STANDARDKONTRAKTSBESTEMMELSER

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

mellem

Navn: _____

CVR: _____

Adresse: _____

Post nr. og by: _____

Danmark

herefter "den dataansvarlige"

og

Aqoola A/S
CVR 32073506
Agern Allé 5A
2970 Hørsholm
Danmark

herefter "databehandleren"

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

HAR AFTALT følgende standardkontraktsbestemmelser ("Bestemmelserne") med henblik på at overholde databeskyttelsesforordningen ("databeskyttelsesforordningen" eller "GDPR") og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. Indhold

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af tjenester, jf. bilag A.1, behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

1 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.

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 pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 60 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   c. indsigtsretten
   d. retten til berigtigelse
   e. retten til sletning ("retten til at blive glemt")
   f. retten til begrænsning af behandling
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

   c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

   d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

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

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

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

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er 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.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift 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	På vegne af databehandleren
Underskrift	*Underskrift*
Navn:	Navn: Niels Legaard Christensen
Stilling:	Stilling: COO
Telefonnummer: +45	Telefonnummer: +45 31378818
E-mail:	E-mail: nlc@aqoola.com

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.

Part	Navn	Stilling	Telefonnummer	E-mail
Dataansvarlig			+45	

Databehandler	Ali Dogan Karatas	DPC	+45 24601811	aka@aqoola.com

Bilag A Oplysninger om behandlingen

Behandlingen af personoplysninger foretages med det formål at muliggøre levering, drift, vedligeholdelse og support af de tjenester, som fremgår af parternes aftale om brugen af Aqoola Workflow-platformen (**"Hovedaftalen"**), jf. også tabellen nedenfor. Databehandlingen sker i overensstemmelse med databeskyttelsesforordningen samt lov nr. 502 af 23. maj 2018 ("Databeskyttelsesloven" eller "DBL"). Hovedaftalen indeholder specifikation af, hvilke tjenester den dataansvarlige har valgt, og databehandleraftalen regulerer til enhver tid de ydelser, som fremgår heraf. Hvis den dataansvarlige efterfølgende tilføjer eller fravælger én eller flere moduler eller licenser, forbliver databehandleraftalen i kraft og anses som automatisk tilpasset.

Behandlingen varer, så længe databehandleren leverer de pågældende tjenester til den dataansvarlige i henhold til Hovedaftalen, og ophører ved endeligt ophør af samarbejdet, hvorefter personoplysninger slettes eller tilbageleveres i henhold til Bestemmelsernes punkt 11.1, jf. Bilag C.4.

Tjeneste(r)	**Karakteren af behandlingen**	**Typer af personoplysninger**			**Kategorier af registrerede**
		GDPR art. 6	*DBL § 8 og § 11*	*GDPR art. 9*	
Aqoola Workflow	Indsamling, opbevaring, overvågning, backup, vedligehold, organisering, systematisering, facilitering, fejlfinding, kryptering, tilpasning eller ændring, genfinding, søgning, brug, sammenstilling, samkøring, sletning	Navn, e-mailadresse, telefonnummer, adresse, stillingsbetegnelse, initialer/login.	CPR-nr.		Medarbejdere og eksterne leverandører
Contract Management	Indsamling, opbevaring, overvågning, backup, vedligehold, organisering, systematisering, facilitering, fejlfinding, kryptering, tilpasning eller ændring, genfinding, søgning, brug, sammenstilling, samkøring, sletning	Navn, e-mailadresse, telefonnummer, adresse, stillingsbetegnelse, initialer/login.	CPR-nr.		Medarbejdere og eksterne leverandører
Expense Management	Indsamling, opbevaring, overvågning, backup, vedligehold, organisering, systematisering, facilitering, fejlfinding, kryptering, tilpasning eller ændring, genfinding, søgning, brug, sammenstilling, samkøring, sletning	Navn, e-mailadresse, telefonnummer, adresse, stillingsbetegnelse, initialer/login.	CPR-nr.		Medarbejdere og eksterne leverandører

