Databehandleraftale

- version 1.0 af 1. november 2017 -

DATABEHANDLERAFTALE

Mellem

«KundeNavn»

«KundeAdresse»

«PostNrBy»

CVR. nr.: «KundeCVR»
(herefter benævnt "Dataansvarlig")

og

CompuSoft A/S
Sunekær 9
5471 Søndersø
CVR-Nr.: 21774774
(Herefter benævnt "Databehandler")

er der indgået nedenstående databehandleraftale (herefter "Aftalen")

vedrørende

Bookingsoftware leveret af CompuSoft A/S

hvor data opbevares

på CompuSoft's adresser på Fyn.

1 Baggrund, formål og omfang.

1.1 Som led i den Dataansvarliges indgåelse af aftale om levering af tjenester fra CompuSoft A/S, foretager Databehandleren behandling af personoplysninger, som den Dataansvarlige er ansvarlig for.

1.2 Databehandleren skal overholde Persondataloven (lov nr. 421 af 31. maj 2000 med senere ændringer) med tilhørende bekendtgørelser.

1.3 Databehandleren skal fra 25. maj 2018 i stedet for Persondataloven overholde Persondataforordningen (Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) med tilhørende retsakter samt heraf afledt national lovgivning.

1.4 Det er et krav i såvel Persondataloven som Persondataforordningen, at der mellem den dataansvarlige og databehandleren indgås skriftlig aftale om den behandling, som skal foretages; en såkaldt 'databehandleraftale'. Denne Aftale udgør sådan databehandleraftale.

1.5 Databehandleren handler alene efter instruks fra den dataansvarlige. Databehandleren skal træffe 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 lov om behandling af personoplysninger. Databehandleren skal på den dataansvarliges anmodning give den dataansvarlige tilstrækkelige oplysninger til, at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

1.6 Denne aftale er et supplement til CompuSoft, Vilkår for hosting, som er at betragte som "Hostingaftalen". Disse vilkår kan findes på: **http://www.compusoft.dk/uploads/file/terms/Hostingvilkår%201.pdf**.

2 Personoplysninger omfattet af aftalen

2.1 Denne aftale og tilhørende instruks omfatter alle følgende typer af personoplysninger:

2.2 Navn, adresse, telefonnummer, fødselsdato, forbrugshistorik, betalingsinformationer, opholdshistorik, familie-relationer, registreringsnummer, internetforbrug og kom-og-gå-statistik.

2.3 Det er den dataansvarliges ansvar, at der kun afleveres data til databehandleren, efter at der er indgået samtykke til brug af persondata med slutkunden/gæsten.

3 Geografiske krav

3.1 Den behandling af persondata, som Databehandleren foretager efter aftale med den Dataansvarlige, må alene foretages af Databehandleren eller underdatabehandlere, jf. pkt. 5, indenfor det Europæiske Økonomiske Samarbejde (EØS). Databehandleren er ingenlunde berettiget til at lade databehandling foregå udenfor EØS uden den Dataansvarliges skriftlige samtykke.

4 Instruks

4.1 Omfanget af de opgaver, som den Dataansvarlige skal levere og understøtte, betyder, at der i medfør af Parternes aftale, vil ske forskellige former for behandling af personoplysninger. De forskellige former for behandling af personoplysninger er beskrevet i afsnit 2.

4.2 Databehandleren handler alene efter dokumenteret instruks fra den Dataansvarlige. Databehandleren skal sikre, at de overladte personoplysninger ikke benyttes til andre formål eller behandles på anden måde, end hvad der fremgår af den Dataansvarliges instruks. Alle de i Hostingaftalen nødvendige og beskrevne behandlinger betragtes som dokumenterede.

a) Såfremt en instruktion efter Databehandlerens opfattelse er i strid med Persondataloven eller Persondataforordningen, skal Databehandleren orientere den Dataansvarlige herom.

b) Denne Aftale og tilhørende instruks omfatter hovedsageligt den dataansvarliges kunder/gæster og ansatte.

c) Såfremt behandlingen af personoplysninger hos Databehandleren sker helt eller delvist ved anvendelse af fjernopkobling, herunder hjemmearbejdspladser, skal Databehandleren fastsætte retningslinjer for medarbejdernes behandling af personoplysninger ved anvendelse af fjernopkobling, som i øvrigt skal opfylde de i aftalen stillede krav.

d) Databehandleren skal så vidt muligt bistå den Dataansvarlige med opfyldelse af den Dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder, herunder om indsigt, berigtigelse, begrænsning eller sletning, hvis de relevante personoplysninger behandles af Databehandleren. Modtager Databehandleren sådan henvendelse fra den registrerede, orienterer Databehandleren den Dataansvarlige herom.

