DATABEHANDLERAFTALE

Version: 29. september 2025

Standardkontraktsbestemmelser

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

mellem

brugeren

herefter "den dataansvarlige"

og

GoWiser ApS, CVR-nr.: 41878150, Dampfærgevej 2A, 1. th, 2100 København Ø, Danmark
(som nærmere defineret i Konsulentaftalen)

herefter "databehandleren"

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

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen 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 "arbejdspapirer til brug for revisioner" 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.

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[1] 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

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

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 90 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 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 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 på den dataansvarliges hjemsted, 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 på den dataansvarliges hjemsted, 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 nærmeret 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 skriftlig varsel af begge parter.

5. Underskrift

   Disse Bestemmelser skal anses som en integreret del af Konsulentaftalen mellem parterne og er vedlagt Konsulentaftalen som bilag.

   Vedtagelsen af disse Bestemmelser skal derfor anses for at være sket ved indgåelsen af Konsulentaftalen.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

   Kontaktpersonen hos den dataansvarlige fremgår af Konsulentaftalen.

Navn	Alexander Christensen
Stilling	Direktør
Telefonnummer	52112222
E-mail	ac@gowiser.com

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Bilag A Oplysninger om behandlingen

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

1. Formålet med databehandlingen er, at databehandleren skal danne en række arbejdspa-pirer, som dataansvarlige kan anvende i revisionen af deres revisionskunder. Databehand-leren udarbejder arbejdspapirerne på baggrund af data fra revisionskundernes økonomisy-stemer i databehandlerens egenudviklede Microsoft Excel system.

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

1. Databehandlerens behandling af personoplysninger drejer sig udelukkende om udarbejdelsen af arbejdspapirerne. Processen omfatter følgende behandlingsaktiviteter:

   1) Indsamling: Databehandleren modtager personoplysningerne ved at hente data fra data-behandlerens Microsoft Azure Blob Storage når dataansvarlige uploader data fra revisionskun-derens økonomisystemer dertil.

   2) Opbevaring: I forbindelse med overførsel og opbevaring af data, benytter databehandleren Microsoft Azure Blob Storage. Kunden (den dataansvarlige) uploader rådata til databehand-lerens Azure Blob Storage, hvorfra databehandleren henter det ned på databehandlerens PC for dannelsen af arbejdspapirerne. I overensstemmelse med databehandlerens databehand-lingspolitik lagres alle data i denne sammenhæng kun i AppData-mappen på databehandle-rens PC. Denne specifikke placering er valgt for at sikre en konsistent, kontrolleret og sikker behandling af data. Efter dannelse af arbejdspapirerne vil disse blive uploadet tilbage til databehandlerens Microsoft Azure Blob Storage. Derudover uploader databehandleren pro-grammer og filer som benyttes af databehandleren i forbindelse med dannelse af arbejdspa-pirer til databehandlerens Microsoft Azure Blob Storage. Alle korrespondancer på databe-handlerens platform mellem databehandleren og den dataansvarlige opbevares i databehand-lerens Azure SQL-database.

   Som udgangspunkt anvendes udelukkende databehandlerens Microsoft Azure Blob Storage til opbevaring og overførsel af data, medmindre andet skriftligt aftales mellem parterne.

   3) Organisering og Strukturering: Databehandler strukturerer data inden arbejdspapirerne dannes.

   4) Behandling gennem egenudviklet Microsoft Excel system: Efter strukturering af data vil arbejdspapirerne blive dannet ud fra databehandlerens egenudviklede system. Dette system er skræddersyet til at transformere de strukturerede data til meningsfulde analyser og rap-porter til brug for dataansvarliges revision.

   5) Sletning: Formålet med opbevaring af data ophører på forskellige tidspunkter, afhængig af datatypen. Databehandleren har opsat automatiske kørsler som løbende og automatisk sletter data fra på databehandlerens Microsoft Azure Blob Storage når formålet ophører:

5.1 Data generelt
Alt data vedrørende en sag, med undtagelse af data specificeret i pkt. 5.2, 5.3, 5.4, 5.5 og 5.6, vil automatisk blive slettet i databehandlerens Microsoft Azure Blob Storage 910 dage efter databehandleren har markeret en sag som "Udført" på Platformen.