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

Navn	CVR/SE nr.	Adresse	Beskrivelse af behandling	Typer af personoplysninger			Tjeneste(r)
				GDPR art. 6	*DBL § 8 og § 11*	*GDPR art. 9*	
Formula Micro Bornholm A/S	14798684	Lillevangsvej 6 3700 Rønne, Danmark	Hosting af tjenesterne, herunder den dataansvarliges personoplysninger	Navn, e-mailadresse, telefonnummer, adresse, stillingsbetegnelse, initialer/login.	CPR-nr.		Aqoola Workflow Contract Management Expense Management
Paperflow ApS	37035785	Dampfærgevej 8, 2. 2100 København Ø, Danmark	Automatiseret scanning og behandling af den dataansvarliges fakturaer, kvitteringer og kreditnotaer.	Firma e-mailadresse			Aqoola Workflow Expense Management
mySupply ApS	25894375	Peter Løths Vej 2 9440 Aabybro, Danmark	Levering af VAX 360, så den dataansvarlige kan udveksle og opbevare forretningsdokumenter og meddelelser med tredjeparter, f.eks. kunder.	Navn, e-mailadresse, telefonnummer, adresse, stillingsbetegnelse, initialer/login.	CPR-nr.		Aqoola Workflow

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse, jf. Bestemmelsernes pkt. 7.3 – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

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 leverer, drifter, vedligeholder og yder support på Aqoola Workflow-platformen samt tilhørende moduler og integrationer, jf. Bilag A.1 og A.2.

Tjeneste(r)	Behandlingens genstand/instruks
Aqoola Workflow	Digital behandling og godkendelse af kreditorbilag og fakturaer, herunder workflowstyring, integration til økonomisystemer, adgangsstyring, logning og support.
Contract Management	Registrering, vedligeholdelse og overvågning af kontrakter, herunder opfølgning på udløb og fornyelse samt tildeling af ansvarlige brugere.
Expense Management	Registrering og behandling af medarbejderudlæg, herunder upload af bilag, godkendelsesflow og integration til økonomisystemer for bogføring og refusion.

Databehandleren udfører alene behandling efter dokumenteret instruks fra den dataansvarlige og i det omfang, det er nødvendigt for at opfylde forpligtelserne i Hovedaftalen.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. Som følge heraf har den dataansvarlige og databehandleren begge udarbejdet en risikoanalyse vedrørende databehandlingen og er enige om de foranstaltninger som er beskrevet i det følgende:

Behandlingen omfatter følgende antal registrerede:	☒ 1-100 ☒ 101-1000 ☒ 1001-5000 ☐ 5001-10000 ☐ Over 10000

Behandlingen omfatter behandling af følgende typer personoplysninger:		☒ GDPR art. 6 ☒ DBL § 8 og § 11 ☐ GDPR art. 9	
Over 10000			
5001-10000			
1001-5000			
101-1000			
1-100			
	GDPR art. 6	**DBL § 8 og § 11**	**GDPR art. 9**

På baggrund af ovenstående matrix etableres følgende sikkerhedsniveau:

	Lavt	**Middel**	**Højt**
	Grøn	**Gul**	**Rød**
	☐	☒	☐

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:

Kontrolmål	**Implementerede sikkerhedsforanstaltninger**
Efterlevelse af instruks i henhold til databehandleraftalen	- Databehandleren har skriftlige procedurer, der fastslår, at behandling af personoplysninger kun må ske efter skriftlig instruks fra den dataansvarlige. Procedurerne opdateres mindst én gang årligt og ved væsentlige ændringer. Ledelsen fører kontrol med efterlevelsen, bl.a. via stikprøver, og der er etableret en proces for vurdering af instruksers lovlighed. Hvis en instruks vurderes at være i strid med databeskyttelseslovgivningen, underrettes den dataansvarlige straks.
Teknisk behandlingssikkerhed	- Databehandleren har skriftlige procedurer for tekniske sikkerhedsforanstaltninger, som opdateres mindst én gang årligt. På baggrund af risikovurderinger er der implementeret passende tiltag, herunder antivirus, firewall, netværkssegmentering og adgangsstyring. Adgang til personoplysninger er begrænset til brugere med arbejdsbetinget behov, og der foretages regelmæssig gennemgang og deaktivering af adgange. Alle medarbejdere har to-faktor autentifikation (2FA) aktiveret ved