4.3 Den Dataansvarlige hæfter for alle Databehandlerens omkostninger ved sådan bistand, jf. pkt. 4.6, herunder til underdatabehandleren. Databehandlerens bistand afregnes til Databehandlerens til enhver tid gældende timetakst for sådant arbejde.

5 Brug af underdatabehandlere

5.1 Den Dataansvarlige giver Databehandleren samtykke til anvendelse af underdatabehandlere, forudsat at de i Aftalen stillede betingelser for dette er opfyldt. Databehandleren underretter den Dataansvarlige om sådanne underdatabehandlere.

5.2 Underdatabehandleren er under Databehandlerens instruks. Databehandleren har indgået skriftlig databehandleraftale med underdatabehandleren, hvori det er sikret, at underdatabehandleren opfylder krav tilsvarende dem, som stilles til Databehandleren af den Dataansvarlige i medfør af Aftalen.

5.3 Omkostninger forbundet med etablering af aftaleforholdet til en underdatabehandler, herunder omkostninger til udarbejdelse af databehandleraftale og eventuel etablering af grundlag for overførsel til tredjelande, afholdes af Databehandleren og er således den Dataansvarlige uvedkommende.

5.4 Såfremt den Dataansvarlige måtte ønske at instruere underdatabehandlere direkte, bør dette alene ske efter drøftelse med og via Databehandleren. Hvis den Dataansvarlige afgiver instruks direkte overfor underdatabehandlere, skal den Dataansvarlige senest samtidig underrette Databehandleren om instruksen og baggrunden for denne. Hvor den Dataansvarlige instruerer underdatabehandlere direkte, a) er Databehandleren fritaget for ethvert ansvar, og enhver følge af sådan instruks er alene den Dataansvarliges ansvar, b) hæfter den Dataansvarlige for enhver omkostning, som instruksen måtte medføre for Databehandleren, herunder er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al arbejdstid, som en sådan direkte instruks måtte medføre for Databehandleren og c) den Dataansvarlige er selv ansvarlig overfor underdatabehandlere for enhver omkostning, vederlag eller anden betaling til underdatabehandleren, som den direkte instruks måtte medføre.

5.5 Databehandleren anvender enkelte underbehandlere.

5.6 Den Dataansvarlige accepterer ved indgåelsen af nærværende Aftale, at Databehandleren er berettiget til at skifte underdatabehandler, forudsat, at a) en eventuel ny underdatabehandler overholder tilsvarende betingelser, som stilles i nærværende pkt. 5 til den nuværende underdatabehandler og, at b) den Dataansvarlige senest ved en eventuel anden underdatabehandlers påbegyndelse af behandlingen af personoplysninger, som den Dataansvarlige er dataansvarlig for, af Databehandleren orienteres om den nye underdatabehandlers identitet.

6 Behandling og videregivelse af personoplysninger

6.1 Den Dataansvarlige indestår for at have fornøden hjemmel til behandling af personoplysningerne omfattet af nærværende Aftale.

6.2 Databehandleren må ikke uden skriftligt samtykke fra den Dataansvarlige videregive oplysninger til tredjemand, medmindre sådan videregivelse følger af lovgivningen eller af en bindende anmodning fra en retsinstans eller en databeskyttelses-myndighed, eller det fremgår af denne Aftale.

7 Sikkerhed

7.1 Databehandleren skal træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.2 og pkt. 1.3 ovenfor.

7.2 Sikkerhedsbekendtgørelsen (bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001) skal tillige overholdes, såfremt der er tale om behandling af personoplysninger for den offentlige forvaltning.

7.3 Databehandleren implementerer og opretholder de i bilag 1 beskrevne sikkerhedsforanstaltninger og i øvrigt opfylde de i "Vilkår for hosting" stillede krav. De i bilag 1 stillede sikkerhedskrav udgør den Dataansvarliges krav til sikkerhedsforhold hos Databehandleren.

