Databehandleraftale

Start med at downloade databehandleraftalen. Åbn derefter PDF'en, udfyld alle felter herunder, sæt jeres underskrift på side 10, og send et eksemplar til support@farpay.dk.

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

Standardkontraktsbestemmelser

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

CVR-nr.

("Kunden" eller den "Dataansvarlige")

Og

FarPay ApS
Wildersgade 10B, 2.
1408 København K
CVR-nr. 37295043

("FarPay" eller "Databehandleren")

Parterne har aftalt følgende standardkontraktsbestemmelser (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

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 af omfattet af Bestemmelserne.

11. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge par- ter.

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[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.

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.

5. Fortrolighed

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

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de

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

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 til- fælde 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 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 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 databeskyttelses-forordningen.

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 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.

10. Underretning om brud på persondatasikkerheden

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

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 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 persondatasikker- heden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette eller anonymisere alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet eller anonymiseret.

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 dataansvar- lige eller en anden revisor, som er bemyndiget af den dataansvarlige.

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

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 friheds- rettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

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

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssig- heder 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		**På vegne af databehandleren**	
Navn:		Navn:	Rasmus O. Christensen
Stilling:		Stilling:	Direktør
Telefon:		Telefon:	(+45) 2118 93 45
E-mail:		E-mail:	roc@farpay.dk
Underskrift:		Underskrift:	

15. 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		**På vegne af databehandleren**	
Navn:		Navn:	Jákup Martin Vandsdal
Stilling:		Stilling:	COO
Telefon:		Telefon:	(+45) 81 95 39 69
E-mail:		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 betalingsserviceaftaler 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 Databehandleraftale 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

I forbindelse med leveringen af ydelsen kan følgende typer af personoplysninger blive behandlet afhængigt af de konkrete omstændigheder:

- 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))
- Betalingsservice oplysninger
- Religiøse eller fagforeningsmæssige tilhørsforhold

Bemærk, at ikke alle oplysninger nødvendigvis behandles i alle tilfælde, men kun når det er relevant for den specifikke ydelse.

Databehandleren må kun behandle særlige kategorier af personoplysninger efter særskilt, skriftlig instruks fra den dataansvarlige. Den dataansvarlige garanterer gyldigt behandlingsgrundlag efter GDPR art. 9 og stiller dokumentation til rådighed på anmodning.

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 medarbejdere
- Den Dataansvarliges kunders kunder (Såfremt den Dataansvarlige betegnes som "Reseller" af FarPay systemet)

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

Varigheden af behandlingen følger ikrafttræden og ophør af parternes hovedaftale.

Bilag B: Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere, som bistår databehandleren i forbindelse med levering af ydelser i henhold til hovedaftalen:

Navn	Produkter	Hosting lokation	Behandlingsaktivitet
Microsoft Ireland Operations Ltd One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521 Irland CVR: IE8256796U	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.
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.
Stýr Sp/f Undir Bryggjubakka 13 FO-100 Tórshavn CVR-nr.: 594377	MS Business Central integration	Ingen	Konsulentydelser ifm. implementering af FarPay Extension til MS Business Central. 2nd level support af løsningen
FarPay Sp/F Skansavegur 1 FO-110 Tórshavn CVR: 607525	FarPay	EU	Drift, udvikling, vedligeholdelse og support.
QuickPay ApS Dagmar Petersens Gade 104 8000 Aarhus C Danmark CVR-nr. 21822434	Betalingskort Gate- way (PSP)	EU	Gennemfører kortbetalingstransaktioner og gemmer kortoplysninger (abonnement). Der gemmes ingen persondata, kun kortdata. PCI DSS standarden, som QuickPay er underlagt og opererer i henhold til er beskrevet her: https://quickpay.net/dk/helpdesk/pci/
PostNord Strålfors A/S Hedegaardsvej 88 2300 København S Danmark CVR-nr. 10068657	Print, kuvertering og forsendelse	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. Registrering og styring af supportsager, når kunder henvender sig til FarPay *(ikke slutbrugere/kunders kunder)*.
e-Boks Nordic A/S Hans Bekkevolds Allé 7 2900 Hellerup Danmark CVR-nr. 25674154	e-Boks ISV Integration Service	EU	Integration med e-Boks-platformen til sikker digital distribution af dokumenter til slutbrugere/kunder.