	login til relevante systemer og enheder. Dette gælder både ved lokal adgang og fjernadgang, og anvendelsen af 2FA er en fast del af den tekniske sikkerhedsarkitektur. - Systemer og databaser er beskyttet med overvågning og alarmering, og hændelser følges op og rapporteres til den dataansvarlige. Logning er aktiveret og sikret mod manipulation. Personoplysninger transmitteres krypteret over åbne netværk, herunder e-mail, ved brug af stærk kryptering baseret på tidssvarende og bredt anerkendte standarder. Derudover krypteres personoplysninger også ved opbevaring (data-at-rest) for at beskytte mod uautoriseret adgang. Al adgang til systemer – uanset om det sker fra kontoret eller fra distancen (f.eks. hjemmearbejde) – foregår via krypteret VPN-forbindelse, og hjemmearbejdspladser er generelt beskyttet på tilsvarende vis som på arbejdspladsen. I udvikling og test anvendes kun pseudonymiserede eller anonymiserede data, medmindre andet er aftalt. - Tekniske foranstaltninger kontrolleres løbende via sårbarhedsscanninger og penetrationstests. Ændringer til systemer foretages efter formaliserede procedurer og inkluderer opdateringer og sikkerhedspatches. Fysisk adgang til behandlingslokationer er begrænset til autoriserede personer med adgangs- og indbrudssikring.
Fysisk adgangssikkerhed	- Fysisk adgang til databehandlerens kontor er begrænset til autoriserede personer via et elektronisk låsesystem. Kun medarbejdere eller personer med legitimt ærinde har adgang, og besøgende må kun opholde sig på kontoret med ledsagelse af en autoriseret medarbejder. Listen over udstedte elektroniske nøgler ajourføres ved medarbejders ansættelse og fratrædelse. Derudover er kontoret placeret i en bygning med fysisk sikring, herunder aflåste døre, brandsikringsudstyr, videoovervågning og alarmanlæg.
Organisatorisk behandlingssikkerhed	- Databehandleren har en ledelsesgodkendt informationssikkerhedspolitik, som er baseret på risikovurdering og ajourføres mindst én gang årligt. Politikken er i overensstemmelse med kravene i databehandleraftaler og kommunikeres til alle relevante medarbejdere. - Ved ansættelse efterprøves medarbejdere ud fra stillingens karakter (fx CV, referencer, evt. straffeattest). Nye medarbejdere underskriver fortrolighedserklæring og introduceres til gældende sikkerhedsprocedurer. Ved fratrædelse deaktiveres adgange rettidigt, og adgangsaktiver inddrages. Fratrådte informeres om fortsat gældende tavshedspligt. - Alle medarbejdere med adgang til personoplysninger gennemfører årlig awareness-træning om informations- og behandlingssikkerhed. Gennemførelse dokumenteres og følges op.

Sletning og tilbagelevering af personoplysninger	- Databehandleren har skriftlige procedurer for opbevaring, sletning og tilbagelevering af personoplysninger i overensstemmelse med aftale og instruks fra den dataansvarlige. Procedurerne opdateres mindst én gang årligt og ved ændringer i behandlingsaktiviteter. - Ved ophør af behandlingsforholdet slettes personoplysninger senest to måneder efter, medmindre andet er aftalt. Sletning eller tilbagelevering udføres efter den dataansvarliges valg, og databehandleren fører dokumentation for gennemførelsen. Der er etableret kontrolmekanismer og stikprøvekontrol, som sikrer korrekt og rettidig håndtering.
Opbevaring af personoplysninger	- Databehandleren har skriftlige procedurer, som sikrer, at personoplysninger kun opbevares i overensstemmelse med den dataansvarliges instruks og databehandleraftalen. Procedurerne opdateres mindst én gang årligt og ved ændringer i behandlingsaktiviteter. - Der føres en opdateret oversigt over behandlingsaktiviteter og opbevaringslokationer, som kun omfatter af den dataansvarlige godkendte lokaliteter. Overholdelsen kontrolleres løbende gennem dokumentation og stikprøver.
Anvendelse og kontrol af underdatabehandlere	- Databehandleren har skriftlige procedurer for anvendelse af underdatabehandlere, som kræver skriftlig aftale og godkendelse fra den dataansvarlige. Procedurerne opdateres mindst årligt. - Der føres en ajourført oversigt over alle godkendte underdatabehandlere med relevante oplysninger. Underdatabehandlere anvendes kun ved specifik eller generel godkendelse, og ændringer meddeles rettidigt til den dataansvarlige. - Underdatabehandleraftaler pålægger samme forpligtelser som databehandleren selv er underlagt. Databehandleren følger løbende op på underdatabehandleres tekniske og organisatoriske foranstaltninger via risikovurderinger, revisionserklæringer eller inspektioner, og orienterer den dataansvarlige om opfølgningen.
Overførsel til tredjelande	- Databehandleren har skriftlige procedurer, der sikrer, at overførsel af personoplysninger til tredjelande eller internationale organisationer kun sker i henhold til aftale eller instruks fra den dataansvarlige og med et gyldigt overførselsgrundlag i henhold til databeskyttelseslovgivningen. Procedurerne opdateres mindst én gang årligt og ved ændringer i regler eller praksis.
Bistand ved registreredes rettigheder	- Databehandleren har skriftlige procedurer, der sikrer bistand til den dataansvarlige ved udlevering, rettelse, sletning, begrænsning og oplysning om behandling af personoplysninger, i det omfang det er aftalt. Procedurerne opdateres mindst én gang årligt.

