DATABEHANDLERAFTALE

VERSION 4.0 FEBRUAR 2024

CompuSoft A/S

Sunekær 9

5471 Søndersø

Danmark

CVR-nr.: 21774774

Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

«COMPANY»
CVR «COMPANYCVR»
«COMPANYADRESS»
«COMPANYZIPCITY»

herefter "den dataansvarlige"

og

CompuSoft A/S
CVR 21774774
Sunekær 9
DK-5471 Søndersø

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. INDHOLD

2. PRÆAMBEL

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af databehandlerens booking- og betalingssystem som nærmere angivet i CompuSofts VILKÅR for hosting ("**Hovedaftalen**") behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. DEN DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSER

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. DATABEHANDLEREN HANDLER EFTER INSTRUKS

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. FORTROLIGHED

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

1 Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt

6. BEHANDLINGSSIKKERHED

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. pseudonymisering og kryptering af personoplysninger

   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

   c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

   d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede

har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. ANDVENDELSE AF UNDERDATABEHANDLERE

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående specifik skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 2 måneder inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis databehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    c. behandle personoplysningerne i et tredjeland.

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. BISTAND TIL DEN DATAANSVARLIGE

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af

den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. indsigtsretten
d. retten til berigtigelse
e. retten til sletning ("retten til at blive glemt")
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering.

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. Den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. Den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

   c. Den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

   d. Den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 12 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a. Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. De sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag D angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. SLETNING OG RETURNERING AF OPLYSNINGER

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

    Arkivloven – Lovbekendtgørelse nr. 1201 af 28/09/2016

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. REVISION, HERUNDER INSPEKTION

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. PARTERNES AFTALE OM ANDRE FORHOLD

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. IKRAFTTRÆDEN OG OPHØR

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige

Navn	«PERSONSIGNATURETEXT»
Stilling	«PERSONPOSITION»
Telefonnummer	«PERSONPHONENUMBER»
E-mail	«PERSONEMAIL»

Dato og underskrift: «PERSONSIGNATUREDATE»

På vegne af databehandleren

Navn	Thomas Traberg-Larsen
Stilling	Direktør
Telefonnummer	+45 63186318
E-mail	TTL@COMPUSOFT.COM

Dato og underskrift: «CSSIGNATUREDATE»

15. KONTAKPERSONER HOS DEN DATAANSVARLIGE OG DATABEHANDLEREN

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Navn	«PERSONSIGNATURETEXT»
Stilling	«PERSONPOSITION»
Telefonnummer	«PERSONPHONENUMBER»
E-mail	«PERSONEMAIL»
Navn	Thomas Traberg-Larsen
Stilling	Direktør
Telefonnummer	+45 63186318
E-mail	TTL@COMPUSOFT.COM

BILAG A OPLYSNINGER OM BEHANDLINGEN

CompuSoft A/S udbyder som databehandler en række IT-tjenester, der omfatter hosting, bookinger og betaling ("**Systemet**"). Behandlingen er nærmere beskrevet nedenfor.

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålene er at give dataansvarliges personale adgang til et system, der kan hjælpe dem med at håndtere kundens bookinger og billetter samt i denne forbindelse opkræve betalinger og udstede fakturaer, yde teknisk support, fejlfinding og vedligeholdelse af Systemet samt beskytte imod svig, uretmæssige handlinger og sikkerhedsbrud.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Indsamling, registrering, organisering, strukturering, opbevaring, tilpasning eller ændring af personoplysninger i overensstemmelse med den dataansvarliges instruktioner.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6)

☒Almindelige personoplysninger:

Kunder og gæster: Navn, adresse, postnummer, by, nationalitet, telefonnummer, kortoplysninger, korrespondance, indhold i fritekstfelter, købte produkter, e-mailadresse samt i visse tilfælde CPR-nummer for statslige og kommunale kunder. Herudover registreres evt. opholdsperiode, antal personer, alder og køn.

Medarbejdere: Navn, adresse, telefonnummer og e-mailadresse.

Følsomme personoplysninger om (jf. Databeskyttelsesforordningens artikel 9):

☐Race eller etnisk oprindelse

☐Politisk overbevisning

☐Religiøs overbevisning

☐Filosofisk overbevisning

☐Fagforeningsmæssigt tilhørsforhold

☐Genetiske data

☐Biometriske data

☐Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v.

☐En fysisk persons seksuelle forhold eller seksuelle orientering

Personoplysninger om straffedomme og lovovertrædelser (jf. Databeskyttelses-forordningens artikel 10):

☐Straffedomme

☐Lovovertrædelser

Oplysninger om cpr-nummer (jf. Databeskyttelseslovens § 11)

☒CPR-numre (i særlige tilfælde, og udelukkende når dataansvarlig er en kommune eller statslig organisation og kun det omfang at det er nødvendigt for dataansvarlige af hensyn til opkrævning af betalinger)

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Kunder, potentielle kunder og gæster
- Medarbejdere.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Indtil aftalen opsiges.

