

## DATABEHANDLERAFTALE

### Standardkontraktbestemmelser

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

Mellem

Kunder i Danmark, der anvender løsningen SalesHero™

herefter benævnt "Kunden"

og

Beezy365 A/S  
CVR.: 25470168  
Danmarksgade 2A  
4690 Haslev  
Danmark

herefter benævnt "Databehandleren"

der hver især er en "Part" og sammen udgør "Parterne"

er aftalt følgende standardkontraktbestemmelser (herefter benævnt "Bestemmelserne") med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

# Indholdsfortegnelse

<b>1. Indhold</b>	
1. Præambel .....	3
2. Kundens rettigheder og forpligtelser .....	4
3. Databehandleren handler efter instruks .....	4
4. Fortrolighed .....	4
5. Behandlingssikkerhed .....	4
6. Anvendelse af underdatabehandlere .....	5
7. Overførsel til tredjelande eller internationale organisationer .....	6
8. Bistand til den dataansvarlige .....	7
9. Underretning om brud på persondatasikkerheden .....	8
10. Sletning og returnering af oplysninger .....	8
11. Revision, herunder inspektion .....	8
12. Parternes aftale om andre forhold .....	9
13. Ikrafttræden og ophør .....	9
Bilag A Oplysninger om behandlingen .....	10
Bilag B Underdatabehandlere .....	12
Bilag C Instruks vedrørende behandling af personoplysninger .....	13
Bilag D Parternes regulering af andre forhold .....	18

## 1. Præambel

1. Bestemmelserne fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af Kunden.
2. Bestemmelserne 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 "SalesHero - Master Subscription Agreement" (i det følgende benævnt Hovedaftalen) behandler databehandleren personoplysninger på vegne af Kunden i overensstemmelse med Bestemmelserne.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til Bestemmelserne, 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 Kundens betingelser for databehandlerens brug af en anden databehandler (underdatabehandler) og en liste over underdatabehandlere, som Kunden har godkendt brugen af på tidspunktet for Bestemmelsernes ikrafttræden.
8. Bilag C indeholder Kundens 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 er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Bestemmelserne frigør ikke databehandleren fra forpligtelser, som denne er pålagt efter Databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og enhver anden lovgivning.

## 2. Kundens rettigheder og forpligtelser

1. Kunden er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med Databeskyttelsesforordningen (se artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes<sup>1</sup> nationale ret og Bestemmelserne.
2. Kunden har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Kunden 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 Kunden, 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 Kunden, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med Bestemmelserne.
2. Databehandleren underretter omgående Kunden, hvis en instruks efter vedkommendes mening er i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.
3. Databehandleren anses som selvstændig dataansvarlig for en eventuel behandling, som databehandleren foretager i strid med instruksen fra Kunden.

## 4. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på Kundens 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.
2. Databehandleren skal efter anmodning fra Kunden kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

## 5. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at Kunden og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varie-

---

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

rende 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.

Kunden 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 Databeskyttelsesforordningens artikel 32 skal databehandleren – uafhængigt af Kunden – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal Kunden 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 Kunden med vedkommendes overholdelse af Kundens forpligtelse efter Databeskyttelsesforordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for Kunden vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til Databeskyttelsesforordningens artikel 32, og al anden information, der er nødvendig for Kundens overholdelse af sin forpligtelse efter Databeskyttelsesforordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter Kundens vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal Kunden 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 underdatabehandler.
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af Bestemmelserne uden forudgående specifik skriftlig godkendelse fra Kunden.
3. Databehandleren må kun gøre brug af underdatabehandlere med den Kundens forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 60 kalenderdage inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt på tidspunktet for Bestemmelsernes ikrafttræden, fremgår af Bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af Kunden, 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 Bestemmelserne, 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 Bestemmelserne og Databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter Bestemmelserne og Databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter Kundens anmodning herom – i kopi til Kunden, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af Bestemmelserne er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til Kunden.
6. Databehandleren skal i sin aftale med underdatabehandleren indføre Kunden som begunstiget tredjemand i tilfælde af databehandlerens konkurs, så Kunden kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør Kunden 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 Kunden for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af Databeskyttelsesforordningen, herunder særligt artikel 79 og 82, over for Kunden og databehandleren, herunder underdatabehandleren.

