Databehandleraftale
zExpense

Ændringslog

Version	Ændringer
1.1 - Tilpasset af Datatilsynet	Ændringer i Bestemmelserne 7.7, 9.2, 10.4 og Bilag C.8 *(Tastefejl og opdaterede krydshenvisninger).*
1.2 - Tilpasset af Azets Insight 16. oktober 2023 (V.1.2.3)	• Ændret placering af baggrund og formål • 7.2: Valg af mulighed 2 • 7.3: Valg af mulighed 2 og min. to (2) uger • 9.2: Valg af tilsynsmyndighed (Datatilsynet) • 10.2: Valg af 48 timer, om muligt • 11.1: Valg af mulighed 2 • 11.2: Tilføjelse af den danske Bogføringslov • Bilag A-C tilpasset behandlingen • Bilag D tilpasset databehandleren specifikt

1. Baggrund og formål

1.1 Databehandleren (Leverandøren) og den dataansvarlige (Kunden) har aftalt følgende standard-kontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og friheds-rettigheder.

1.2 Bestemmelserne tager udgangspunkt i Datatilsynets standardkontraktbestemmelser (version 1.1 - januar 2020) i henhold til artikel 28, stk. 3 i forordning 2016/679 med henblik på databehandlerens behandling af personoplysninger.

2. Præambel

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

2.2 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).

2.3 I forbindelse med leveringen af Services behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

2.6 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.

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

2.8 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.

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

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

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

3. Den dataansvarliges rettigheder og forpligtelser

3.1 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 medlemsstaternes1 nationale ret og disse Bestemmelser.

3.2 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.

3.3 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

4.1 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.

4.2 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.

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

5. Fortrolighed

5.1 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.

5.2 Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

6.1 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.

6.2 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.

6.3 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

7.1 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).

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

7.3 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 to (2) ugers 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.

7.4 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.

7.5 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 følge af disse Bestemmelser, er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

7.6 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.

7.7 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

8.1 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.

8.2 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.

8.3 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

8.4 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.

8.5 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

9.1 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

9.2 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 friheds-rettigheder
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.

9.3 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

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

10.2 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.

10.3 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.

10.4 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

11.1 Ved ophør af Services vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11.2 Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

a. Bogføringsloven (Danmark)

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

12. Revision, herunder inspektion

12.1 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.

12.2 Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

12.3 Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning 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

13.1 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

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

14.2 Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

14.3 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.

14.4 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.

15. Kontaktpersoner hos databehandleren

15.1 Databehandleren kan kontaktes nedenstående kontaktperson.

Telefonnummer	+45 70 27 31 30
E-mail	gdpr-dk@azets.com

Bilag A Oplysninger om behandlingen

A.1 Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige og **A.2** Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)	Databehandleren må alene behandle personoplysninger til de formål, som er nødvendige for at opfylde aftalen med den dataansvarlige. Formål skal være angivet her eller evt. i skriftlige tillæg/supplerende aftaler. Databehandleren er berettiget til at lade personoplysninger indgå i databehandlerens sædvanlige backup-procedure. Databehandleren må, i det omfang andet ikke følger af databehandleraftalen, benytte alle relevante hjælpemidler, herunder IT-systemer. ☒ Applikationen zExpense (rejseafregninger): • Databehandleren stiller på abonnementsbasis cloud-baseret løsning til rådighed for den dataansvarlige. Løsningen benyttes til håndtering, godkendelse og opbevaring af informationer i forbindelse med behandling af udlæg, rejseafregninger, dokumentation af køb på firma(kredit)kort samt indsamling af oplysninger i forbindelse med kørselsgodtgørelse og diæter m.m. med eventuel integration til løn- eller økonomisystem • Løsningen tilbyder mobil app (iOS og Android) til brug for den dataansvarliges medarbejdere • Databehandleren leverer SaaS-løsning inklusive vedligehold, support og hosting til brug for den dataansvarlige • Som led i leverancen vil databehandleren få adgang til personoplysninger vedrørende den dataansvarliges medarbejdere • Databehandleren benytter applikationen Visma Case (ESDH system)
A.3 Behandlingen kan omfatte følgende typer af personoplysninger om de registrerede	☒ Applikationen zExpense (rejseafregninger): Den dataansvarliges nuværende og tidligere medarbejdere Almindelige personoplysninger: • medarbejdernummer • ansættelses- og fratrædelsesdato • navn og adresse • kontaktoplysninger, herunder telefon, e-mail, titel, afdeling, adresse • bankoplysninger • registreringsnummer (bil) tilknyttet medarbejder • kørte kilometer inkl. rute (GPS-oplysninger) • elektroniske udlæg/rejseafregninger Følsomme personoplysninger: • helbredsoplysninger i form af elektroniske bilag Fortrolige personoplysninger: • CPR-nummer ☒ Applikationen Visma Case (ESDH system): Den dataansvarliges nuværende og tidligere medarbejdere Almindelige, følsomme og fortrolige personoplysninger: .
A.4 Behandlingen omfatter følgende kategorier af registrerede	Se oversigten i A.3.
A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan	Databehandlingen af personoplysninger følger varigheden anført i enhver aktiv serviceaftale, samt dataansvarliges instruktion i Bestemmelse 11.1 og 11.2. Jf. dog undtagelser i C.4 (Opbevaringsperioder/sletterutiner).

