke personoplysninger der er relevante for den konkrete test samt hvorfor.

3.4 Kundens øverste sikkerhedsansvarlige

Det påhviler Kunden at indberette Kundens øverste sikkerhedsansvarlige, samt substitut herfor, i relation til opgaver, som Leverandøren løser for Kunden. Kunden skal således give meddelelse om navn, titel, kontoradresse, email samt direkte telefonnummer på øverste sikkerhedsansvarlig og substitut til privacy@subit.dk. Leverandøren skal give Kunden besked om ændringer på tilsvarende vis.

BILAG 2 – ANVENDTE UNDERDATABEHANDLERE

1 ANVENDTE UNDERDATABEHANDLERE

1.1 Til brug for Leverandørens behandling af personoplysninger på vegne af Kunden anvendes følgende Underdatabehandlere:

Amazon Web Services	Hosting af systemet	Dublin, Irland	EU lovgivning
Cloudflare	Sikkerhed og stabilitet <i>Persondata bliver alene overført – ikke lagret.</i>	USA	EU Standard Contractual Clauses samt EU-U.S. Privacy Shield
DigitalOcean	Hosting af systemet	Amsterdam, Holland	EU lovgivning
Intercom	Support beskeder i Systemet	Amazon Web Services, USA	EU-U.S. Privacy Shield
Mailgun	Udsendelse af email-beskeder. <i>E-mailadresse lagres i logfil i en begrænset periode. Ingen andre persondata lagres.</i>	USA	EU Standard Contractual Clauses samt EU-U.S. Privacy Shield
Tabulex	Opdatering af skema- og fraværsoplysninger	Danmark	Dansk og EU lovgivning
Twilio	Udsendelse af SMS-beskeder. <i>Telefonnr. lagres i logfil i en begrænset periode. Ingen andre persondata lagres.</i>	USA	Binding Corporate Rules (Irland) samt EU-U.S. Privacy Shield

1.2 Hvis Leverandøren ønsker at tilføje, fjerne eller udskifte underdatabehandlere på denne liste, fremsender Leverandøren anmodninger herom til Kundens godkendelse til den e-mailadresse hos Kunden, som denne Databehandleraftale er fremsendt til.

1.3 Enhver tilføjelse, fjernelse eller udskiftning sker jf. pkt. 5 i denne Databehandleraftale.

- 1.4 Kunden skal straks underrette Leverandøren, hvis anmodninger om ændringer af underdatabehandlere skal fremsendes til en anden e-mailadresse.

2 ANVENDTE UNDERDATABEHANDLERE MED SÆRLIGE VILKÅR

Til brug for Leverandørens behandling af personoplysninger på vegne af Kunden anvendes følgende Underdatabehandlere med nedenstående særlige vilkår:

Der anvendes ikke underdatabehandlere med særlige vilkår i forbindelse med Subit's online vikarløsning.