# DATABEHANDLERAFTALE

## Standardkontraktsbestemmelser

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

mellem

Kunden

herefter "den dataansvarlige"

og

Databehandleren
Aveo A/S
CVR 36944293
Jægergårdsgade 118
8000 Aarhus C
DK

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: udarbejdede hjemmesider og webshops, hosting og support af hjemmesider og webshops, samt online markedsføring 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

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

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.

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. 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 med mindst 14 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. 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 underdatabehandleren 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 uden unødig forsinkelse 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 C 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.

## 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 nærmeret 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 / accept 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 accepteres Bestemmelserne elektronisk.

På vegne af databehandleren

| | |
|---|---|
| Navn | Anders Linddahl |
| Stilling | Partner / Head of Web & Support |
| Telefonnummer | +45 70 40 40 50 |
| E-mail | al@aveo.dk |
| Underskrift |  |

## 15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående eller særskilt oplyste kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

| | |
|---|---|
| Navn | Anders Linddahl |
| Stilling | Partner / Head of Web & Support |
| Telefonnummer | +45 70 40 40 50 |
| E-mail | al@aveo.dk |

## Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen er, at den dataansvarlige kan anvende tjenesten (herefter "Tjenesten"), som databehandleren leverer til den dataansvarlige.

Tjenesten er, at databehandleren skal bistå den dataansvarlige med at udarbejdede hjemmeside og/eller webshop, med hosting og support af hjemmeside og/eller webshop, samt med online markedsføring af den dataansvarlige.

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

Databehandlingen indebærer primært, at databehandleren via levering af Tjenesten får adgang til at se og tilgå den dataansvarliges og registreredes personoplysninger, som behandles som led i leveringen af Tjenesten og som behandles på den dataansvarliges hjemmeside og/eller webshop. Databehandleren kan således med sin adgang se den dataansvarliges og den registreredes personoplysninger. Databehandleren tilgår og behandler udelukkende personoplysninger i den dataansvarliges systemer og behandler således aldrig personoplysningerne i sine egne systemer.

Databehandler udfører alene Tjenesten efter den dataansvarliges instrukser og kan således ikke selvstændigt behandle den dataansvarliges eller registreredes personoplysninger til egne formål.

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

- Almindelige personoplysninger om virksomhedsdeltagere og medarbejdere hos den dataansvarlige: Navn, e-mailadresse, telefonnummer, stillingsbetegnelse og arbejdsplads.
- Almindelige personoplysninger om den dataansvarliges kunder, leverandører, samarbejdspartnere, brugere, kandidater, forbrugere, patienter og andre interessenter eller lignende, herunder kontaktpersoner hos forannævnte, så som: Navn, e-mailadresse, telefonnummer, adresse, betalingskortoplysninger, medlemsnummer, type af medlemskab, stillingsbetegnelse og arbejdsplads.

### A.4. Behandlingen omfatter følgende kategorier af registrerede

- Den dataansvarliges virksomhedsdeltagere (bestyrelsesmedlemmer, direktionsmedlemmer og medejere).
- Den dataansvarliges medarbejdere.
- Den dataansvarliges kunder, leverandører, samarbejdspartnere, brugere, kandidater, forbrugere, patienter og andre interessenter eller lignende, herunder kontaktpersoner hos forannævnte.

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

Behandlingen er ikke tidsbegrænset og varer indtil det tidspunkt, hvor databehandleren ophører med at levere Tjenesten til den dataansvarlige, medmindre databehandleren modtager andre instrukser fra den dataansvarlige

## Bilag B Underdatabehandlere

### B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

| NAVN | CVR | ADRESSE | BESKRIVELSE AF BEHAND-LING |
|---|---|---|---|
| Curanet A/S (en del af team.blue) | 29 41 20 06 | Højvangen 4, 8660 Skander-borg (tem.blue: Skaldenstraat 121, 9042 Gent, Belgium) | Opbevaring af data i skyen og backup |
| | | | |
| | | | |

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

Der henvises til aftalens Bestemmelse 7.3.