påbegyndes efter disse Bestem-melsers ikrafttræden. Behand-lingen har følgende varighed	

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

	NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
☒	Zebon ApS	CVR nr. 32 36 64 49	Nordre Strandvej 119 A DK-3150 Hellebæk	Hosting, udvikling og vedligeholdelse af rejseafregningssystemet zExpense

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

Databehandleren kan generelt ændre eller indføre underdatabehandlere, forudsat at behandlingen er inden for EU/EØS, ved at give meddelelse som angivet i Bestemmelse 7.3.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1 Behandlingens genstand/instruks	Databehandlerens behandling af data på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende: Se Bilag A punkt A.1/A.2.
C.2 Behandlingssikkerhed. Sikkerhedsniveauet skal afspejle:	Behandlingen af data omfatter personoplysninger, som nævnt i Bilag A punkt A.3/A.4 og som kan være – men ikke nødvendigvis er – omfattet af Databeskyttelsesforordningen artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et "højt" sikkerhedsniveau. Databehandleren er 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 garanterer over for den dataansvarlige, at databehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at databehandlerens behandling af personoplysninger opfylder kravene i den til enhver tid gældende persondataretlige regulering. Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre foranstaltningerne beskrevet i punkt C.2.1-C.2.15, som er aftalt med den dataansvarlige.
C.2.1 Pseudonymisering og kryptering af personoplysninger	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger pseudonymiseres, hvor relevant for services. Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysningerne krypteres eller på anden vis beskyttes mod bl.a. uvedkommendes adgang og/eller manipulation, herunder særligt i forbindelse med transmission via åbne netværk og/eller eksterne kommunikationsforbindelser. Niveauet af kryptering skal være passende for effektivt at forhindre uvedkommende i at få adgang til personoplysninger. Se punkt C.2.7.
C.2.2 Sikring af fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -services	Databehandlerens medarbejderes tavshedspligt er specificeret i punkt C.2.6. Databehandlerens tekniske sikkerhed: • Virusdefinitioner opdateres dagligt • Lokal firewall på Pc'er og servere er aktiveret • Netværk er beskyttet af firewall • Løbende interne og eksterne sårbarhedsscanninger for at sikre optimal konfiguration • Medarbejdere og eksternt tilknyttede konsulenter har ekstern adgang til netværk via krypterede forbindelser med MFA • Data på alle Pc'er er krypteret • Der anvendes komplekse passwords • Udveksling af persondata med dataansvarlig m.fl. sker via krypterede forbindelser, for eksempel SFTP eller webportaler • Løbende backup af data