	- Systemer og databaser understøtter søgning, eksport, redigering og sletning af personoplysninger i overensstemmelse med databeskyttelsesforordningen. Der er etableret interne processer og kontaktpunkter, som sikrer rettidig og korrekt håndtering. Databehandleren dokumenterer gennemførte bistandsopgaver og foretager løbende kvalitetssikring.
Håndtering af sikkerhedsbrud	- Databehandleren har skriftlige procedurer for håndtering og rapportering af brud på persondatasikkerheden i overensstemmelse med databehandleraftalen og gældende lovgivning. Procedurerne opdateres mindst én gang årligt og omfatter krav om hurtig underretning til den dataansvarlige ved brud hos databehandleren eller en underdatabehandler. - Medarbejdere gennemfører årlig træning i identifikation og eskalering af sikkerhedsbrud. Alle hændelser dokumenteres i en hændelsesoversigt, og oplysninger om brud fra underdatabehandlere registreres tilsvarende. - Databehandleren bistår den dataansvarlige ved anmeldelse til Datatilsynet og har procedurer med klare anvisninger på beskrivelse af bruddets karakter, konsekvenser og iværksatte foranstaltninger. Relevante medarbejdere er instrueret og i stand til at assistere uden unødig forsinkelse, og procedurernes funktionalitet er dokumenteret.

Ud over de sikkerhedsforanstaltninger, som databehandleren selv har implementeret, benyttes underdatabehandleren Formula Micro A/S til hosting af tjenesterne, jf. Bilag A.1. Formula Micro A/S er ansvarlig for drift af datacentre, infrastruktur og relaterede systemer, som anvendes til behandling og opbevaring af personoplysninger på vegne af databehandlerens kunder.

Formula Micro A/S har implementeret omfattende tekniske og organisatoriske sikkerhedsforanstaltninger, der dokumenteres via en uafhængig ISAE 3402-erklæring, som revideres årligt. Deres datacentre er placeret i Danmark og lever op til gældende krav til driftssikkerhed, adgangskontrol og databeskyttelse. Formula Micro A/S' sikkerhedssetup evalueres årligt, og databehandleren fører løbende tilsyn via kvartalsvise møder.

Kontrolmål	Implementerede sikkerhedsforanstaltninger (Formula Micro A/S)
Hosting og drift	Alle kundeløsninger hostes i datacentre i Danmark. Behandling sker kun efter instruks fra den dataansvarlige. Tilsyn foretages løbende af databehandleren.
Certificering og dokumentation	ISAE 3402-revisionserklæring dokumenterer sikkerhedsforanstaltninger. Databehandleren afholder kvartalsvise tilsynsmøder.
Netværkssikkerhed og firewall	Både centrale og lokale firewalls opdateres løbende. Al adgang sker via krypterede VPN-forbindelser og TrustGate VPN Firewalls.

