

Skriv venligst direkte i felterne herunder, sæt jeres stempel og underskrift på side 10, og send et eksemplar til [support@farpay.dk](mailto:support@farpay.dk).

Modtager	
Virksomhedsnavn	
Adresse	
Postnr.	
By	
CVR-nr.	
Kontaktperson	
Stilling	
Telefon	
E-mail	

## Standardkontraktbestemmelser

I henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger, er denne databehandlersaftale indgået mellem;

CVR-nr.

*("Kunden" eller den "Dataansvarlige")*

og

### FarPay ApS

Wildersgade 14, 3.

1408 København K

CVR-nr. 37295043

*("FarPay" eller "Databehandleren")*

Parterne har aftalt følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen, for at sikre beskyttelse af privatlivets fred, og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

## 1. Indholdsfortegnelse

2. Præambel .....	3
3. Den dataansvarliges rettigheder og forpligtelser .....	3
4. Databehandleren handler efter instruks .....	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 .....	9
12. Parternes aftale om andre forhold .....	9
13. Ikrafttræden og ophør.....	9
14. Kontaktpersoner hos den dataansvarlige og databehandleren .....	10
Bilag A: Oplysninger om behandlingen .....	11
Bilag B: Underdatabehandlere .....	13
Bilag C: Instruks vedrørende behandling af personoplysninger .....	15
Bilag D: Parternes regulering af andre forhold .....	19

## 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. Parterne har indgået en abonnementsaftale om den Dataansvarliges brug af FarPays Applikation ("Ydelserne").
4. I forbindelse med leveringen af Ydelserne behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
5. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
6. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
7. 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.
8. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
9. 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.
10. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
11. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
12. 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<sup>1</sup> nationale ret og disse Bestemmelser.

---

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

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.
3. Hvis databehandleren er af den opfattelse, at udførelsen af instruksen fra den dataansvarlige højst sandsynlig vil være i strid med gældende lovgivning, skal databehandleren straks underrette den dataansvarlige herom. Hvis den dataansvarlige fastholder, at instruksen er i overensstemmelse med gældende lovgivning og fastholder, at instruksen skal udføres, kan databehandleren udføre instruksen uden at ifalde ansvar overfor den dataansvarlige, ligesom den dataansvarlige skal friholde databehandleren fra eventuelle tredjemands krav, herunder krav fra de registrerede, som følge af den udførte instruks. Fortrolighed
4. 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.
5. 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.

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 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 30 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 Be-

stemmelser, 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. Hvis en global leverandør, såsom Microsoft, Google eller amazone, anvendes som underdatabehandler, accepterer den dataansvarlige, at det er den globale leverandørs til enhver tid gældende vilkår der er aftalt mellem parterne, som er grundlag for den globale leverandørs behandling af den dataansvarliges data, herunder i relation til krav til inspektion, audit, kontrol og dokumentation samt ansvar. Link til de seneste vilkår for disse underdatabehandlere findes på underdatabehandlerens hjemmeside.
6. 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.
7. Databehandleren skal i sin aftale med underdatabehandleren indføre 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.
8. 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.

## 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 standardkontraktbestemmelser 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. indsigtretten
  - 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 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 at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
    - b. den dataansvarliges 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. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de på-

tænkte 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.

## 9. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt 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 48 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 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.

