Databehandleraftale

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

mellem

Firmanavn:_____
CVR:_____
Gade:_____
Post nummer og by:_____
Land:_____

herefter "den dataansvarlige"

og

IOspect ApS
CVR 40562362
Brendstrupvej 61
8200 Aarhus N
Danmark

herefter "databehandleren"

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

Har med afsæt i Datatilsynets Standardkontraktsbestemmelser (december 2019) aftalt følgende (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Indhold

1. 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 IOSPECTS softwareløsninger som defineret i Bilag A 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.

2. 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.

3. 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.

4. 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 bestemmelse 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.

5. 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, jf. Bilag C.

   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.

6. Anvendelse 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 generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere som angivet i Bilag B og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). 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.

7. 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.

8. 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 i Danmark, 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 i Danmark, 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.

9. 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 24 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.

10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11. 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 samt de økonomiske forhold herom 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.

12. 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.

13. 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 skriftlig varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

   Navn _____
   Stilling _____
   Telefonnummer _____
   E-mail _____

   Underskrift

På vegne af databehandler

Navn
Stilling
Telefonnummer 4290 9008
E-mail
Underskrift

14. Kontaktpersoner 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.
   På vegne af den dataansvarlige:
   Navn _____
   Stilling _____
   Telefonnummer _____
   E-mail _____

På vegne af databehandler

Navn
Stilling
Telefonnummer 4290 9008
E-mail

15. Bilag A Oplysninger om behandlingen

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

Behandling af personoplysninger sker for at den dataansvarlige kan anvende alle funktionaliteter i DOMUSPECT app'en, dvs. herunder registrere oplysninger om lejere og håndtere digitale ind-og fraflytningssyn i de lejemål, den dataansvarlige udlejer eller administrerer for andre.

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

Via app'en sker der behandling af personoplysninger i form af bl.a.:
- Opbevaring (af de personoplysninger, som lagres i app'en)
- Systematisering (strukturerede filer)
- Transmission (til/fra underdatabehandlere)
- Videregivelse (såfremt den dataansvarlige anvender tredjeparts email leverandør til at sende rapporter fra app'en)
- Brug (når den dataansvarlige har brug for at kunne tilgå oplysningerne i app'en)
- Sletning (når den dataansvarlige sletter oplysninger i app'en)

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

Navn, e-mailadresse, telefonnummer, adresse, personnummer, betalingskortoplysninger, medlemsnummer/lejernummer, billeder af lejemål samt øvrige personhenførbare oplysninger om lejere, som den dataansvarlige registrerer i app'en, f.eks. om medarbejdere, der skal have adgang til app'en.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Lejere og andre personer, som den dataansvarlige registrerer i app'en
- Den dataansvarliges medarbejdere, der skal have adgang til app'en

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

Behandlingen af personoplysninger sker, indtil aftaleforholdet mellem Parterne ophører.

16. Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

Leverandør	Land	Lovligt grundlag for processering uden for EU	Funktion
Google	Irland/Holland		Hosting, statistik
Firebase	USA (United States)	EU-US Privacy Shield	Hosting, statistik
Hubspot	USA (United States)	EU-US Privacy Shield	CRM, E-mail flow, nyheds emails, styring af markedsføringsstrategi

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.

B.2. Varsel for godkendelse af underdatabehandlere

Varslet i medfør af punkt 7.3 er 30 dage.

17. Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

- Opbevarer de personoplysninger, den dataansvarlige lagrer i app'en
- Systematiserer og strukturerer de filer og personoplysninger, som den dataansvarlige lagrer i app'en, med henblik på fortrolighed, integritet og tilgængelighed

- Foretager transmission af personoplysninger, som den dataansvarlige lagrer i app'en, til/fra underdatabehandlere i fornødent omfang og med henblik på fuld funktionalitet i app'en
- Videregiver personoplysninger, som den dataansvarlige lagrer i app'en, såfremt den dataansvarlige anvender tredjeparts email leverandør til at sende rapporter fra app'en
- Bruger de personoplysninger, som den dataansvarlige lagrer i app'en, hvorved forstås, at brug skal ske i et omfang, så den dataansvarlige til enhver tid skal kunne tilgå oplysningerne i app'en
- Foretager sletning af oplysninger i bagvedliggende IT-systemer og IT-udstyr, som den dataansvarlige lagrer i app'en, når den dataansvarlige foretager sletning i app'en

Instruksen udføres ved, at den dataansvarlige foretager indtastninger og registreringer i app'en, som databehandleren herved anmodes om at udføre automatisk, eller meddeler databehandleren dette skriftligt på anden vis.