Antivirus og malwarebeskyttelse	Alle servere har opdateret antivirus- og antimalwaresoftware samt mail-spamfiltre. Systemerne beskytter mod skadevoldende programmer og opdateres løbende.
Backup og gendannelseskapacitet	Daglig backup foretages til lokal NAS-enhed og ugentlig fuld backup til ekstern, brandsikker og aflåst lokation. Dette sikrer robust datagendannelse ved hændelser eller systemnedbrud.
Kryptering og transmission	Al datakommunikation over internettet foregår krypteret. Personoplysninger beskyttes i transit og ved opbevaring (data-at-rest) i overensstemmelse med gældende standarder.
Fjernadgang og hjemmearbejde	Adgang til systemer, uanset placering, sker via VPN-forbindelser og sikre adgangskontroller, hvilket muliggør sikker behandling af data fra distancen.
Logning og hændelseskontrol	Adgang til og ændringer i personoplysninger logges. Logfiler opsamles centralt, hvor det er muligt, og sikres mod manipulation og sletning. Hændelser registreres og følges op.
Fysisk adgangskontrol	Dobbelte døre med adgangskode, betonvægge, overvågning 24/7, adgang kun for godkendte personer. Alarmanlæg for brand, adgang og fugt.
Driftssikkerhed og overvågning	Driftssystemer er sikret med UPS og nødstrøm. Køleanlæg og brandsikringsudstyr er implementeret. Drift overvåges 24/7, og hændelser afhjælpes straks.

C.3 Bistand til den dataansvarlige

Databehandleren skal bistå den dataansvarlige i overensstemmelse med punkt 9.1 og 9.2 i det omfang, dette er muligt, ved gennemførelse af passende tekniske og organisatoriske foranstaltninger, således at den dataansvarlige kan opfylde sine forpligtelser efter databeskyttelsesforordningens artikel 32–36.
Databehandleren har implementeret og efterlever interne politikker og procedurer, der sikrer, at god sikkerhedspraksis overholdes, og at databehandleren rettidigt kan yde den nødvendige bistand. Dette inkluderer:

- Bistand med at sikre, at de registreredes rettigheder kan opfyldes, herunder indsigt, berigtigelse, sletning, begrænsning, indsigelse og dataportabilitet.
- Hurtig og skriftlig underretning til den dataansvarlige uden unødig forsinkelse, hvis databehandleren eller en underdatabehandler modtager en anmodning direkte fra en registreret.
- Bistand i forbindelse med anmeldelse af brud på persondatasikkerheden, ved at levere de nødvendige oplysninger til brug for den dataansvarliges opfyldelse af sine forpligtelser efter artikel 33 og 34, herunder (i) bruddets karakter, (ii) de sandsynlige konsekvenser og (iii) trufne eller foreslåede afhjælpende foranstaltninger.

- Bistand ved konsekvensanalyser (DPIA) i henhold til artikel 35 og, om nødvendigt, ved forudgående høring af Datatilsynet efter artikel 36.
- Dokumentation og tekniske/organisatoriske foranstaltninger, der understøtter den dataansvarliges overholdelse af sine forpligtelser efter artikel 32–36, herunder gennem foranstaltninger angivet i bilag C.2.

C.4 Opbevaringsperiode/sletterutine

I Hovedaftalens løbetid slettes bilag og anden dokumentation, som den dataansvarlige uploader til tjenesterne, jf. bilag A.1, automatisk efter 5 år fra udgangen af det regnskabsår, materialet vedrører, og senest seks (6) år efter upload-tidspunktet, medmindre andet følger af den dataansvarliges instruks.

Ved ophør af Hovedaftalen, skal databehandleren slette personoplysningerne i overensstemmelse med Bestemmelsernes punkt 11.1.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Navn	CVR/SE nr.	Adresse	Beskrivelse af behandling	Tjeneste(r)
Aqoola A/S	32073506	Agern Alle 5 A, 2970 Hørsholm, Danmark	Leverandør af tjenesterne, jf. Bilag A.1	Aqoola Workflow Contract Management Expense Management
Formula Micro Bornholm A/S	14798684	Lillevangsvej 6 3700 Rønne, Danmark	Hosting af tjenesterne, herunder den dataansvarliges personoplysninger	Aqoola Workflow Contract Management Expense Management
Paperflow ApS	37035785	Dampfærgevej 8, 2. 2100 København Ø, Danmark	Automatiseret scanning og behandling af den dataansvarliges fakturaer, kvitteringer og kreditnotaer.	Aqoola Workflow Expense Management
mySupply ApS	25894375	Peter Løths Vej 2 9440 Aabybro, Danmark	Levering af VAX 360, så den dataansvarlige kan udveksle og opbevare forretningsdokumenter og meddelelser med tredjeparter, f.eks. kunder.	Aqoola Workflow

Behandling af personoplysninger kan også ske via fjernadgang fra databehandlerens medarbejdere, samt hos underdatabehandlernes medarbejdere og eventuelle egne underdatabehandlere, forudsat at adgangen sker under passende tekniske og organisatoriske sikkerhedsforanstaltninger.