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



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

## 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. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

## 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 skriftligt varsel af begge parter.

## 5. Underskrift

### På vegne af den dataansvarlige

Navn: \_\_\_\_\_

Stilling: \_\_\_\_\_

Telefon: \_\_\_\_\_

E-mail: \_\_\_\_\_

Underskrift: \_\_\_\_\_

### På vegne af databehandleren

Navn: Sámal Samuelson

Stilling: Direktør

Telefon: (+45) 71 99 33 55

E-mail: sasa@farpay.dk

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: \_\_\_\_\_

Telefon: \_\_\_\_\_

E-mail: \_\_\_\_\_

### På vegne af databehandleren

Navn: Jákup Martin Vandsdal

Stilling: Økonomi- og administrationschef

Telefon: (+45) 81 95 39 69

E-mail: jmv@farpay.dk

## Bilag A: Oplysninger om behandlingen

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

Databehandleren stiller en cloud-baseret software løsning (Applikationen/Ydelsen) til rådighed for den Dataansvarlige til dennes brug for automatiseret dataintegration vedrørende udstedelse af fakturaer, opkrævning og modtagelse af betalinger, herunder afsendelse, monitorering og bogføring af fakturaer til kunder, samt automatiseret dataintegration og bogføring ved den Dataansvarliges modtagelse af betalinger fra dennes debitorer, uanset den af debitorerne anvendte betalingsløsning. Applikationen omfatter desuden visse integrerede tilvalgsmoduler, så som et faktureringsmodul og et abonnementsbetalingsmodul.

Den Dataansvarlige kan ligeledes instruere Databehandleren i at modtage den Dataansvarliges kunders betalingserviceaftaler fra betalingsformidlere for at sikre, at de anvendte oplysninger om den Dataansvarliges kunders forhold er opdaterede, når den Dataansvarlige bruger Applikationen.

Brug af Applikationen sker ved den Dataansvarliges egen brug af denne (dvs. selvbetjening via et bruger ID og adgangskode), hvorfor Databehandleren ikke egenhændigt udfører databehandling på Applikationen. Databehandleren tilbyder derudover, eller vil tilbyde, visse yderligere tilvalgsmoduler, som den Dataansvarlige mod yderligere betaling kan tilvælge til sit abonnement.

Ved tilvalg af sådanne yderligere moduler gælder denne Databehandlersaftale tillige sådanne ydelser og udtrykket Applikationen skal læses som også omfattende de tilvalgte moduler.

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

Databehandleren indsamler, opbevarer, analyserer og bruger den Dataansvarliges og dennes kunders personoplysninger til at sende fakturaer og modtage betalingsinformation fra betalingsformidlere og videregive informationen til den Dataansvarlige

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

Typer af personoplysninger, der behandles i sammenhæng med levering af ydelsen.

- Navn
- Adresse
- Telefonnr.
- E-mail
- CPR-nummer
- CVR-nummer
- Bankkonti til brug for Applikationen
- Bankkonti eller kreditkort eller betalings-ID for andre betalingsløsninger til brug for betalinger (ikke kortnummeret (PAN))
- Betalingservice oplysninger

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

- Den Dataansvarliges kunder (såfremt disse efter databeskyttelsesreglerne anses som en fysisk person)

- Den Dataansvarliges kunders medarbejdere
- Den Dataansvarlige (såfremt den Dataansvarlige efter databeskyttelsesreglerne anses som en fysisk person)
- Den Dataansvarliges medarbejder

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

Varigheden af behandlingen følger i krafttræden og ophør af parternes hovedaftale.