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Cloudflare Inc.		101 Townsend Street, San Francisco, California, 94107 USA. Supportadgang kan ske fra USA. ClaudFlare Inc. er certificeret under EU-U.S. Data Privacy Framework Oplysningerne opbevares dog alene direkte via Europæiske datacentre i København, Frankfurt, Amsterdam, Hamburg og Oslo.	Cloudflare er et indholdsleveringsnetværk (CDN) og cybersikkerhedsvirksomhed, der leverer webstedsoptimering, DDoS-beskyttelse og andre sikkerhedsfunktioner for at forbedre Systemets ydeevne og beskytte mod onlinetrusler. Cloudflare yder en række sikkerhedsfunktioner, der hjælper med at beskytte Systemet mod cyberangreb. Cloudflares firewall blokerer ondsindet trafik, mens dets SSL-certifikat krypterer webtrafik for at beskytte brugerdata. Cloudflares DNS-tjenester hjælper med at beskytte mod DNS-angreb, mens dens browserisoleringsteknologi hjælper med at beskytte mod malware og andre trusler.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

Personoplysninger må alene opbevares på de steder, der er angivet i skemaet ovenfor samt på følgende adresser via databehandleren:

- Sunekær 9 | DK-5471 Søndersø
- Anderupvej 16 | DK-5270 Odense N

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 2 måneder inden anvendelsen af den pågældende underdatabehandler.

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører opgaver i henhold til Hovedaftalen.

Databehandleren skal behandle personoplysningerne på vegne af den dataansvarlige i overensstemmelse med de skriftlige instrukser fra den dataansvarlige og kun til det formål, der er angivet i databehandleraftalen. Instrukserne omfatter udtømmende følgende:

- Levering af Systemet
- Indsamling, lagring, og håndtering af personoplysningerne i overensstemmelse med den dataansvarliges instruktioner og gældende databeskyttelseslovgivning
- Sikring af fortrolighed, integritet, og tilgængelighed af personoplysningerne gennem passende tekniske og organisatoriske sikkerhedsforanstaltninger
- Sletning eller tilbagelevering af personoplysningerne efter den dataansvarliges anvisning ved afslutning af databehandleraftalen
- Rapportering af eventuelle sikkerhedsbrud, uautoriseret adgang eller lækager af personoplysningerne til den dataansvarlige inden for et rimeligt tidsrum efter opdagelsen
- Anonymisering af oplysninger til følgende formål:
    - Udvikle, optimere og analysere Systemet
    - Udarbejde og offentliggøre statistikker, rapporter og beregninger relateret til Systemet
    - Dele og sælge anonyme data til tredjeparter.

  Databehandleren indestår for, at data udelukkende behandles i fuldstændig og uigenkaldelig anonymiseret form, hvorved det hverken for databehandleren eller andre personer vil være muligt at udlede, hvilke data der er relateret til hvilke fysiske personer.

C.2. Behandlingssikkerhed

Databehandleren skal gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Generelle sikkerhedsforanstaltninger

Databehandleren skal opretholde et formelt, velimplementeret og professionelt ledelsessystem for informationssikkerhed baseret på lovgivningens krav og god databehandlingsskik. Databehandleren skal fastsætte og implementere interne politikker og bestemmelser, der er fyldestgørende og afspejler de faktiske forhold. Derudover skal Databehandleren opretholde procedurer for regelmæssig afprøvning,

vurdering og evaluering af de tekniske og organisatoriske foranstaltninger, som Databehandleren har implementeret til sikring af personoplysningerne. Databehandleren sikrer:

- Penetrationstests (sårbarhedsskanninger) både fra LAN- og WAN-siden
- Systematisk patching/opdatering af software (OS, mv.)
- Monitorering af kritiske systemer, som leverer notifikationer hvis et eller flere systemer ikke agerer som forventet
- Uafhængige backupløsninger
- Datacentrene er forsvarligt aflåst - og der forefindes kameraovervågning
- Automatisk brandslukningsanlæg er aktiveret i datacentrene
- Der er etableret redundante kølesystemer i vores datacentre
- To uafhængige nødstrømssystemer er til rådighed
- Kryptering
- Implementering af IT-sikkerhedspolitik
- Netværksovervågning
- Spejling af data
- 24/7 support
- Security incident management (nedbrudsprocedurer)
- Logning af netværksaktivitet
- Adskillelse af konto og rettigheder.

Håndtering af personoplysninger

Dokumenter og data (herunder mobile lagringsmedier), der indeholder personoplysninger, behandles så fortrolighed, integritet, tilgængelighed og robusthed bevares for at sikre, at de ikke mistes eller kommer i forkerte hænder samt for at hindre de skadevirkninger, sådanne brud måtte have for registrerede personer.

Instruktion af medarbejdere m.v.