	Databehandlerens organisatoriske sikkerhed: • Autorisationsprocedurer, adgangsrettigheder, logning mv. i henhold til databehandlerens interne IT-procedurer • Medarbejdere og eksternt tilknyttede konsulenter modtager sikkerhedstræning og fyldestgørende instruktioner i og retningslinjer for behandling af personoplysninger og IT-sikkerhed
C.2.3 Genoprettelse af personoplysningerne og drift	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer rettidig genoprettelse af tilgængelighed til personoplysningerne i tilfælde af fysiske hændelser (f.eks. strømafbrydelse, brand, oversvømmelse, lynnedslag mv.) og/eller tekniske hændelser (systemnedbrud mv.), herunder i form af beredskabsplaner, procedurer mv. Databehandler er forpligtet til at gennemføre og opretholde dokumenterede beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser.
C.2.4 Procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed (omfatter alle systemer medmindre de er anført med særlig kommentar)	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Databehandleren gennemfører årlig kontrol med underleverandører ved gennemgang af databehandleraftaler for de enkelte underleverandører samt en risikovurdering. Eventuelle problemstillinger følges op (jf. punkt C.8). ☒ Applikationen zExpense (rejseafregninger): • Underdatabehandler har dokumenterede procedurer for sikring af tekniske og organisatoriske foranstaltninger, der årligt er revideret i en eksternt udarbejdet revisorerklæring (jf. punkt C.8).
C.2.5 Personalets adgang til personoplysninger	Databehandleren sikrer via formelle godkendelsesprocesser samt tilbagevendende kontrol af adgange, at kun personer med et dokumenteret arbejdsrelateret behov, har adgang til personoplysninger. Databehandleren skal uden ugrundet ophold annullere autorisationer (og herunder adgange) for brugere, der ikke længere har et arbejdsbetinget behov for autorisation.
C.2.6 Tavshedspligt	Alle medarbejdere hos databehandleren og eksternt tilknyttede konsulenter er underlagt kontraktuel tavshedspligt med hensyn til alt, hvad medarbejderen under sit arbejde for databehandleren erfarer om alle forretningsmæssige og fortrolige oplysninger, som vedrører parter, som databehandleren har forbindelse med. Tavshedspligten er også gældende efter ansættelsesforholdets ophør.
C.2.7 Beskyttelse af data under transmission og opbevaring (omfatter alle systemer medmindre de er anført med særlig kommentar)	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger beskyttes mod bl.a. uvedkommendes adgang og/eller manipulation. Kryptering af transportlaget skal til enhver tid opfylde Datatilsynets minimumskrav.

	☒ Applikationen zExpense (rejseafregninger): • Ekstern fillevering til og fra løsningen sker via SFTP eller FTPS-forbindelse • Al kommunikation til og fra løsningen er krypteret, enten via HTTPS-forespørgsler via webløsningen eller kommunikation til/fra App • Løsningen er krypteret under opbevaring og tilgås i krypteret form via web og/eller via App (iOS og Android)
C.2.8 Fysisk sikring af lokaliteter, hvor der behandles persondata	Databehandleren er forpligtet til at gennemføre og opretholde passende fysiske, tekniske og organisatoriske foranstaltninger, der sikrer de fysiske lokaliteter, hvor personoplysninger behandles mod blandt andet uvedkommendes adgang og/eller manipulation af data. Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.
C.2.9 Sikkerhedskopiering	Sikkerhedskopiering af systemer, konfigurationsfiler og data skal finde sted således, at relevant data kan reetableres. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eksempelvis ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger. Herunder bl.a.: • Der gælder de samme retningslinjer for sikkerhedskopier, som for al anden behandling af personoplysninger i medfør af aftale og denne databehandleraftale • Sikkerhedskopier opbevares geografisk adskilt fra det primære datacenter • Databehandleren kontrollerer løbende, at sikkerhedskopier er læsbare
C.2.10 Passwordpolitik og kontrol med afviste adgangsforsøg	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, som sikrer at adgangskoder har passende længde og kompleksitet for at forhindre, at de kan gættes. Adgangskoder skal være unikke for den enkelte medarbejder og eksternt tilknyttede konsulent. Databehandleren er forpligtet til at registrere afviste adgangsforsøg og blokere for yderligere forsøg efter fastlagt antal på hinanden følgende afviste adgangsforsøg.
C.2.11 Anvendelse af hjemmearbejdspladser	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger beskyttes mod blandt andet uvedkommendes adgang og/eller manipulation, når disse tilgås fra hjemme- og fjernarbejdspladser, og at der ved adgang til personoplysninger fra hjemme- og fjernarbejdspladser anvendes kryptering af kommunikationsforbindelser samt autentifikation af personer, som får adgang. Alle computere er krypterede og adgangskodebeskyttede. Adgang til databehandlerens systemer sker via VPN-forbindelse med MFA. Eventuelt print minimeres i videst mulig omfang og skal makuleres efter brug. Medarbejdere og eksterne konsulenter skal regelmæssigt gennemgå obligatorisk awareness træning i henhold til punkt C.2.12.