Har den dataansvarlige indsigelser mod planlagte ændringer vedrørende tilføjelse eller udskiftning af en underdatabehandler, kan den dataansvarlige opsige sin aftale om Tjenesten med virkning fra tidspunktet for den planlagte ændring. Det er en forudsætning for opsigelse i henhold hertil, at opsigelsen afgives overfor databehandleren inden, at ændringen træder i kraft. Opsigelse af aftale om Tjenesten er den datansvarliges eneste beføjelser overfor databehandleren i denne situation.

## C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

- ved levering af Tjenesten, som omfatter at udarbejdede hjemmeside og/eller webshop, hosting og support af hjemmeside og/eller webshop, samt online markedsføring af den dataansvarlige. Databehandleren kan således med sin adgang se den dataansvarliges og den registreredes personoplysninger i den dataansvarliges systemer.

## C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

At behandlingen omfatter personoplysninger omfattet af databeskyttelsesforordningens artikel 6 om almindelige personoplysninger, og der skal derfor etableres et almindeligt 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:

- **Kryptering af personoplysninger**: Databehandleren sikrer, at al transmission af personoplysninger via netværk og internettet som minimum krypteres i transportlaget.
- **Sikring af vedvarende fortrolighed af behandlingssystemer og -tjenester**: Databehandleren sikrer, at det kun er autoriserede medarbejdere, der har adgang til personoplysninger til det aftalte formål, og at disse personer er underlagt et krav om fortrolighed og er bekendt med, hvordan personoplysninger behandles på en sikker måde. Databehandleren må aldrig videregive eller offentliggøre nogen af de personoplysninger, som databehandleren bliver bekendt med i forbindelse med arbejdet for den dataansvarlige. Alle medarbejdere anvender LastPass, som er en password manager, hvor krypterede adgangskoder anvendes. Alle medarbejdere skal have unikke brugernavne og passwords. Udstyr, som udleveres til medarbejdere til brug i udførelsen af arbejdsfunktioner, skal fornyes med adgangskontrol og må ikke anvendes på offentlige netværk. Medarbejdere er pålagt at opretholde denne adgangskontrol og holde adgangskoder personlige og fortrolige.

- **Sikring af vedvarende integritet af behandlingssystemer og -tjenester:** Databehandleren sikrer via elektronisk signatur, individuelle fortrolige adgangskoder og VPN-forbindelser, samt multifaktor godkendelse eller single sign on, hvor det er muligt at gemte data i systemet forbliver uændret, medmindre det er hensigten at ændre dem.
- **Sikring af vedvarende tilgængelighed af behandlingssystemer og -tjenester:** Databehandleren sikrer en velfungerende 90-dages backup. Databehandleren foretager stikprøvevis tests af backup.
- **Sikring af vedvarende robusthed af behandlingssystemer og -tjenester**: Databehandleren sikrer imod skadelige hændelser via. aftale med underdatabehandleren, Curanet A/S, som har en ISO 27001-sikkerhedsstandard, herunder i relation til udfald ved dublerede diske, køling, nødstrømsanlæg automatisk brandslukning mv.
- **Procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden**: Databehandleren systematiserer gentagne og periodiske procedurer vedrørende scanning, identifikation og afhjælpning af hidtil ukendte sikkerhedsproblemer på servere, arbejdsstationer, netværker, udstyr og applikationer.
- **Adgang til oplysningerne via internettet:** Databehandleren sikrer, at adgang til oplysninger via internettet sker med VPN-forbindelse, individuelle adgangskoder eller elektronisk signatur.
- Beskyttelse af oplysninger under transmission: Databehandleren sikrer en sikker overførelse af personoplysninger mellem databehandleren og den dataansvarlige samt til tredjeparter, der optræder som underdatabehandlere ved udelukkende at bruge krypterede overførelsesprotokoller, som eksempelvis HTTPS eller SSL.
- **Beskyttelse af oplysninger under opbevaring:** Databehandleren opbevarer al data på egen server in house, på virtuelle servere, i et eksternt datacenter eller i et anerkendt cloudmiljø. Al data opbevares indenfor EU og er sikret bag standard firewalls. Databehandleren foretager nødvendig og løbende patching af server og søger at sikre best practice for så vidt angår sikkerhed og adgangsstyring.
- **Fysisk sikring af lokaliteter**: Databehandlerens fysiske lokalitet har sikringsniveau S20 hos Falck/Verisure. Der er alene adgang til databehandlerens fysiske lokaliteter med to personligt udleverede nøgler, nøglebrikker eller lignende, hvor brugen logges og hvor brug af den enkelte nøgle kan spærres. Bærbare computere låses dagligt inde i et særskilt rum med røgkanon, som er aflåst med kodelås og metaldør.
- **Logning**: Databehandleren giver kun autoriserede personer adgang til personoplysninger via sporbare konti, der kan spores