## 7. Overførsel til tredjelande eller internationale organisationer

- Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra Kunden og skal altid ske i overensstemmelse med Databeskyttelsesforordningens kapitel V.
- Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af Kunden, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette Kunden om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
- Uden dokumenteret instruks fra Kunden 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.
- Kundens 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.

- Bestemmelserne skal ikke forveksles med standardkontraktbestemmelser som omhandlet i Databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og Bestemmelserne 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 Kunden ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af Kundens 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 Kunden i forbindelse med, at Kunden 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 indsigelse
  - i. 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 Kundens i henhold til Bestemmelsernes 5.3., bistår databehandleren desuden, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, Kunden med:
    - a. Kundens forpligtelse til uden unødigt 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 det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
    - b. Kundens forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
    - c. Kundens forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse).
    - d. Kundens 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 nødvendige tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå Kunden samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelsernes 8 og 9.

## 9. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødige forsinkelse Kunden efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til Kunden skal om muligt ske senest 24 timer efter, at databehandleren er blevet bekendt med bruddet, sådan at Kunden kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, jf. Databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelsernes 8.2.a skal databehandleren bistå Kunden med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed, Datatilsynet. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge Databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af Kundens anmeldelse af bruddet til den kompetente tilsynsmyndighed, Datatilsynet:
  - 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 Kunden i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet.

## 10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesten vedrørende behandling af personoplysninger er databehandleren forpligtet til at tilbagelevere alle de behandlede personoplysninger og til at slette eksisterende kopier – herunder også fra en eventuel backup – samt skriftligt bekræfte over for Kunden, at personoplysningerne er slettet, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.
2. Databehandleren er forpligtet til at sikre, at eventuelle underdatabehandlere ligeledes tilbageleverer alle de behandlede personoplysninger og sletter eksisterende kopier heraf.

## 11. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af Databeskyttelsesforordningens artikel 28 og Bestemmelserne, til rådighed for Kunden og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af Kunden eller en anden revisor, som er bemyndiget af Kunden.
2. Procedurerne for Kundens 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 lovgivning har adgang til Kundens 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 Kundens oprettelse af brugerkonto på Data-behandlerens hjemmeside.
2. Parterne kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder 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 Bestemmelsernes 10 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af Parterne.
5. Underskrift  
Ved Kundens oprettelse af brugerkonto, accepterer Kunden ved afkrydsning, betingelserne i herværende Databehandleraftale. Accepten er gældende som gyldig underskrift fra Parterne.

## Bilag A Oplysninger om behandlingen

### A.1. Formålet med behandlingen af personoplysningerne

Behandlingen af den Dataansvarliges oplysninger sker i henhold til formålet i Hovedaftalen. dvs. et system til håndtering af den Dataansvarliges B2B virksomheds kundeinformationer, aktiviteter og dokumenter, med de funktioner og moduler som den Dataansvarlige har aktiveret i systemet, samt valgte dataintegrationsløsninger til 3. parts systemer.

### A.2. Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af Kunden drejer sig primært om

- 1) Registrering og lagring af B2B kundeoplysninger og navne på personer der kan modtage tilbud genereret af SalesHero.

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

A.3.1. Behandlingen omfatter nedenfor afkrydsede kategorier om de registrerede.

A.3.2. databehandlerens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle de behandlede personoplysningers følsomhed jf. Bilag C.2.

**Almindelige personoplysninger** (jf. Databeskyttelsesforordningens artikel 6):

Almindelige personoplysninger:

Helt konkret omfatter behandlingen følgende typer af almindelige personoplysninger:

- Navn
- Stillingsbetegnelse, roller eller funktion
- Telefonnummer
- Socialmedia konto, ex. LinkedIn
- E-mailadresser
- Kalender og mødeaktiviteter
- E-mail korrespondance
- Virksomhed, arbejdssted
- CV oplysninger og relationer til andre virksomheder
- Billede

**Følsomme personoplysninger** om (jf. Databeskyttelsesforordningens artikel 9):

Ingen.