C.2.12 Awareness træning	Databehandleren er forpligtet til at sikre, at medarbejdere og eksternt tilknyttede konsulenter regelmæssigt (og mindst årligt) gennemgår obligatorisk undervisning om IT-sikkerhed og databeskyttelse.
C.2.13 Ændringshåndtering	Databehandleren er forpligtet til at have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.
C.2.14 Logning	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, som sikrer logning, så hændelser kan spores. Logs skal indeholde tidsstempling og hvor relevant, bruger-ID, terminal-ID samt netværks adresser. Som minimum skal følgende sikkerhedshændelser logges: • afviste adgangsforsøg • succesfulde og afviste autentifikationsforsøg som følge af konto lockout udløst af adgangskontrolsystem Tilgang til personoplysningerne skal logges i et sådant omfang, at logoplysningerne kan anvendes til at afværge og forebygge uberettiget adgang til personoplysninger. Hvor relevant, skal adgang til personoplysninger logges, herunder, hvilke data der tilgås, behandlingen af data samt tid og identitetsoplysninger. Log opbevares maksimalt i tretten (13) måneder. I tilfælde af hændelser, kan opbevaring forlænges. Backup arkiv gemmes maksimalt i seks (6) år (jf. bilag D vedrørende Bestemmelse 11.1 og 11.2). I samme periode er databehandleren berettiget til at lade personoplysningerne indgå i databehandlerens sædvanlige backupprocedure.
C.2.15 Databeskyttelsesrådgiver og IT-sikkerhedspersonale	Databehandleren er forpligtet til at have udpeget en, eller flere, databeskyttelsesrådgivere, som beskrevet i Databeskyttelsesforordningen. Databehandleren er forpligtet til at have dedikerede ressourcer til at opretholde databehandlerens IT-sikkerhed.
C.3 Bistand til den dataansvarlige	Databehandleren skal i nødvendigt og rimeligt omfang bistå ved den dataansvarliges opfyldelse af dennes forpligtelser ved behandling af personoplysninger, der er omfattet af Bestemmelserne i punkt 9 og 10 ved at gennemføre sådanne tekniske og organisatoriske foranstaltninger, som kan bidrage til den dataansvarliges mulighed for at besvare anmodninger om udøvelse af de registreredes rettigheder.
C.4 Opbevaringsperiode/sletterutiner (omfatter alle systemer medmindre de er anført med særlig kommentar)	Personoplysninger opbevares i maksimalt seks (6) år i henhold bogføringslovens krav (jf. bilag D vedrørende Bestemmelse 11.1 og 11.2). Ved ophør af Services vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med Bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret det oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne. ☒ Applikationen zExpense (rejseafregninger):