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle, at behandlingen som udgangspunkt ikke omfatter personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", men dog "fortrolige" personoplysninger, jf. dansk ret, hvorfor der skal etableres et "relativt højt" sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

- Sikre kryptering af personoplysningerne i relevant omfang, herunder under hensyntagen til transmission over internettet, dvs. via HTTPS, TLS 1.2 eller tilsvarende standarder i det omfang dette sker via databehandlerens app.
- Sikre, at adgang til personoplysninger alene sker for autoriserede brugere og personer
- Sikre, at adgang til databehandlerens fysiske lokaler og anvendt IT-udstyr alene sker for autoriserede brugere og personer
- Sikre, at det alene er de nødvendige personer hos databehandleren, som kan tilgå personoplysningerne
- Sikre, at anvendt IT-udstyr patches og opdateres behørigt
- Sikre, at der til stadighed er opdaterede virus- og malwareprogrammer
- Sikre, at der sker behørig logning af relevante events, herunder login i app'en opslag på personer
- Sikre, at anvendelse af hjemme-/fjernarbejdspladser som minimum sker under anvendelse af tilsvarende sikkerhedsforanstaltninger
- Generelt indføre best practice IT-sikkerhedsmæssige tiltag ud fra et "relativt højt" sikkerhedsniveau med henblik på at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester.

C.3 Bistand til den dataansvarlige
Databehandleren skal tilstræbe, at databehandlerens bistand i medfør af punkt 9 kan ske direkte via app'en uden behov for manuel involvering fra databehandlerens side. Parterne drøfter de aktuelle muligheder, som er det, databehandlerens vederlagsfrit stiller til rådighed.

Såfremt den dataansvarlige ønsker yderligere bistand end det, databehandlerens app muliggør, herunder vedrørende den dokumentation i øvrigt, som den dataansvarlige ønsker stillet til rådighed, sker dette efter vederlagsbaseret (medgået tid til sædvanlig, gældende timetakst for konsulenter hos databehandleren) og efter nærmere aftale med den dataansvarlige.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares i tidsrummet, hvor Parterne har et igangværende kontraktforhold.

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 følgende:

Brendstrupvej 61, 8200 Aarhus N, Danmark
Leopardvej 2, 7700 Thisted, Danmark
De nævnte underdatabehandlere i bilag B, B1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Databehandleren er berettiget til at overføre personoplysninger til tredjelande forudsat, at databehandleren har ret hertil i medfør punkt 8 og databehandleren har sikret gyldigt overførselsgrundlag i medfør af databeskyttelsesforordningens kapitel V.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren
Databehandleren stiller vederlagsfrit én gang årligt en egenerklæring til rådighed for den dataansvarlige, som påviser, hvordan databehandleren overholder databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Første egenerklæring er til rådighed for den dataansvarlige 12 mdr. efter denne aftales indgåelse.

Databehandleren skal herudover én gang årligt – såfremt den dataansvarlige anmoder herom – for den dataansvarliges regning indhente en revisionserklæring/inspektionsrapport fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Den Dataansvarlige meddeler omfanget og typen af den erklæring, der ønskes udarbejdet.

Rapporten/erklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering.

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 én gang årligt. Den dataansvarlige er indforstået med, at der som udgangspunkt ikke er mulighed for fysisk inspektion hos databehandlerens underdatabehandlere.

Databehandlerens udgifter i forbindelse med inspektion afholdes af den dataansvarlige, herunder databehandlerens medgåede tidsforbrug for de involverede medarbejdere. Databehandleren er forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion. Medgået tidsforbrug afregnes efter den til enhver tid gældende takst for databehandlerens konsulenter. Den dataansvarlige refunderer databehandleren for Databehandlerens eventuelle omkostninger/udlæg til tredjeparter.

