SKABELON FOR DATABEHANDLERAFTALER

MELLEM

KUNDER OG KMD

- af 5. december 2017

DATABEHANDLERAFTALE

Mellem

[XXXX] Kunde
[adresse]
[postnr. og by]
CVR. nr.: [XXXX]
(herefter ”Kunden”)

og

KMD A/S
Lautrupparken 40-42 2750 Ballerup
CVR. nr.: DK26911745
(herefter ”Leverandøren”)

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

1. Generelt

1.1 Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:

(i) Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).

(ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).

1.2 Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at Aftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.

1.3 I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.

2. Formål

2.1 Leverandøren behandler i medfør af aftale med Kunden [titel og dato eller anden entydig identifikation] (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. Aftalens pkt. 1.1 og 1.2.

3.3 Der kan i Aftalens underbilag 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 Underbilag 1. Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Kunden, jf. pkt. 6 og Underbilag 1, og alene med henblik på opfyldelse af Hovedaftalen.

4.3 Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. Underbilag 1 – Sikkerhed.

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, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34. Medmindre andet fremgår af Hovedaftalen er Leverandørens bistand særskilt betalbar.

4.5 Leverandøren skal fra 25. maj 2018 i overensstemmelse med Databebekyttelsesforordningen 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 fra 25. maj 2018 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 frem til 25. maj 2018 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 Kommunen anvende andre underdatabehandlere end dem, der er angivet i Underbilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Kommunen 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.

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 Aftalen, herunder, at underdatabehandleren fra 25. maj 2018 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 underdatabehandlernes 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. Underbilag 1.

6.2 Leverandøren giver fra 25. maj 2018 omgående besked til Kunden, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1 Leverandøren skal frem til 25. maj 2018, jf. Underbilag 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 fra 25. maj 2018, jf. Underbilag 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 (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Kundens instruks herfor, jf. Underbilag 3.

8.2 Hvis Kundens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 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 fra 25. maj 2018 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.

10. Kontroller og erklæringer

10.1 Leverandøren er forpligtet til at give Kunden nødvendige oplysninger til, at Kunden 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 Aftalens 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 Aftalens 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 Underbilag 1. Udarbejdelsen af revisonserklæringer som anført i Underbilag 1 sker vederlagsfrit.

11. Ændringer i Aftalen

11.1 Kunden kan til enhver tid, med et forudgående varsel på mindst 30 dage, foretage ændringer i Aftalen og instruksen, jf. Underbilag 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 og 1.2, eller tilhørende praksis, giver anledning til dette, er hver part med et varsel på 90 dage berettiget til at foretage ændringer i Aftalen, I det omfang ændringer i lovgivningen er dækket af et fast vederlag i medfør af Hovedaftalen, modtager Leverandøren ikke særskilt betaling herfor.

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 forsikringsspørgsmål er reguleret i Hovedaftalen.

15. Ikrafttræden og varighed

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

16. Formkrav

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

For Kunden For Leverandøren

Dato Dato

_____ _____

Bilag:

Underbilag 1 –Behandling og sikkerhedsforanstaltninger

Underbilag 2 – Oplysninger om underdatabehandlere

Underbilag 3 – Anvendte underdatabehandlere med særlige vilkår.

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

Dette Underbilag er en integreret del af Databehandleraftalen.

1 INSTRUKS

1.1 Beskrivelse og formålet med behandlingen

[Her skal anføres en kort konkretisering af, hvad indholdet er, og hvad formålet er med behandlingen i løsningen.]

1.2 Kategorier af registrerede personer

[her angives hvilke kategorier af personer, der behandles oplysninger om i løsningen.]

1.3 Kategorier af personoplysninger:

1.3.1 Kategorier af personoplysninger

[indsæt liste over kategorier af personoplysninger for hver af de ovenfor anførte kategorier af personer, der behandles oplysninger om i løsningen]

1.3.2 Særlige kategorier af personoplysninger samt personoplysninger vedrørende straffedomme og lovovertrædelser

[Indsæt for hver af de ovenfor anførte kategorier af personer en liste over eventuelle personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssige tilhørsforhold, der behandles i løsningen. På denne liste skal ligeledes angives behandling i løsningen af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om seksuelle forhold eller seksuel orientering,

personoplysninger vedrørende straffedomme og lovovertrædelser. straffedomme og lovovertrædelser].

2 TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

2.1 KMD træffer de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysningerne beskrevet i dette Underbilag.

2.2 KMD behandler personoplysningerne i overensstemmelse med nærværende Databehandleraftale og de bestemmelser i henholdsvis persondataloven og databeskyttelsesforordningen, der er gældende for databehandlere.

2.3 Ansatte hos KMD, 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 Aftalen, at særlige sikkerhedsgodkendelser er påkrævet for personale, der er beskæftiget med behandling af Kundens personoplysninger, skal KMD sikre, at disse godkendelser tilvejebringes.

2.4 KMD skal sikre, at KMD's medarbejdere modtager tilstrækkelig uddannelse og instruktioner.

2.5 KMD 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 KMD 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 tildeles efter forudgående godkendelse fra KMD. Adgang tilbagekaldes, når brugeren ikke længere opfylder kriterierne for at have adgang. KMD varetager autorisation for KMD's medarbejdere og, i det omfang det er særskilt aftalt i Aftalen eller i Hovedaftalen, for Kundens medarbejdere.