5.2 Automatisk sletning af filer på databehandlerens lokale computere
Når en af GoWisers ServiceHub-medarbejdere påbegynder en sag, oprettes en unik lokal mappe på medarbejderens computer under AppData. Data vedrørende sagen vil kun blive gemt i denne specifikke mappe. Alle computere hos GoWiser har et program installeret, som ved opstart automatisk sletter disse unikke sagsmapper, når de er ældre end 30 dage fra oprettelsestidspunktet.

5.3 Data som forventeligt anvendes i efterfølgende års revisioner
Data som forventeligt skal anvendes i efterfølgende år opbevares i databehandlerens Microsoft Azure Blob Storage. Dette vedrører finansposteringer renset af ServiceHubben, og som I efterfølgende år kan bruges til sammenligningstal. Dette data opbevares i ca. 2,5 år, nærmere bestemt 910 dage, da det muliggør sammenligningstal 2 år bagud, hvorefter databehandleren har opsat sletning af disse data i databehandlerens Microsoft Azure Blob Storage.

5.4 Korrespondancer mellem databehandleren og den dataansvarlige
Alle korrespondancer på databehandlerens platform mellem databehandleren og den dataansvarlige opbevares i databehandlerens Azure SQL database i 910 dage, så det følger øvrig data og filer som forventlig anvendes i efterfølgende års revisioner under punkt 5.3.

5.5 Støttefiler til dannelsen af arbejdspapirer mv.
Programmer og filer som benyttes i forbindelse med dannelse af arbejdspapirer gemmes i databehandlerens Microsoft Azure Blob Storage i 910 dage, i tilfælde af at Kunden (den dataansvarlige) ønsker ændringer til arbejdspapirerne eller sagen genåbnet efter Sagens afslutning.

5.6 Stamdata
Stamdata på revisionskunder opbevares indtil kunden slettes i databehandlerens Microsoft Azure Blob Storage. Stamdata omfatter for eksempel CVR-Nr., selskabsnavn og koncernforhold. Derudover betragtes indstillinger for revisionskunden også som stamdata, f.eks. risikoparametre, kontoplan og mapping til regnskabsposter.

5.7 Data vedrørende den dataansvarliges udgåede kunder
Når et kundeforhold mellem den dataansvarlige og en af dennes kunder ophører, har databehandleren opsat sletning af den udgåede kundes data i databehandlerens Microsoft Azure Blob Storage. Den dataansvarliges udgåede kundes data slettes på databehandlerens PC i overensstemmelse med det angivne i punkt 5.2.

Opsamling på beskrivelserne af opbevaring og sletning under punkt A.2:

Beskrivelse	Placering af data	Opbevaringstid
Den dataansvarlige uploader rådata til databehandlerens Microsoft Azure Blob Storage.	Databehandlerens Microsoft Azure Blob Storage	910 dage
Databehandleren henter rådata ned og påbegynder dannelse af arbejdspapirer.	AppData på databehandlerens PC'er.	30 dage
Programmer og filer som benyttes af databehandleren i forbindelse med dannelse af arbejdspapirer	Databehandlerens Microsoft Azure Blob Storage	910 dage
Databehandleren uploader de færdige arbejdspapirer til den dataansvarlige.	Databehandlerens Microsoft Azure Blob Storage	910 dage
Databehandleren gemmer data som kan bruges i efterfølgende års revisioner.	Databehandlerens Microsoft Azure Blob Storage	910 dage
Databehandleren gemmer korrespondancer mellem databehandleren og den dataansvarlige fra databehandlerens platform.	Databehandlerens Azure SQL-database	910 dage
Stamdata vedrørende virksomhederne i Sagerne.	Databehandlerens Microsoft Azure Blob Storage	Indtil virksomhederne slettes i systemet
Sletning af data ved kundeforholdets ophør	Sletning i databehandlerens Microsoft Azure Blob Storage	Ved kundeforholdets ophør.