Databehandleren garanterer, at samtlige underdatabehandlere, som anført i tabellen ovenfor, er kontraktligt forpligtet til at overholde databeskyttelsesforordningen og har påtaget sig mindst de

samme databeskyttelsesforpligtelser, som følger af denne aftale, jf. artikel 28, stk. 4.

B.2. Opdatering af Bilag B

Databehandleren forpligter sig til at opdatere Bilag B løbende og straks orientere den dataansvarlige om planlagte tilføjelser eller væsentlige ændringer hos underdatabehandlere, herunder ændringer i sikkerhedsforanstaltninger. Den dataansvarlige kan føre indsigelse inden 30 dage efter meddelelse i henhold til Bestemmelse 7.3

Bilag C: Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks
Databehandleren behandler personoplysninger på vegne af den dataansvarlige med henblik på levering af de ydelser, der er beskrevet i hovedaftalen og Bilag A.2. Behandlingen omfatter enhver aktivitet i henhold til GDPR artikel 4(2), herunder, men ikke begrænset til, indsamling, registrering, organisering, opbevaring, tilpasning, søgning, brug, videregivelse, sletning og tilintetgørelse. Behandlingen udføres udelukkende i overensstemmelse med den dataansvarliges dokumenterede instruks, jf. GDPR artikel 28(3)(a).

C.2. Behandlingssikkerhed
Databehandleren sikrer et højt sikkerhedsniveau i overensstemmelse med kravene i GDPR artikel 32. Tekniske og organisatoriske foranstaltninger er implementeret i overensstemmelse med ISO/IEC 27001 og ISO/IEC 27701-standarderne og dækker bl.a. fysisk og logisk adgangskontrol, netværkssikkerhed, kryptering, sletningsrutiner, logning og hændelseshåndtering. Databehandleren er ansvarlig for at evaluere og opdatere sikkerhedsforanstaltningerne løbende og for at kunne dokumentere efterlevelse over for den dataansvarlige.

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 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
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. Enhver adgang via et ikke-sikret netværk, f.eks. fjernopkobling via internet, skal sikres med multifactor authentication (2FA/MFA).

MFA kan være one-time passcode, app.authentication, client certificate eller anden tilsvarende teknologi i kombination med brugernavn og kodeord.

C.2.6 Fortrolighed
Alle medarbejdere hos Databehandleren, der har adgang til personoplysninger, skal være underlagt fortrolighedsaftaler.

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 branchestandarder.

C.2.8 Logning
Alle ind- logninger skal logges. Ændringer der vedrør behandling af persondata skal logges. Der skal være en aktiv systemlog på alle endpoint enheder samt servere.

C.3 Bistand til den dataansvarlige
Databehandleren bistår den dataansvarlige i opfyldelsen af forpligtelserne efter GDPR kapitel III og artiklerne 32–36, herunder håndtering af registreredes rettigheder, sikkerhedsbrud (art. 33–34) og konsekvensanalyser (art. 35–36), jf. artikel 28(3)(f). Databehandleren har udpeget en kontaktperson og implementeret en proces, der sikrer rettidig og effektiv håndtering af sådanne forespørgsler, jf. EDPB Guidelines 07/2020, pkt. 101.