De godkendte underdatabehandlere, som er anført i Bilag C.3, må i det omfang det er nødvendigt for levering af tjenesterne, anvende egne underdatabehandlere, såfremt disse er godkendt af databehandleren og i overensstemmelse med kravene i databehandleraftalen og databeskyttelsesforordningens artikel 28, stk. 2 og 4.

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke ske uden for EU/EØS, medmindre dette sker i overensstemmelse med databeskyttelsesforordningens kapitel V og alene efter forudgående skriftlig godkendelse fra den dataansvarlige, jf. Bilag C.6.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Navn	CVR/SE nr.	Adresse	Beskrivelse af behandling	Overførselsgrundlag

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 én gang årligt for egen regning indhente en revisionserklæring 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 revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

- ISAE 3000
- ISAE 3402
- ISO 27001/2
- ISO 27701
- SOC2

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Baseret på resultaterne af erklæringen, 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. 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 eller en repræsentant for databehandleren skal en gang årligt for databehandlerens regning indhente en revisionserklæring eller inspektionsrapport vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Databehandleren bestemmer tilsynsformen af underdatabehandlere, men tilsynsformen skal have fokus på kontrol af den konkrete behandling af personoplysninger, jf. Bilag B.1, som er overladt til den pågældende underdatabehandler.

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

- ISAE 3000
- ISAE 3402
- ISO 27001/2
- ISO 27701
- SOC2

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.

Dokumentationen for tilsynet indgår i databehandlerens revisionserklæring(er). Den dataansvarlige kan på anmodning få udleveret dokumentation for det gennemførte tilsyn med den/de relevante underdatabehandler(e).

Bilag D Parternes regulering af andre forhold

I relation til databehandlerens behandling af personoplysninger på vegne af den dataansvarlige, har parterne aftalt nedenstående supplerende vilkår. De supplerende vilkår i disse Bestemmelser har forrang i forhold til eventuel tilsvarende regulering i Hovedaftalen mellem parterne vedrørende den del af databehandlerens aktiviteter og ansvar der knytter sig til databehandlingen, mens udførelsen af alle andre aktiviteter vedrørende leveringen af aftalte ydelser er underlagt de øvrige dele af Hovedaftalen. Hovedaftalens øvrige vilkår, herunder ansvarsbegrænsninger m.v., er også gældende for databehandlerens opfyldelse af Bestemmelserne.

D.1 Vederlag

Databehandleren yder bistand i overensstemmelse med sine forpligtelser efter denne databehandleraftale og databeskyttelsesforordningen uden særskilt vederlag. I det omfang den dataansvarlige anmoder om bistand, som klart ligger uden for databehandlerens forpligtelser efter databeskyttelsesforordningen eller denne databehandleraftale – og som har karakter af ekstraordinær eller konsulentpræget bistand – kan der indgås særskilt aftale herom, herunder om eventuel betaling. Sådan bistand ydes alene efter forudgående skriftlig aftale mellem parterne.

Databehandleren er ikke berettiget til vederlag, når bistanden vedrører opfyldelsen af egne forpligtelser i henhold til databeskyttelseslovgivningen eller skyldes forhold, som databehandleren selv eller dennes underdatabehandlere er ansvarlige for, herunder ved sikkerhedsbrud forårsaget af egne forhold.

Databehandleren tilbyder som led i tilsynsforpligtelsen en eller flere årlige uafhængige revisorerklæringer, jf. Bilag C.7, til brug for den dataansvarliges tilsyn. Ønsker den dataansvarlige i tillæg hertil at gennemføre yderligere kontrol eller kræver besvarelse af spørgeskemaer, egenerklæringer eller anden form for dokumentation, som ikke er en del af databehandlerens standardtilsynssetup, sker dette efter medgået tid medmindre andet fremgår eksplicit af Bilag C.