**Personoplysninger om straffedomme og lovovertrædelser** (jf. Databeskyttelsesforordningens artikel 10):

Ingen.

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

Ingen

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

Behandlingen omfatter nedenfor nævnte kategorier af registrerede.

- A. Dataansvarliges medarbejdere med administrative rettigheder i systemet.
- B. Personer og medarbejdere som er ansat eller har relationer til Dataansvarliges kunder/virksomheder.
- C. Samarbejdsrelationer eller andre personer som Dataansvarlige ønsker at registrere i systemet.

#### **A.5. Behandlingens varighed**

A.5.1. databehandlerens behandling af personoplysninger på vegne af Kunden kan påbegyndes efter Bestemmelsernes ikrafttræden jf. Bestemmelsernes 13.1.

A.5.2. Varigheden af databehandlerens behandling af personoplysninger på vegne af Kunden er så længe denne er i besiddelse af personoplysningerne eller på anden vis behandler personoplysninger for Kunden alt efter hvilket tidspunkt, der indtræder senest.

## Bilag B Underdatabehandlere

### B.1. Godkendte underdatabehandlere

B.1.1. Ved Bestemmelsernes ikrafttræden har Kunden godkendt brugen af følgende underdatabehandlere:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
DigitalOcean Netherlands B.V.	NL860939050B01	Barbara Strozziiaan 101, 1083 HN Amsterdam, The Netherlands	Hosting af Webservers og Databaser for SalesHero systemet
Twilio Ireland Limited (on behalf of Send- Grid, Inc.)	IE3582319LH	25-28 North Wall Quay, Dublin 1, D01 H104, Ireland	Sendgrid benyttes til fremsendelse af tilbud, opfølgningsmail og andre typer e-mail der udsendes fra SalesHero
Intuit Inc. MailChimp/Mandrill		Intuit France SAS, 7 rue de Madrid, 75008 Paris, France	Udsendelse af onboarding e-mails, samt nyhedsbreve m.m.
Crisp IM SARL	FR79833085806	2 Boulevard de Launay, 44100 Nantes, France	Kundesupport chat

B.1.2. Ved Bestemmelsernes ikrafttræden har Kunden godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. databehandleren må ikke – uden Kundens forudgående specifikke 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.1.3. Ændringer i forholdene hos underdatabehandleren

Databehandleren forpligtes til straks og senest 1 måned inden ændringen at orientere den dataansvarlige, hvis der sker ændringer i vilkårene for anvendelse af underdatabehandlere, som den Dataansvarlige har accepteret ved denne databehandleraftale. Dette gælder fx ændringer, som har indflydelse på den registreredes rettigheder, og/eller ændringer i et tredjeland, hvor en underdatabehandler befinder sig.

### B.2. Varsel for godkendelse af underdatabehandlere

B.2.1. Ønsker databehandleren at gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte, eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet, skal den dataansvarlige varsles skriftligt senest 60 dage før underdatabehandleren påbegynder behandlingen.

B.2.2. Kunden kan – ved skriftlig henvendelse til databehandleren senest 30 dage efter dennes varsel for godkendelse af underdatabehandlere i henhold Bestemmelsernes B.2.1. – modsætte sig brugen af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og/eller aftalte, og brugen af en anden underdatabehandler til denne behandlingsaktivitet, hvis der foreligger en saglig begrundelse herfor.

Mod sætter Kunden sig brugen af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte og/eller brugen af en anden underdatabehandler til denne behandlingsaktivitet, må behandlingen af personoplysninger hos den pågældende underdatabehandler ikke påbegyndes.

## Bilag C Instruks vedrørende behandling af personoplysninger

### C.1. Behandlingens genstand/instruks

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

- 1) Registrering og lagring af den Dataansvarliges indtastede personoplysninger og informationer samt aktiviteter og uploadede dokumenter og grafik elementer.
- 2) Automatiske overførelser af specifikke datapakker via dataintegrationer valgt og opsat af Dataansvarlige.
- 3) Natlige automatiske datakørsler, med det formål at opdatere, beregne og konsolidere de registrerede og lagrede data.