Databehandleren stiller en kontaktperson til rådighed og besvarer anmodninger uden unødig forsinkelse og senest 10 arbejdsdage efter modtagelse.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares kun så længe det er nødvendigt for opfyldelsen af formålene med behandlingen i henhold til hovedaftalen. Ved ophør af aftalen slettes eller returneres personoplysningerne til den dataansvarlige uden unødig forsinkelse, i overensstemmelse med bestemmelsen 11.1, og senest 90 dage efter ophør, medmindre andet er aftalt skriftligt. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling
Behandling af personoplysninger finder sted på databehandlerens lokationer inden for EU/EØS samt hos de underdatabehandlere, der fremgår af Bilag B.1. Fjernarbejde udføres i overensstemmelse med databehandlerens interne sikkerhedspolitikker, herunder adgangsbegrænsning og kryptering. Der sker ikke behandling på andre lokaliteter uden forudgående skriftligt samtykke fra den dataansvarlige.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Databehandleren overfører som udgangspunkt ikke personoplysninger til lande uden for EU/EØS i forbindelse med levering af tjenesten. Al primær behandling og lagring finder sted inden for EU/EØS.

Databehandleren anvender dog visse underdatabehandlere, der er globalt ejede virksomheder med hjemsted i tredjelande. Et eksempel herpå er Microsoft (Se nærmere oplysninger i Bilag B, hvor alle

underdatabehandlere, deres lokationer og overførselsgrundlag fremgår). Microsoft opbevarer kundedata i EU-datacentre, men da moderselskabet har hovedsæde i USA, kan det ikke udelukkes, at medarbejdere uden for EU/EØS (f.eks. i USA) får fjernadgang til personoplysninger som led i support eller vedligehold.

Databehandleren understreger, at der ikke sker aktiv, vedvarende eksport af personoplysninger til tredjelande; oplysningerne forbliver lagret i EU/EØS. Muligheden for fjernadgang anses dog juridisk som en overførsel til tredjeland (jf. GDPR art. 44 og EDPB Guidelines 05/2021, pkt. 19 og eksempel 7), selvom data ikke fysisk forlader EU/EØS. Sådanne overførsler sker kun, når det er strengt nødvendigt, og alene med henblik på driftsmæssig support, fejlfinding eller tilsvarende.

Databehandleren sikrer, at enhver adgang til personoplysninger fra tredjelande sker i overensstemmelse med GDPR kapitel V og alene på grundlag af gyldige overførselsmekanismer, herunder EU-Kommissionens Standardkontraktbestemmelser eller tilstrækkelighedsbeslutninger i henhold til artikel 45. Databehandleren gennemfører, hvor relevant, en overførselsvurdering (TIA) og iværksætter supplerende tekniske og organisatoriske foranstaltninger i overensstemmelse med Schrems II-dommen (C-311/18) og EDPB's Anbefalinger 01/2020, herunder kryptering, adgangskontrol og principper om "need-to-know".

Underdatabehandlere med forbindelse til tredjelande er kontraktligt forpligtet til at implementere tilsvarende beskyttelsesforanstaltninger, for at minimere og kontrollere eventuel fjernadgang.

Databehandleren fører løbende kontrol med disse foranstaltninger og er forpligtet til på anmodning og uden unødig forsinkelse at fremlægge dokumentation herfor, herunder en opdateret liste over alle underdatabehandlere, deres lokationer, behandlingsaktivitet og det anvendte overførselsgrundlag, hvis relevant, (jf. Bilag B.1).

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

Databehandleren skal én gang årligt og for egen regning indhente en uafhængig tredjepartscertificering, som dokumenterer overholdelsen af databeskyttelsesforordningen, anden relevant EU-ret eller national lovgivning samt denne databehandleraftale.

Parterne er enige om, at følgende certificeringer anses som fyldestgørende dokumentation:

- **ISO/IEC 27001** (eller tilsvarende ISAE 3402 type II for informationssikkerhed)
- **ISO/IEC 27701** (eller tilsvarende ISAE 3000 for databeskyttelse og GDPR)

Såfremt den dataansvarlige specifikt ønsker en ISAE 3000- eller ISAE 3402-erklæring udarbejdet, sker dette for den dataansvarliges egen regning.