7.4 Databehandleren er altid berettiget til at implementere alternative sikkerhedsforanstaltninger under forudsætning af, at sådanne sikkerhedsforanstaltninger som minimum opfylder eller giver større sikkerhed end de i bilag 1, jf. pkt. 7.3, beskrevne sikkerhedsforanstaltninger og i øvrigt opfylder de i Hostingaftalen stillede krav til sikkerhed. Databehandleren kan ikke uden den Dataansvarliges skriftlige forudgående godkendelse foretage forringelse af sikkerhedsforholdene.

7.5 Hvis Databehandleren er etableret i en anden EU-medlemsstat, skal de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den EU-medlemsstat, hvor Databehandleren er etableret, derudover gælde for Databehandleren. Hvis Databehandleren er etableret i en anden EUmedlemsstat, skal Databehandleren således overholde såvel sikkerhedskrav omfattet af gældende lovgivning i Danmark som sikkerhedskrav i Databehandlerens hjemland. Det samme gælder for underdatabehandlere.

7.6 Databehandleren skal efter nærmere aftale med den Dataansvarlige, så vidt muligt, bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i forordningens artikel 32 (gennemførelse af passende tekniske og organisatoriske foranstaltninger), 35 (foretagelse af konsekvensanalyse vedrørende databeskyttelse) og 36 (forudgående høring). I den forbindelse er Databehandleren berettiget til at fakturer den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådan aftale måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

7.7 Såfremt det i pkt. 7.6 anførte fører til skærpede sikkerhedsforanstaltninger i forhold til det allerede aftalte mellem Parterne i medfør af denne Aftale, implementerer Databehandleren, så vidt det er muligt, sådanne foranstaltninger, forudsat at Databehandleren modtager betaling herfor, jf. pkt. 7.8 nedenfor.

7.8 Omkostninger forbundet med sådan implementering af foranstaltninger, jf. pkt. 7.7, afholdes af den Dataansvarlige og er således Databehandleren uvedkommende. Databehandleren er endvidere berettiget til at fakturer den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådan implementering måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

8 Tilsynsret

8.1 Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige informationer til, at denne kan påse, at Databehandleren har truffet de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger.

8.2 I det omfang den Dataansvarlige tillige ønsker, at dette skal omfatte den behandling, som sker hos underdatabehandlere, oplyses Databehandleren om dette. Databehandleren indhenter herefter tilstrækkelige oplysninger fra underdatabehandleren.

8.3 Såfremt den Dataansvarlige ønsker at foretage tilsyn, som anført i dette pkt. 8, skal den Dataansvarlige altid give Databehandleren et varsel på mindst 30 dage i sådan forbindelse.

8.4 Såfremt den Dataansvarlige ønsker at få udarbejdet en sikkerhedsrevisionsrapport eller at der i øvrigt ønskes foretaget tilsyn af Databehandlerens eller underdatabehandlerens persondatabehandling, herunder såfremt den Dataansvarlige ønsker sikkerhedsrevisionsrapport udarbejdet på et nærmere bestemt tidspunkt, aftales dette nærmere med Databehandleren. Databehandleren eller underdatabehandleren kan til enhver tid kræve, at en sådan sikkerhedsrevisionsrapport udarbejdes i overensstemmelse med en anerkendt revisionsstandard (fx ISAE 3402 med referenceramme til ISO 27002:2014 eller lignende) af en alment anerkendt og uafhængig tredjepart, som beskæftiger sig med sådanne forhold.

8.5 Den Dataansvarlige afholder alle omkostninger i forbindelse med tilsyn af sikkerhedsforhold hos Databehandleren samt i forhold til underdatabehandleren, herunder er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådant tilsyn måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

9 Persondatasikkerhedsbrud

9.1 Såfremt Databehandleren måtte blive bekendt med et persondatasikkerhedsbrud, hvorved forstås et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, er Databehandleren forpligtet til uden unødig forsinkelse at søge at lokalisere sådan brud og søge at begrænse opstået skade i videst muligt omfang, samt i det omfang det er muligt reetablere eventuelt mistede data.

9.2 Databehandleren er endvidere forpligtet til uden unødig forsinkelse at underrette den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden. Databehandleren skal herefter uden unødig forsinkelse, i det omfang det er muligt, give skriftlig meddelelse til den Dataansvarlige, som så vidt muligt skal indeholde:

9.3 En beskrivelse af karakteren af bruddet, herunder kategorierne og det omtrentlige antal berørte registrerede og registreringer af personoplysninger.