## Bilag B: Underdatabehandlere

### B.1. Godkendte underdatabehandlere

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

Navn	Produkter	Hosting lokation	Behandlingsaktivitet
Microsoft Ireland Operations Ltd One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521 Irland CVR: DK20812842	Azure hosting  Office 365	EU	Microsoft Azure anvendes til at opbevare og behandle alle oplysninger i FarPay systemet. Data opbevares og behandles kun indenfor EU's grænser.  Office 365 anvendes som BackOffice system internt i FarPay.
Visma e-conomic A/S Gærtorvet 1-5 1799 København V CVR: 29403473	Regnskabssystem	EU	FarPay anvender e-conomic som internt regnskabssystem.
SMTP2GO EPIC Centre 96-106 Manchester Street Christchurch 8011 New Zealand	E-mail gateway	EU	Forsendelse af faktura- og notifikationsmails.
Sproom A/S Visma e-conomic a/s Gærtorvet 1-5 1799 København V CVR: 29403473	EAN-fakturering	EU	EAN-fakturaer sendes og modtages via Sproom.
Intercom 18-21 St. Stephen's Green Dublin 2, Ireland CVR: IE3273393EH	Support og chat	EU	Kunder hos FarPay har mulighed for at få support gennem Intercom chat klienten (ikke slutbrugere/kunders kunder).
Styr Sp/f Undir Bryggjubakka 13 FO-100 Tórshavn CVR-nr.: 594377	Implementering og 2'nd level support af Business Central integration	Ingen	Konsulentydelse ifm. implementering af FarPay Extension til MS Business Central. 2nd level support af samme løsning
FarPay Sp/F Skansavegur 1 FO-110 Tórshavn CVR: 607525	FarPay	EU	Drift, udvikling, vedligehold og support.
QuickPay ApS Dagmar Petersens Gade 104 8000 Aarhus C Danmark CVR-nr. 21822434	Betalingskort Gateway (PSP)	EU	Gennemfører kortbetalingstransaktioner og gemmer kortoplysninger.  Der gemmes ingen persondata, kun kort-data.
MobilePay A/S Vester Søgade 10, 6. 1601 København V Danmark CVR-nr. 26045231	Betalingsløsninger: MobilePay Invoice MobilePay Subscriptions	EU	Håndterer betalingsaftaler, gennemfører betalingstransaktioner, og gemmer kort- og bankkontooplysninger.
Mastercard Payment Services Arne Jacobsens Allé 13 2300 København S Danmark CVR-nr. 40695869	Betalingsløsninger: Betalingservice og Leverandørservice.	EU	Håndterer betalingsaftaler og gennemfører automatiske betalinger med Betalingservice og Leverandørservice.
PostNord Strålfors A/S Hedegaardsvej 88 2300 København S Danmark CVR-nr. 10068657	Print og kuvertering	EU	Print og kuvertering af fysiske breve, som sendes til den Dataansvarliges kunder.
HubSpot HubSpot Ireland Limited One Dockland Central Guild Street, Dublin 1 Irland	CRM-system	EU	Registrering af kunder og potentielle kunder/kontaktpersoner, i forbindelse med salg og markedsføring.

Atlassian Jira Ltd Level 6 341 George St. Sydney NSW 2000 Australia	Supportsystem	EU	Registrering og styring af supportsager, når kunder henvender sig til FarPay.  (Ikke slutbrugere/kunders kunder).
Clearhaus A/S P. O. Pedersens Vej 14 8200 Aarhus Danmark CVR-nr. 33749996	Kortindløsning	EU	Registrering af kortindløsningsaftaler.
Swedbank Kalvebod Brygge 45 1560 København V Danmark CVR-nr. 28487150	Kortindløsning	EU	Registrering af kortindløsningsaftaler.

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

Varslingsperioden for godkendelse af underdatabehandlere fremgår af Bestemmelse 6.3.

## 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:

Behandling sker i henhold til denne aftale, jf. og Bilag A.2. En behandling kan omfatte enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, søgning, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse herunder support.

### C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Sikkerhedsniveauet afspejler et højt sikkerhedsniveau, som afspejler de typer af data, der behandles. Tekniske og organisatoriske foranstaltninger er implementeret i henhold til ISO 27001/ISO27701-standarderne, og kontroller herfra er implementeret og efterleves. ISO27701 er implementeret så den dækker den til enhver tid gældende databeskyttelsesforordningen (GDPR)

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

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

#### C.2.1 Fysisk sikkerhed

Brand, strømafbrydelser, oversvømmelser m.v.

Der skal sikres på sædvanlig vis mod brand og således, at driften kan fortsætte, også ved strømafbrydelser ser af en vis varighed, ligesom der er beskyttet på sædvanlig vis mod oversvømmelse. Når udstyr og mobile enheder ikke anvendes, skal udstyret og enhederne være låst og/eller låst inde. Der skal være udarbejdet en Disaster & Recovery plan (DRP) som omhandler fysisk sikkerhed.