2.6.1 Adgangsrettigheder gennemgås periodisk.

2.6.2 KMD 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 KMD har passende tekniske foranstaltninger til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode. Sådanne foranstaltninger kan omfatte, firewalls, anti-virus software og malware-beskyttelse. KMD har formelle procedurer til sikring af, at sikkerhedssystemerne holdes opdaterede.

2.8 KMD 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 Aftalen med Kunden, anvender KMD relevante krypteringsteknologier og andre tilsvarende foranstaltninger.

2.10 I det omfang at det følger af Hovedaftalen, skal KMD foranstalte, at systemer og data sikkerhedskopieres, samt at sikkerhedskopier opbevares betryggende og i overensstemmelse med det i Aftalen anførte.

2.11 KMD foretager logning af personoplysninger i overensstemmelse med det i Aftalen indeholdte. Kunden er ansvarlig for selv at kontrollere Kundens adgang til og behandling af personoplysninger.

2.12 KMD foretager i overensstemmelse med det i Aftalen indeholdte, registrering af afviste adgangsforsøg og blokering for yderligere forsøg efter et nærmere antal på hinanden følgende afviste adgangsforsøg.

2.13 Produktion og test foregår i adskilte miljøer.

2.14 KMD har processer for håndtering af brud på datasikkerheden.

2.15 KMD sikrer, at der sker sletning af data inden udstyr overgives til tredjepart eller i øvrigt bortskaffes.

2.16 KMD er certificeret i ISO27001:2013, og har implementeret kontroller for de i ISO 27002 indeholdte kontrolmål. Senest fra databeskyttelsesforordningens ikrafttræden er også indeholdt kontroller for overholdelse af databeskyttelsesforordningen. De dertil hørende politikker og processer har til formål at regulere de områder, der har indflydelse på KMD's samlede sikkerhedsniveau. Kunden kan på anmodning få udleveret en kopi af KMD's "Statement of Applicability". For så vidt angår underdatabehandlere kan hensynene i dette punkt opfyldes via andre passende foranstaltninger.

2.17 KMD skal hvert år uden særskilt vederlag foranledige udarbejdet en erklæring fra en uafhængig statsautoriseret revisor om KMD's overholdelse af generelle it-kontroller. Erklæringen skal være af en ISAE 3402 type 2-erklæring, eller erklæringer der måtte træde i stedet for denne. KMD skal endvidere uden særskilt vederlag hvert år foranledige udarbejdet en generel erklæring fra en uafhængig statsautoriseret revisor vedrørende KMD's behandlingssikkerhed i relation til persondata. Erklæringen skal udarbejdes som en ISAE 3000-erklæring, eller erklæringer, der måtte træde i stedet for denne. For så vidt angår underdatabehandlere kan hensynene i dette punkt opfyldes via andre passende foranstaltninger.

3 ØVRIGE FORHOLD

3.1 Gældende lovgivning

KMD's 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 KMD herom samt hvilke yderligere foranstaltninger, dette måtte medføre. Eventulle omkostninger, som KMD måtte blive påført som følge heraf, skal afholdes af Kunden.

3.2 Test

Kunden giver KMD ret til at behandle alle relevante personoplysninger i det omfang det er nødvendigt for, at KMD 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.

3.3 Indberetning til KMD's aftalespecifikationssystem ved printydelser.

For hvert it-system KMD driftsafvikler for Kunden fastlægges en produktionsplan, der nærmere angiver hvorledes ind- og uddata skal håndteres i normalsituationer.

Af hensyn til det praktiske arbejde er det nødvendigt, at det for hvert it-system (lønsystem, økonomisystem m.v.) fastlægges og til aftalespecifikationssystemet indberettes

(1) hvem konkret (f.eks. kontorchef N.N.) hos Kunden, der er bemyndiget til at bestille produktionsafvikling (f.eks. bestilling af ekstra økonomirapporter) uden for den normale mellem parterne aftalte produktionsplan, samt

(2) til hvilken modtager på hvilken postadresse fysiske uddata for de forskellige systemområder skal sendes.

Denne indberetning pr. system til aftalespecifikationssystemet samt ændringer hertil foretages af Kunden selv, medmindre andet aftales. Indberetning sker via aftalespecifikationssystemets indberetningsbillede Z051. (KMD kan efter aftale foretage indberetning som betalbar ydelse). Spørgsmål om indberetning kan rettes til KMD's Access Management afdeling på 44 60 42 71/iam@kmd.dk.

3.4 Kundens øverste sikkerhedsansvarlige

Det påhviler Kunden at indberette Kundens øverste sikkerhedsansvarlige, samt substitut herfor, i relation til opgaver, som KMD løser for Kunden. Kunden skal således give meddelelse om navn, titel, kontoradresse, email samt direkte telefonnummer på øverste sikkerhedsansvarlig og substitut til KMD's Access Management afdeling på 44604271/iam@kmd.dk. Kunden skal give KMD besked om ændringer på tilsvarende vis.

UNDERBILAG 2 – ANVENDTE UNDERDATABEHANDLERE

1 ANVENDTE UNDERDATABEHANDLERE

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

[indsæt navn og adresse]

UNDERBILAG 3 – ANVENDTE UNDERDATABEHANDLERE MED SÆRLIGE VILKÅR

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

[indsæt navn og adresse]

[indsæt vilkår]