9.4 Navn på og kontaktoplysninger for databeskyttelsesrådgiveren.

9.5 En beskrivelse af de sandsynlige konsekvenser af bruddet.

9.6 En beskrivelse af den foranstaltninger, som Databehandleren eller underdatabehandleren har truffet eller foreslår truffet for at håndtere bruddet, herunder foranstaltninger for at begrænse dets mulige skadevirkninger.

9.7 For så vidt det ikke er muligt at give de i pkt. 9.2 anførte oplysninger samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

9.8 Tilsvarende er underdatabehandlere pålagt uden unødig forsinkelse at underrette Databehandleren i overensstemmelse med pkt. 9.2 og 9.3.

10 Tavshedspligt

10.1 Databehandleren skal holde personoplysningerne fortrolige, og er således alene berettiget til at anvende personoplysningerne som led i opfyldelsen af sine forpligtelser og rettigheder i henhold til Aftalen.

10.2 Databehandleren skal sikre, at de medarbejdere og eventuelle andre, herunder underdatabehandlere, der er autoriseret til at behandle de i Aftalen omfattede personoplysninger, er pålagt tavshedspligt.

11 Varighed og ophør af databehandleraftalen

11.1 Aftalen træder i kraft ved Parternes underskrift.

11.2 I tilfælde af at Hostingaftalen ophører, uanset årsag, ophører databehandleraftalen også. Databehandleren er dog forpligtet af denne aftale, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige, idet den Dataansvarlige snarest muligt og senest 14 dage efter ophør af Hostingaftalen skal oplyse Databehandleren skriftligt, hvorledes Databehandleren skal håndtere de behandlede personoplysninger. 30 dage efter ophøret af Hostingaftalen er Databehandleren berettiget og forpligtet til at slette alle personoplysninger, som er blevet behandlet under den ophørte Hostingaftale på vegne af den Dataansvarlige.

12 Underskrift

12.1 Ovenstående tiltrædes hermed med virkning fra Parternes underskrift.

12.2 Nærværende Aftale er underskrevet i to enslydende eksemplarer, hvoraf hver af Parterne beholder ét.

For Kunden	For CompuSoft A/S
Dato: «KundeUndeskriftDato»	Dato: «CompuSoftUnderskriftDato»
«KundeUnderskriftNavn»	Thomas Traberg-Larsen

BILAG 1 – BESKRIVELSE AF SIKKERHEDSFORANSTALTNINGER

1 INDLEDNING

1.1 Dette bilag udgør det bilag, der refereres til i pkt. 7.3 i databehandleraftale, som er indgået mellem Databehandler og Dataansvarlige om levering af tjenester.

1.2 Bilaget beskriver de sikkerhedsforanstaltninger, som den Dataansvarlige stiller til den fysiske, tekniske og organisatoriske sikkerhed i forbindelse med Databehandlerens levering af tjenester.

2 FYSISK SIKKERHED

2.1 Brand, strømafbrydelser, oversvømmelser m.v. Foranstaltninger mod tyveri, brand, vand, temperatur og redundans på strøm, efter gældende branchestandarder.

2.2 Adgangskontrol Udelukkende autoriserede personer har adgang til lokalet. Eksterne personer, som leverandører eller kunder, har udelukkende adgang i følgeskab med autoriserede personer.

3 TEKNISK SIKKERHED

3.1 Firewalls og antivirus: Systemerne er beskyttet bag firewalls, der er installeret antivirus på relevante servere og systemerne er sikret mod afvikling af skadevoldende kode, efter gældende branchestandarder.

3.2 Kryptering: Al adgang til systemerne, fra andre lokationer, sker via krypterede forbindelser.

3.3 Backup og genetablering: Der tages daglig backup af alle databærende servere og backup replikeres til sekundært backup-site. Der foretages løbende tests af validiteten af backups i form af genetableringskontroller.

4 ORGANISATORISK SIKKERHED

4.1 Adgangsrettigheder: Adgangskonti er opsat med differentieret adgang, medarbejdere (og kunder) har således alene adgang til de systemer og data, som er relevant for arbejdsindsatsen.

4.2 Fortrolighed: Alle medarbejdere med adgang til systemerne er underlagt fortrolighed gennem ansættelseskontrakter eller samarbejdsaftaler.

5 Logning

5.1 Der udføres hændelseslogning, personhenførbar logning af driftsmedarbejderes adgang samt proaktiv logning med henblik på overvågning af ressourceforbrug **m.m.**

6 Sletning og kassation

6.1 Alt databærende udstyr destrueres inden bortskaffelse.