Certificeringen eller erklæringen skal uden unødig forsinkelse fremsendes til den dataansvarlige. Hvis den dataansvarlige har væsentlige indsigelser mod metodik eller omfang, kan vedkommende anmode om en ny revision under andre forudsætninger, dog for egen regning.

På baggrund af revisionens resultater er den dataansvarlige berettiget til at anmode om, at databehandleren implementerer yderligere relevante foranstaltninger, i det omfang det er nødvendigt for at sikre overholdelse af databeskyttelsesreglerne og denne aftale.

Den dataansvarlige, eller dennes bemyndigede repræsentant, har derudover ret til at gennemføre inspektioner, herunder fysiske inspektioner, på de lokaliteter, hvor databehandleren foretager behandling af personoplysninger. Dette omfatter både fysiske faciliteter og systemer, som anvendes

til eller i forbindelse med behandlingen.
Sådanne inspektioner skal varsles med minimum 30 kalenderdage og kan kun foretages, når den dataansvarlige har en sagligt begrundet anledning hertil.

Eventuelle omkostninger, som den dataansvarlige pådrager sig i forbindelse med sådanne inspektioner, afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til loyalt at bistå med rimelige ressourcer, navnlig i form af den nødvendige tid og adgang, for at inspektionen kan gennemføres effektivt.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere
Databehandleren er forpligtet til at sikre, at alle underdatabehandlere, som behandler personoplysninger på vegne af den dataansvarlige, overholder databeskyttelsesforordningen samt de forpligtelser, som følger af denne aftale.

Med henblik på dette gælder følgende bestemmelser:

C.8.1 Tredjepartsrevisionsrapporter og certificeringer
Databehandleren skal sikre, at relevante underdatabehandlere løbende indhenter og opretholder anerkendte tredjepartsrevisionsrapporter eller certificeringer, der dokumenterer overholdelse af gældende databeskyttelseskrav.

Følgende certificeringer anses som acceptable:
- **ISO/IEC 27001** (eller tilsvarende ISAE 3402 type II for informationssikkerhed)
- **ISO/IEC 27701** (eller tilsvarende ISAE 3000 for databeskyttelse og GDPR)

Dokumentation for sådanne certificeringer skal kunne fremvises for den dataansvarlige uden unødig forsinkelse ved anmodning.

C.8.2 Gennemsigtighed og kontrol
Databehandleren skal efter anmodning dokumentere over for den dataansvarlige, at der er indgået databehandleraftaler med underdatabehandlere, og at disse indeholder krav, der som minimum svarer til de forpligtelser, der følger af denne aftale.

C.8.3 Ret til inspektion
Hvis den dataansvarlige har en berettiget grund til at betvivle en underdatabehandlers overholdelse af sine forpligtelser, kan den dataansvarlige anmode om, at databehandleren gennemfører en særskilt inspektion hos den pågældende underdatabehandler.

Inspektionen skal foretages uden unødig forsinkelse og dokumenteres skriftligt.
Inspektionsrapporten fremsendes til den dataansvarlige, så snart den foreligger.

C.8.4 Dataansvarliges ret til deltagelse
Såfremt den dataansvarlige vurderer, at en inspektion gennemført af databehandleren ikke giver tilstrækkelig indsigt eller sikkerhed, kan den dataansvarlige, i samarbejde med databehandleren og for egen regning, anmode om selv at deltage i en inspektion hos underdatabehandleren.

C.8.5 Omkostningsfordeling

Databehandleren afholder egne omkostninger i forbindelse med almindelige inspektioner og audits af underdatabehandlere. Hvis den dataansvarlige anmoder om udvidede eller gentagne inspektioner, eller ønsker at deltage i en sådan inspektion, afholder den dataansvarlige selv de hermed forbundne omkostninger, medmindre andet er skriftligt aftalt.

Bilag D: Parternes regulering af andre forhold

Øvrige forhold reguleres i hovedaftalen mellem parterne.