ved navn og som ved brug bliver tilstrækkeligt logget. Databehandleren fører altid log over de personer, der har været logget på.
- **Anvendelse af hjemme-/fjernarbejdspladser:** Der kan alene oprettes forbindelse via enten VPN eller anden sikker protokol for netværksforbindelse.

**C.3 Bistand til den dataansvarlige**
Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

**Omfang og udstrækning af bistanden, som skal ydes af databehandleren:**

- Når databehandleren modtager en anmodning fra en registreret om en behandling, skal databehandleren meddele den dataansvarlige herom hurtigst muligst efter modtagelsen af anmodning. Databehandleren skal samtidig oplyse den dataansvarlige om enhver relevant information vedrørende anmodningen. Databehandleren besvarer ikke anmodninger uden at have fået skriftlig godkendelse fra den dataansvarlige, medmindre der foreligger et lovligt grundlag, som eksempel forespørgsler fra politiet.
- Databehandleren er ikke berettiget til vederlag i forbindelse med sin bistand til den dataansvarlige medmindre bistanden kræver særlige tiltag, som den dataansvarlige ikke med rette kunne forvente, at databehandleren var i stand til på tidspunktet.

**Underretning om brud på persondatasikkerheden**

- Databehandleren skal underrette den dataansvarlige om ethvert brud på persondatasikkerheden. Databehandleren kan derfor ikke undlade at underrette den dataansvarlige om et brud på persondatasikkerheden, fordi databehandleren har en formodning om, at den dataansvarlige er bekendt med bruddet, eller fordi bruddet efter databehandlerens egen vurdering ikke skal anmeldes.
- Så snart databehandleren opdager et brud på persondatasikkerheden, skal databehandleren straks foretage de nødvendige foranstaltninger for at begrænse de negative konsekvenser af bruddet og for at begrænse gentagelse heraf.
- Databehandleren har ikke den dataansvarliges bemyndigelse til at anmelde brud på persondatasikkerheden til Datatilsynet eller andre myndigheder.
- Databehandleren må ikke offentliggøre et brud på persondatasikkerheden til tredjeparter uden den dataansvarliges skriftlige

tilladelse, medmindre dette er et krav efter databeskyttelsesforordningen eller gældende ret, og i så fald skal databehandleren underrette den dataansvarlige herom, inden offentliggørelsen.

**C.4 Opbevaringsperiode/sletterutine**
Personoplysninger opbevares ikke af databehandleren, da databehandleren kun behandler og tilgår personoplysningerne i den dataansvarliges systemer.

Når samarbejdet mellem parterne ophører, slettes databehandlerens adgang til den dataansvarliges system, således at databehandleren ikke længere kan tilgå systemet.

**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:

- Behandlingen af personoplysninger finder sted hos den dataansvarlige og databehandleren på deres adresser, samt fra elektroniske enheder der har sikker fjernadgang til Tjenesten.
- Behandling kan endvidere finde sted hos de underdatabehandlere, som fremgår, jf. bilag B.