### C.2. Behandlingsikkerhed

C.2.1. Sikkerhedsniveauet skal afspejle behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

C.2.1.1. LAVT: Behandlingen af personoplysninger omfatter alene almindelige personoplysninger, og mængden af de personoplysninger, der behandles, er mindre.

C.2.2. 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.

C.2.3. databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med Kunden.

#### Pseudonymisering og kryptering af personoplysninger

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysningerne **pseudonymiseres**, herunder særligt når og hvis det ikke (længere) er nødvendigt at kunne identificere de(n) registrerede.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Alle brugernavne og authentication/godkendelses koder krypteres med 256-bit kryptering.

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysningerne **krypteres**, når og hvis det er nødvendigt, herunder særligt i forbindelse med transmission via åbne netværk og/eller eksterne kommunikationsforbindelser jf. også nedenfor under 'beskyttelse af personoplysninger ved transmission'.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Ved overførelse af data beskyttes data med SSL-certifikat og https-kryptering.

#### Sikring af varierende fortrolighed, integritet, tilgængelighed og robusthed af systemet

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer, at en passende **fortrolighed** er allestedsværende ved behandlingen af personoplysningerne, herunder i forbindelse med systemadgang og fysisk adgang til lokationerne for behandlingen.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Alle data er placeret i Digital Oceans datacenter og ingen medarbejdere har fysisk adgang til data.
- B. Kun godkendte medarbejdere med de godkendte og tildelte rettigheder har systemadgang til Dataansvarliges data.

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer, at en passende **integritet** er allestedsværende ved behandlingen af personoplysningerne, herunder sikre personoplysningernes troværdighed og korrekthed.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Databehandler ikke manuelle opgaver på Dataansvarliges data uden direkte instruks fra Dataansvarlige

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer en allestedsværende **tilgængelighed** af personoplysningerne, herunder ved fysiske og tekniske hændelser jf. nedenfor om 'genoprettelse af personoplysningerne'.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Der foretages daglige backup af Dataansvarliges database.

#### **Genoprettelse af personoplysningerne**

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer rettidig genoprettelse af tilgængelighed til personoplysningerne i tilfælde af fysiske hændelser (strømafbrydelse, brand, oversvømmelse, lynnedslag mv.) og/eller tekniske hændelser (systemnedbrud DoS mv.), herunder i form af beredskabsplaner, procedurer mv.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Digital Oceans datacentre er opbygget med en infrastruktur som sikrer 24/7/365 drift og dataadgang.
- B. Ved 3. parts produktadgang er der indgået en 24 timers SLA

#### **Adgang til personoplysningerne via Internettet**

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysningerne beskyttes mod blandt andet uvedkommendes adgang og/eller manipulation når og hvis der er adgang til disse via Internettet jf. også ovenfor under 'pseudonymisering og kryptering'.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Bruger adgang og styring sker igennem OAuth 2.0 Authorization Framework, beskrevet i RFC 6749.
- B. Det er også muligt for brugere af systemet at opsætte 2-factor authentication.

#### **Beskyttelse af personoplysningerne under transmission**

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysningerne krypteres eller på anden vis beskyttes mod blandt andet uvedkommendes adgang og/eller manipulation når og hvis disse transmitteres jf. også ovenfor under 'pseudonymisering og kryptering'.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Der sker ingen yderligere kryptering af personoplysninger ind dem som er indeholdt https-krypteringen.

#### Anvendelse af hjemme- og fjernarbejdspladser

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger beskyttes mod blandt andet uvedkommende adgang og/eller manipulation, når disse tilgås fra hjemme- og fjernarbejdspladser, og at der ved adgang til personoplysninger fra hjemme- og fjernarbejdspladser anvendes kryptering af kommunikationsforbindelser samt autentifikation af personer, som får adgang.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Databehandler anvender hjemmearbejdspladser.
- B. Sikringen af adgang til data sker på IP-adresse niveau, kun godkendte ip-adresse har adgang til data.
- C. Adgang til data sker med OAuth 2.0 Authorization uanset hvor Databehandlers medarbejder arbejder.