	• Ved ophør skal den dataansvarlige senest tre (3) måneder efter serviceaftalens ophør via applikationens eksportfacilitet eksportere alle data inklusive billeder af fakturaer, kvitteringer og lignende til Excel med henblik på overholdelse af bogføringsloven
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 ud over hos de i bilag B anførte underdatabehandlere: • Databehandlerens til enhver tid værende lokationer i Danmark • Hjemme- og fjernarbejdspladser (databehandlerens medarbejdere og eksternt tilknyttede konsulenter)
C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande	Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.
C.6.1 Cloud-leverandør og dataoverførselsmekanisme	Såfremt databehandleren anvender cloud-leverandør i forbindelse med levering af Services (jf. bilag B) må der udelukkende anvendes datacentre inden for EU/EØS.
C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren	Den dataansvarlige eller en repræsentant for den dataansvarlige har 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. Dette gælder dog ikke databehandlerens hjemmearbejdspladser. Den dataansvarlige skal give databehandleren et varsel på mindst tredive (30) dage inden inspektion. Såfremt dataansvarlig eller en repræsentant for den dataansvarlige foretager inspektion hos databehandler, skal vedkommende fremvise gyldig billedidentifikation. Vedkommendes identitet og formål skal bekræftes af dataansvarliges kontaktperson, forinden vedkommende får adgang til fortrolige oplysninger. Dataansvarlig eller repræsentant for den dataansvarlige skal overholde alle sikkerhedskrav, som måtte være gældende for lokationen. Den dataansvarliges udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige. Databehandleren er forpligtet til mod vederlag at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion. Den dataansvarlige har ret til at gennemføre et årligt skriftlig tilsyn med databehandlerens overholdelse af disse Bestemmelser såfremt der ikke foreligger årlig ISAE 3000 og/eller ISAE 3402 eller tilsvarende erklæring. Metoden for skriftligt tilsyn baseres på den dataansvarliges spørgeskema, som fremsendes til databehandleren. Afhængig af omfang kan skriftligt tilsyn være en betalbar ydelse, hvilket aftales mellem parterne før gennemførelse.
C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger,	Databehandleren eller en repræsentant for databehandleren kan årligt foretage en fysisk inspektion af lokaliteterne, hvorfra underdatabehandlere foretager behandling af personoplysninger, herunder fysiske

som er overladt til underdatabehandlere (omfatter alle systemer medmindre de er anført med særlig kommentar)	lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Ud over det årlige tilsyn, skal databehandleren gennemføre en inspektion med underdatabehandleren, når databehandleren finder det nødvendigt. Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til for egen regning og risiko 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. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde for egen regning og risiko anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode. Parterne er enige om, at følgende type af revisionserklæring kan anvendes i overensstemmelse med disse Bestemmelser på følgende områder med underdatabehandler: ☒ Applikationen zExpense (rejseafregninger): • ISAE 3402 Type II • ISAE 3000 Type II ☒ Applikationen Visma Case (ESDH system): • ISAE 3000 Type I • ISAE 3402 Type II • ISO27001 Compliance Ovenstående revisionserklæringer fremsendes på anmodning uden vederlag og unødig forsinkelse til den dataansvarlige til orientering. Revisionserklæringer er fortrolige og må ikke deles med uvedkommende.

Bilag D Parternes regulering af andre forhold

Som supplement til Bestemmelserne har parterne aftalt følgende:

Vedrørende Bestemmelse 7.6:

Parterne har fraveget Bestemmelse 7.6, som ikke er gældende for aftalen.

Vedrørende Bestemmelse 11.1 og 11.2:

Databehandleren opbevarer bogførings- og regnskabsmateriale på betryggende vis i fem (5) år fra udgangen af det regnskabsår, som materialet vedrører, med mindre den dataansvarlige skriftligt bekræfter at overtage ansvaret herfor.

Vedrørende Bestemmelse 13.1:

Ansvar:

Parternes ansvar i henhold til Bestemmelserne er underlagt samme ansvarsbegrænsning som aftalt mellem parterne i den/de serviceaftale(r), hvorunder personoplysningerne behandles.

Den dataansvarlige er ansvarlig for skader forårsaget af behandling, der er i strid med gældende databeskyttelseslovgivning. Databehandleren er kun ansvarlig for direkte og dokumenterede skader forårsaget af behandling, hvor databehandleren har overtrådt disse Bestemmelser og/eller gældende databeskyttelseslovgivning, der specifikt er rettet mod databehandlerens forpligtelser.

For at undgå tvivl er parterne enige om og anerkender, at hver part skal være ansvarlig for og holdes ansvarlig for at betale alle administrative bøder og skader påført den registrerede, som en part er blevet pålagt at betale i overensstemmelse med gældende databeskyttelseslovgivning.