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

1. I denne aftale vil personoplysningerne fremgå af data fra revisionskundernes økonomisystemer, som dataansvarlige uploader til databehandlerens platform. Dette vil typisk omfatte følgende kategorier af almindelige personoplysninger:

   Navn
   Løn
   Medarbejdernummer
   Initialer
   Adresse
   E-mailadresse

A.4. Behandlingen omfatter følgende kategorier af registrerede

1. De personoplysninger, der kan fremgå af dataudtrækket fra revisionskundernes økonomisystem, kan omfatte personer, der er involveret i virksomhedens drift i den afgrænsede periode. Dette kan inkludere virksomhedens ejere, medarbejdere, leverandører og andre parter der optræder i virksomhedernes transaktionsdata.

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

1. Behandlingen er ikke tidsbegrænset og foretages derfor så længe tjenesten vedrørende behandling af personoplysninger varer, hvorefter personoplysningerne slettes eller tilbageleveres i overensstemmelse med punkt 11.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND SAMT GRUNDLAG
Microsoft Azure	N/A	Microsoft Azure Datacenter Germany West Central Frankfurt	Databehandleren anvender underdatabehandlerens platform til opbevaring af data	Ja EU-U.S Data Privacy Framework, jf. artikel 45 GDPR anvendes som overførselsgrundlag

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden skriftligt at have underrettet den dataansvarlige – 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

Den dataansvarlige har givet databehandleren sin forudgående generelle skriftlige godkendelse til tilføjelse eller erstatning af underdatabehandlere. Underretning om tilføjelse eller erstatning af underdatabehandler, skal være den dataansvarlige i hænde minimum 90 dage, før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give databehandleren meddelelse herom inden ændringens varslede virkningstidspunkt. Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

Hvis den dataansvarlige afslår, at der foretages ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere, kan dette medføre, at databehandleren kan blive afskåret fra at opfylde tjenesterne. Hvis det er tilfældet, accepterer den dataansvarlige, at manglende levering af tjenester ikke anses for en misligholdelse af en aftale. Parterne kan herefter opsige Hovedaftalen med 30 dages skriftlig varsel til udgangen af en kalendermåned, hvis databehandleren som følge af den dataansvarliges indsigelse ikke kan levere alle de aftalte tjenester i overensstemmelse med Hovedaftalen. Forudbetalt vederlag for perioden efter opsigelsesperiodens udløb vil blive tilbagebetalt til den dataansvarlige.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Som tillæg til beskrivelserne i A.2. hører dette afsnit. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Databehandleren har til opgave at udarbejde arbejdspapirer til revisionen, som dataansvarlige efterspørger.
Databehandleren har dermed fået instruks fra dataansvarlige om indledningsvist at indsamle, opbevare og strukturere data til, at arbejdspapirerne kan dannes i databehandlerens egenudviklede program samt at generere de efterspurgte arbejdspapirer.

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle:

Behandlingsprocessen involverer opbevaring, organisering og analyse af omfattende data-udtræk fra virksomheders økonomisystemer. Hovedparten af disse data repræsenterer økonomiske oplysninger uden personlig karakter. Imidlertid kan der, som angivet i afsnit A.3, være tilfælde, hvor personoplysninger såsom navne, løninformation, adresser og medarbejdernumre optræder i virksomhedernes finansposteringer. Sådanne oplysninger vil være kategoriseret som almindelige personoplysninger. Selvom behandlingen indebærer en betydelig mængde data, forventes personoplysninger kun at udgøre en forholdsvis lille del af det samlede datasæt.

Der etableres et "højt" sikkerhedsniveau.

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 gennemfører passende sikkerhedsforanstaltninger for at beskytte de overladte personoplysninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, utilgængelighed, uautoriseret videregivelse af eller adgang til personoplysningerne. Databehandleren kan løbende ændre i gennemførte sikkerhedsforanstaltninger, idet ændringer i sikkerhedsforanstaltninger dog aldrig må føre til en forringelse af det aftalte sikkerhedsniveau.