#### C.2.2 Teknisk sikkerhed

Firewalls og antivirus mm.

Databehandleren skal sørge for, at alle arbejdsmaskiner og servere er udstyret med antivirus software med henblik på at blokere vira, malware m.v. Netværket skal være placeret bag firewalls for at kunne beskytte netværket mod uautoriseret adgang.

#### C.2.3 Kryptering

Databehandleren skal sørge for, at al kommunikation af følsomme personoplysninger sker over sikre forbindelser. Følsomme personoplysninger, der overføres uden for et lukket netværk kontrolleret af Databehandleren, skal beskyttes med kryptering.

#### C.2.4 Lagring af data og backup

Databehandleren skal rutinemæssigt sikkerhedskopiere personoplysningerne. Kopierne skal opbevares adskilt og forsvarligt, så personoplysningerne kan genskabes. Backup skal være krypteret.

## C.2.5 Organisatorisk sikkerhed

### Adgangsrettigheder

Databehandleren skal sikre, at medarbejdere hos Databehandleren alene har adgang til de systemer, der er relevante for den enkelte medarbejder.

Alle ansatte skal have unikke brugernavne og passwords. Brugernavne og passwords skal oprettes og ændres efter alment anerkendte principper. Så vidt det er muligt skal der benyttes 2FA/MFA til indlogning og verificering.

## C.2.6 Fortrolighed

Alle medarbejdere hos Databehandleren, der har adgang til personoplysninger, skal være underlagt for troldighedsaftaler.

## C.2.7 Sletning og kassation

### IT-lagermedier

Harddiske og øvrige lagermedier, der udgår fra driften, skal destrueres på en måde, så det ikke er muligt at genetablere data. Alle genbrugte diske skal formateres i overensstemmelse med gældende branche standarder.

## C.2.8 Logning

Alle indlogninger skal logges. Ændringer der vedrører behandling af persondata skal logges. Der skal være en aktiv systemlog på alle endpoint enheder samt servere.

## 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:

Databehandleren har udpeget en person, der er dedikeret til at svare på anmodninger vedrørende personoplysninger. Databehandleren har implementeret en proces til håndtering af sådanne forespørgsler under hensyntagen til eksisterende lovkrav med hensyn til rettidigt svar.

## C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i henhold denne aftale hvorefter de slettes hos databehandleren.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 10/11.1, 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 Lokaltet 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 persondata sker på databehandlerens adresser, samt hos de anførte underdatabehandlere. Derudover kan der udføres remote arbejde i overensstemmelse med databehandlerens politik for remote arbejde.



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

Der overføres ikke personoplysninger til tredjelande

Hvis den dataansvarlige 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 den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren**

Databehandleren skal hvert år for egen regning indhente en certificering fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af certifikat kan anvendes i overensstemmelse med disse Bestemmelser:

**ISO27001 svarende til ISAE3402**

**ISO27701 svarende til ISAE3000**

Såfremt der ønskes udarbejdet en ISAE3000 eller ISAE3402 revisorerklæring sker dette for den dataansvarliges regning.

Certifikatet fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i auditeringen og kan i sådanne tilfælde anmode om en ny auditering for egen regning under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af auditeringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt og med minimum 30 dages varsel.”

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

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

Databehandleren skal en gang årligt for egen regning indhente en revisorerklæring/certificering/inspektionsrapport fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisorerklæringer/Certificering/inspektionsrapporter

kan anvendes i overensstemmelse med disse bestemmelser:

**ISO27001**

**ISO27701**

**ISAE3402**

**ISAE3000**

**SOC 2**

Ovenstående rapporter fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden og kan i sådanne tilfælde anmode om en ny rapport under andre rammer og/eller under anvendelse af anden metode for egen regning

Baseret på resultaterne af rapporten, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

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

Dokumentation for sådanne inspektioner fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.”

Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.”

## **Bilag D: Parternes regulering af andre forhold**

Øvrige forhold reguleres i hovedaftalen mellem parterne.