Databehandleren sikrer at ansatte og eventuelle samarbejdspartnere til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

Adgangsstyring og administration af brugeradgang

Kun medarbejdere, som har et arbejdsbetinget behov for at behandle personoplysninger i forhold til Hovedaftalen, må være oprettet som brugere med adgang til Dataansvarliges personoplysninger. Kun de personer, der af den bemyndigede er autoriseret hertil, må have adgang til personoplysningerne.

Databehandleren skal uden ugrundet ophold annullere autorisationer (og herunder adgange) for brugere, der ikke længere har et arbejdsbetinget behov for autorisation.

Der føres en liste over autoriserede medarbejdere med angivelse af, hvilken type adgang autorisationen dækker. Listen over autoriserede medarbejdere opdateres løbende iht. god databehandlingsskik. Efterspørger Dataansvarlig listen, skal listen gøres tilgængelig uden unødigt ophold.

Ved ydelsens afslutning lukkes medarbejdernes adgang.

Databehandleren skal anvende sikre identifikations- og autorisationsteknologier, f.eks. adgangskoder, biometri eller lignende. De anvendte autentifikations-metoder skal leve op til seneste vejledning fra Digitaliseringsstyrelsen, og god skik på området.

Kontrol med afviste adgangsforsøg
Med udgangspunkt i en risikobaseret tilgang foretager Databehandleren registrering af afviste adgangsforsøg og blokerer for yderligere forsøg efter fastlagte antal på hinanden følgende afviste adgangsforsøg.

Databehandleren skal endvidere opretholde procedurer, som sikrer rettidig opfølgning på alle afviste adgangsforsøg, hvor opfølgning er nødvendig for at forhindre brud på persondatasikkerheden og skadevirkninger for registrerede personer.

Ændringshåndtering
Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.

Driftsafbrydelser
Databehandleren skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen.

Eksterne kommunikationsforbindelser
Databehandleren har passende tekniske foranstaltninger til at beskytte systemer og netværk samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

I det omfang det er et krav i medfør af gældende lovgivning, god databehandlingsskik eller i øvrigt er omfattet af hovedaftalen anvender Databehandleren krypteringsteknologier og andre tilsvarende foranstaltninger.

Ad hoc og hjemmearbejdspladser

Såfremt Databehandleren foretager databehandling fra ad hoc og/eller hjemmearbejdspladser, skal Databehandleren sikre, at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag, lovgivning i øvrigt samt Datatilsynets vejledninger herom.

Databehandleren skal blandt andet opfylde og kunne dokumentere følgende:

- Beskrivelse af anvendt krypteret forbindelse mellem ad hoc arbejdspladsen og Databehandlerens/Dataansvarliges netværk
- Databehandlerens interne instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser.

Derudover skal Databehandleren, hvis det er teknisk muligt anvende 2-faktor-autentifikation.

Bortskaffelse af udstyr

Databehandleren skal have formelle processer med henblik på at sikre, at der sker en effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2.

Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a. Forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
b. Forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

c. Forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
d. Forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
e. Forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

C.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret eller så længe, der er et sagligt grundlag for opbevaring.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de, som er angivet i Bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den dataansvarlige ikke i dette afsnit eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må databehandleren ikke foretage en sådan overførsel.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandleren skal minimum én gang årligt gennemgå sine interne sikkerhedsforanstaltninger.

Databehandleren skal for egen regning indhente en erklæring eller anden form for auditering fra en uafhængig tredjepart, angående Databehandlerens overholdelse af nærværende databehandleraftale med bilag.

Erklæringen eller resultatet af auditeringen sendes snarest muligt efter indhentelsen til orientering hos den dataansvarlige.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

BILAG D PARTERNES REGULERING AF ANDRE FORHOLD

D.1. Underretning om brud på persondatasikkerheden

I overensstemmelse med databehandleraftalens punkt 10 skal databehandleren uden unødig forsinkelse underrette den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 12 timer efter, at denne er blevet bekendt med bruddet.

Databehandlerens underretning til den dataansvarlige skal indeholde oplysninger om følgende:

- Beskrivelse af bruddet og årsagen til bruddet
- Dato og tidspunktet for bruddets start
- Dato og tidspunkt for bruddets konstatering
- Sammenlagt varighed af bruddet
- Oplistning af typen af de personoplysninger, der er berørt af bruddet (f.eks. navn, cpr.nr., oplysninger om økonomi mv.)
- Antal registrerede (personer), der er berørt af bruddet
- Beskrivelse af de sandsynlige konsekvenser/skadevirkninger af bruddet
- Beskrivelse af de foranstaltninger, der er foretaget for at standse eller begrænse bruddet, herunder dato og tidspunkt
- Oplysning om hvorvidt de berørte registrerede (personer) er blevet underrettet om bruddet, og hvordan de evt. er blevet underrettet
- Navn på *og* kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- Evt. andre oplysninger, som er nødvendige for, at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens art. 33.

Databehandleren skal i øvrigt bistå den dataansvarlige med at tilvejebringe ovenstående information i forbindelse med den dataansvarliges forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

SLUT