#### Logning

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer logning af al tilgang til personoplysningerne i et sådant omfang, at logoplysningerne til enhver tid kan anvendes til at opklare, og i videst mulig forebygge uberettiget adgang til og misbrug af personoplysningerne.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Logning af dataadgang sker på database niveau.

#### Regelmæssig afprøvning, vurdering og evaluering af foranstaltninger til sikring af behandlingssikkerheden

Databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer regelmæssig afprøvning, vurdering og evaluering af effektiviteten af foranstaltninger til sikring af behandlingssikkerheden.

Med henblik på at opfylde ovennævnte har databehandleren helt konkret gennemført følgende:

- A. Afprøvning, vurdering og evaluering af foranstaltninger sker løbende i forbindelse med tilsyn.

### **C.3 Bistand til den dataansvarlige**

C.3.1. databehandleren skal så vidt muligt bistå Kunden med følgende i overensstemmelse med Bestemmelsernes 8 og 9:

#### Opfyldelse af Kundens forpligtelser

Databehandleren skal på opfordring fra Kunden hjælpe med at opfylde og efterleve dennes forpligtelser, herunder i relation til følgende:

1. Den registreredes rettigheder, herunder blandt andet besvarelse af anmodninger om indsigt, berigtigelse og sletning, jf. Databeskyttelsesforordningens kapitel III.
2. Underretning af de registrerede ved brud på persondatasikkerheden jf. Databeskyttelsesforordningens artikel 34.

3. Sikring af overholdelse af forpligtelserne i Databeskyttelsesforordningens artikel 32-36 jf. artikel 28, stk. 3, litra f.

#### **Brud på persondatasikkerheden**

Databehandleren skal ved brud på persondatasikkerheden fremsende dokumentation for de faktiske omstændigheder herved, dets virkning og de trufne afhjælpende foranstaltninger. Indholdet af den fremsendte dokumentation skal være så fyldestgørende, at den om nødvendigt kan tjene som en anmeldelse til Datatilsynet og/eller underretning af den registrerede.

Databehandleren skal – uden unødigt forsinkelse og om muligt senest 24 timer efter, at databehandleren er blevet bekendt med bruddet på persondatasikkerheden – underrette Kunden herom ved skriftlig henvendelse til Kundens systemansvarlige, så Kunden kan overholde sin forpligtelse til at anmelde det til Datatilsynet jf. Databeskyttelsesforordningens artikel 33.

C.3.2. databehandleren skal så vidt det er muligt indrette tjenesten vedrørende behandling af personoplysninger (systemet) på en sådan måde, at Kunden let kan efterleve sine forpligtelser over for den registrerede.

Såfremt det ikke er muligt at indrette tjenesten vedrørende behandling af personoplysninger (systemet) på en sådan måde, at Kunden let kan efterleve sine forpligtelser over for den registrerede, skal databehandleren bistå Kunden hermed. En sådan bistand er uden omkostninger for Kunden.

C.3.3. databehandleren har i øvrigt de forpligtelser, der følger af Databeskyttelsesforordningen og øvrig relevant lovgivning på området. Disse forpligtelser forbliver hos databehandleren, og skal opfyldes uden omkostninger fra Kunden.

#### **C.4 Opbevaringsperiode/sletterutine**

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren tilbagelevere og slette alle de behandlede personoplysninger i overensstemmelse med Bestemmelse 10.1, medmindre Kunden – efter underskriften af disse Bestemmelser – har ændret sit oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

#### **C.5 Lokalitet for behandlingen**

C..5.1. Lokaliteten for databehandlerens behandling af de af Bestemmelserne omfattede personoplysninger er følgende:

- Beezy365 A/S, Danmarksgade 2A, 4690 Haslev

C.5.2. Lokaliteten for de på tidspunktet for Bestemmelsernes ikrafttræden godkendte underdatabehandlers behandling af de i Bestemmelserne omfattede personoplysninger følger af Bestemmelsernes B.1.1.