C.8

1) [Beskriv eventuelle krav vedrørende pseudonymisering og kryptering af personoplysninger]

Data bliver lagret i databasen under et unikt GUID hvorunder data ligger. Transmission sker via Google Firebase vha. ssl, OAUTH, API nøgle kryptering, herunder ISO 27001 27017 27018 og det samme er gældende for firebase authentification.

2)[Beskriv eventuelle krav vedrørende evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og - tjenester]

Adgang er password protected vha 2 factor login og er begrænset til udvalgte nøglemedarbejdere. Der foretages løbende evaluering af adgang og robusthed i form at overvågning af backups og logning.

3)[Beskriv eventuelle krav vedrørende evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse]

Procedurer findes til nulstilling af adgang i tilfælde af fysisk kompromittering. Redundans i form af backups hos underdatabehandler er tilstede.

4)[Beskriv eventuelle krav vedrørende procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed]

Løbende evaluering og gennemgang af sikkerhedsregler, internt såvel som teknisk, herunder vurdering af om adgang internt skal revurderes i forhold til nøglemedarbejdere. Teknisk kontrol af behandlingssikkerheden foregår løbende i forbindelse med udvikling og opdatering af datastrømmen.

5)[Beskriv eventuelle krav vedrørende adgang til data via internettet]

Adgang er begrænset via 2 factor login og fra godkendte arbejdsstationer.

6)[Beskriv eventuelle krav vedrørende beskyttelse af data, hvor de transmitteres]

Data transmitteres via ssl sikker forbindelse.

7)[Beskriv eventuelle krav vedrørende beskyttelse af data, hvor de opbevares]

Data lagres ikke selvstændigt hos databehandleren men udelukkende hos de anførte under-databehandlere som anført i databehandleraftalen. Det kontrolleres løbende, at der er anvendt tekniske indstillinger, som forhindrer, at data transmitteres ud af EU.

8)[Beskriv eventuelle krav vedrørende fysisk sikring af lokaliteter, hvor der behandles personoplysninger]

Arbejdsstationer er 2 factor beskyttede og lokaliteterne er aflåst med nøglebrik og pinkode.

9)[Beskriv eventuelle krav vedrørende anvendelse af hjemme-/fjernarbejdspladser]

Arbejdsstationer er 2 factor beskyttede og benytter vpn forbindelse.

10)[Beskriv eventuelle krav vedrørende logning]

Der logges kun til internt brug i forhold til at opretholde den tekniske stabilitet, herunder logges kun ændringer på enkelte data strenge, som kun vedrører den dataansvarlige.

18. Bilag D Parternes regulering af andre forhold

Ansvarsfraskrivelse
Der er mellem Parterne aftalt fuldstændig ansvarsfraskrivelse i enhver henseende for alle skader, tab (såvel direkte/indirekte) og andre former for omkostninger som den dataansvarlige måtte blive påført som følge af anvendelse af databehandlerens app. Dette gælder såvel interne og eksterne omkostninger, herunder til de registrerede personer i medfør af disse Bestemmelser.

I tilfælde af tilsidesættelse af ansvarsfraskrivelsen er Parterne enige om, at et eventuelt erstatningsansvar er beløbsmæssigt begrænset (”cap”) til det beløb, den dataansvarlige har betalt til databehandleren i de sidste 3 måneder beregnet fra skadestidspunktet.

Oplysninger i medfør af punkt 10.4

Nedenstående oplysninger i det omfang, dog alene i det omfang oplysningerne kan fremskaffes fra eventuelle underdatabehandlere, såfremt sådanne har været involveret i sikkerhedsbruddet.

Brud på persondatasikkerheden hos Databehandleren	**Beskrivelse af sikkerhedsbruddet**
Dato og tidspunkt for bruddet?	
Hvad er der sket?	
Hvad er årsagen?	
Typen af berørte personoplysninger?	
Hvad er konsekvenserne for de berørte personer?	

Hvilke afhjælpende foranstaltninger har virksomheden gjort?	
Er der sket underretning af de berørte personer? (Hvis ja, hvornår?)	
Hvis personer berørt af sikkerhedsbruddet ikke er orienteret, hvad er da begrundelsen herfor?	