**C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande**

Databehandleren må ikke overføre personoplysninger til tredjelande eller internationale organisationer.

Hvis den dataansvarlige ikke herudover i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

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

Den dataansvarlige eller en repræsentant for den dataansvarlige har ret til efter begrundet anmodning, at foretage et tilsyn, hvert 2. år, vedrørende overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og af denne databehandleraftale hos databehandleren. Databehandleren skal stille de nødvendige oplysninger til rådighed for den dataansvarlige

Såfremt den dataansvarlige ønsker at foretage tilsyn, i henhold til dette pkt. C.7, skal den dataansvarlige altid give databehandleren et varsel på mindst 30 dage i sådan forbindelse.

Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sit tilsyn. Den dataansvarlige betaler for databehandlerens tidsforbrug i forbindelse med tilsyn.

Alternativt kan den dataansvarlige anmode databehandleren om udfyldelse af et tilsynsskema, som den dataansvarlige sender til databehandleren. Den dataansvarlige betaler for databehandlerens tidsforbrug i forbundet med udfyldelsen af skemaet. Det udfyldte tilsynsskema fremsendes uden unødig forsinkelse til dataansvarlige. Den dataansvarlige kan anfægte rammerne for og/eller metoden i dokumentationen og kan i sådanne tilfælde anmode om ny dokumentation under andre rammer og/eller under anvendelse af anden metode, herunder tilsyn i overensstemmelse med det føromtalte.

**C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere**

På den dataansvarliges anmodning kan denne få udleveret kopi af underdatabehandleres eventuelt årligt udarbejdede sikkerhedsrevisionserklæring, som beskriver sikkerhedsforholdene hos underdatabehandlerne. Sikkerhedsrevisionserklæringen fra underdatabehandleren, Curanet A/S, kan i øvrigt altid hentes på dennes hjemmeside.

Databehandleren eller en repræsentant for databehandleren vurderer årligt (dog tidligst efter 2 år), om der er (yderligere) behov for et fysisk tilsyn vedrørende overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og af denne databehandleraftale hos underdatabehandlerne.

Såfremt den dataansvarlige ønsker at få udarbejdet anden eller yderligere sikkerhedsrevisionserklæring udover de erklæringer som underdatabehandleren, Curanet A/S, allerede får udarbejdet på eget initiativ, eller at der i øvrigt ønskes foretaget tilsyn af underdatabehandlernes persondatabehandling, herunder såfremt den dataansvarlige ønsker sikkerhedsrevisionserklæring udarbejdet på et nærmere bestemt tidspunkt, aftales dette nærmere med underdatabehandlerne. Når tilsyn sker på anmodning fra den dataansvarlige, fra tredjeparter på foranledning af den dataansvarlige, eller fra myndigheder grundet forhold hos den dataansvarlige afholder den dataansvarlige alle omkostninger i forbindelse med tilsyn af sikkerhedsforhold hos underdatabehandlerne, herunder er underdatabehandlerne, såvel som databehandleren,

berettiget til at fakturere den dataansvarlige med sin sædvanlige timetakst for al underdatabehandlernes og databehandlerens arbejdstid, som sådant tilsyn måtte medføre for underdatabehandlerne og databehandleren.

Dokumentation for sikkerhedsrevisionserklæringen eller for de afholdte tilsyn kan efter anmodning udleveres til orientering hos den dataansvarlige.

Den dataansvarliges eventuelle deltagelse i et tilsyn hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og af denne databehandleraftale.

Såfremt inspektion og eller kontrol, som medfører udgifter, initieres af databehandleren, skal dette være godkendt af den dataansvarlige på forhånd, for at den Dataansvarlige kan pålægges at afholde disse udgifter.

## Bilag D Parternes regulering af andre forhold

**Ikke relevant.**

Aveo A/S
Tlf. 70 40 40 50
kontakt@aveo.dk
CVR 36944293
Jægergårdsgade 118
8000 Aarhus C