C.5.3. Ændring af lokaliteten for databehandlerens såvel som de af Kunden til enhver tid godkendte underdatabehandlers behandling af de i Bestemmelserne omfattede personoplysninger forudsætter Kundens forudgående skriftlige godkendelse.

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

C.6.1. Databehandleren må ikke overføre Kundens personoplysninger til tredjelande.



C.6.2. Hvis Kunden ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til, inden for rammerne af disse Bestemmelser, at foretage sådanne overførsler.

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

C.7.1. Databehandleren stiller vederlagsfrit hvert andet år en egen erklæring til rådighed for den dataansvarlige, som påviser, dennes overholdelse af Databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

C.7.2. Baseret på resultaterne af ledelseserklæringen er Kunden berettiget til at anmode om gennemførelse af yderligere (kontrol)foranstaltninger med henblik på at sikre overholdelsen af Databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

C.7.4. Kunden eller en repræsentant for Kunden har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af Kundens personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner gennemføres, når Kunden finder det nødvendigt.

C.7.5. Eventuelle udgifter i forbindelse med en sådan inspektion afholdes af Kunden. databehandleren er dog forpligtet til at afsætte de nødvendige ressourcer (hovedsageligt den nødvendige tid), der er nødvendig for, at inspektionen kan gennemføres.

C.7.5. Foretager Datatilsynet tilsyn med databehandleren på eget initiativ afholdes alle udgifter i forbindelse hermed af databehandleren.

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

C.8.1. databehandleren skal hvert andet år indhente en erklæring vedrørende underdatabehandlerens overholdelse af Databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

## Bilag D Parternes regulering af andre forhold

### 1. Misligholdelse og tvistigheder

- 1.1. Som misligholdelse anses enhver tilsidesættelse af parternes forpligtelser i henhold til Bestemmelserne.
- 1.2. Dersom en Part gentagne gange gør sig skyldig i misligholdelse jf. pkt. 1.1. vil dette være at betragte som væsentlig misligholdelse.
- 1.3. Parterne er ansvarlige efter dansk rets almindelige regler om misligholdelse, herunder om afhjælpning og ophævelse ved væsentlig misligholdelse.
- 1.4. Misligholder en Part en forpligtelse i henhold til Bestemmelserne, skal den anden Part, uden ugrundet ophold, ved skriftlig erklæring fastsætte en efter karakteren af misligholdelsen rimelig frist, inden for hvilken misligholdelsen skal bringes til ophør.
- 1.5. Består Partens misligholdelse fortsat efter udløbet af den fastsatte tidsfrist jf. punkt 1.4., vil dette være at betragte som væsentlig misligholdelse.
- 1.6. Parterne kan ikke anses for ansvarlig over for hinanden for så vidt angår forhold, som ligger uden for deres kontrol, og som de ikke ved databehandleraftalens indgåelse burde have taget i betragtning, og ej heller burde have undgået eller overvundet (force majeure).
- 1.7. Påberåbelse af force majeure forudsætter, at Parten opfylder følgende betingelser:
  - Parten skal, uden ugrundet ophold efter konstateringen af force majeure-situationen, skriftligt informere den anden Part om grundlaget herfor, varigheden heraf, hvis muligt, samt hvilke forholdsregler pågældende har truffet for at bringe force majeure-situationen til ophør.
  - Parten skal over for den anden Part, uopfordret skriftligt dokumentere, at en forsinkelse skyldes force majeure.
- 1.8. Databehandleren er ikke berettiget til at tilbageholde Kundens personoplysninger i tilfælde af dennes misligholdelse af Hovedaftalen.

### 2. Erstatning og forsikring

- 1.1. Parterne er i det hele erstatningspligtige i henhold til dansk rets til enhver tid gældende almindelige regler herom.
- 1.2. Parterne er egenhændigt forpligtet til, og ansvarlige for at tegne eventuelle forsikringer, som er nødvendige for pågældendes opfyldelse af forpligtelserne i henhold til Bestemmelserne.