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

Krav til pseudonymisering og kryptering af personoplysninger

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kryptering:

a) Adgangskoder opbevaret på databehandlerens PC er krypteret.
b) Databehandlernes computere har krypteret harddisk.
c) Personoplysninger er som standard krypteret ved brugen af Azure Blob Storage.

Krav vedrørende adgang til oplysningerne via internettet
Adgang til de lagrede data via internettet sker udelukkende gennem databehandlerens platform, der er udarbejdet i Microsoft Azure Blob Storage, en pålidelig og sikker cloud-tjeneste, der sikrer integritet og fortrolighed af data gennem avanceret kryptering. Kun autoriserede og udvalgte brugere, hvis identitet og adgangsrettigheder er blevet verificeret og godkendt, vil have mulighed for at tilgå disse oplysninger. Dette sikkerhedslag sikrer, at fortrolige og følsomme data beskyttes imod uautoriseret adgang.

Krav vedrørende beskyttelse af oplysninger under transmission
I aftalen om databehandling er antallet af overførsler af data mellem de to involverede parter og anvendte systemer strengt begrænset. Første transmission initieres, når den dataansvarlige uploader materiale til databehandlerens Microsoft Azure Blob Storage. Derefter henter databehandleren dataene til sin AppData-mappe, hvor analysen af data finder sted. Efter endt behandling uploades de respektive arbejdspapirer atter til databehandlerens Azure Blob Storage, hvor de er tilgængelige for dataansvarlige. Antallet af berøringspunkter i overførselsprocessen er omhyggeligt begrænset, som muliggør en mere præcis styring og restriktion af adgang til kun autoriserede brugere.

Krav vedrørende beskyttelse af oplysninger under opbevaring
Opbevaring af data, der behandles inden for rammerne af denne aftale, er nøje begrænset til to specifikke lokationer hos databehandleren. Til upload og udveksling af data samt arbejdspapirer mellem dataansvarlig og databehandler anvendes Microsoft Azure Blob Storage til lagring i skyen. Til den efterfølgende udarbejdelse af de ønskede arbejdspapirer lagres data i databehandlerens AppData-mappe på de specifikke PC'er, der benyttes til behandlingsaktiviteterne.
For at sikre en høj grad af fortrolighed og integritet af data, er alle PC'er inden for virksomheden og til databehandlingen krypteret ved hjælp af BitLocker, Microsofts diskkrypteringsteknologi. BitLocker tilbyder en robust og pålidelig løsning, der krypterer hele diskdrevet og beskytter således følsomme data mod uautoriseret adgang og potentielle sikkerhedstrusler. Yderligere sikkerhed under opbevaring i AppData er implementeret gennem integrationen med Micosoft Azure, hvor BitLocker-nøglerne opbevares. Azure's overholdelse af globale standarder og regulativer sikrer yderligere, at nøgleopbevaringen overholder relevante lovkrav og industripraksis.

Ingen data vil blive lagret eller behandlet af databehandleren uden for disse to lokationer.

Krav vedrørende fysisk sikring af lokaliteter, hvor der behandles oplysninger
Databehandlingen sker udelukkende fra databehandlerens sikrede kontorfaciliteter. Adgang til databehandlerens hovedbygning er begrænset til personer med autoriseret adgang. Tilsvarende gælder for databehandlerens eget kontor.

Krav vedrørende logning
Databehandleren logger hvilke brugere, der har adgang til systemet med persondata. Desuden holdes der log over hvilke filer der åbnes, gemmes og ændres.

Krav vedrørende backup
Databehandleren anvender Azure Backup-tjenesten til regelmæssigt at foretage en sikkerhedskopi hver 24. time. Databehandleren opbevarer sikkerhedskopien i syv dage, hvorefter sikkerhedskopien slettes.

Tilsvarende foretager databehandleren en sikkerhedskopi af databehandlerens Azure Storage til en Azure Backup Vault hver 24. time. Disse data opbevares i 30 dage, hvorefter de sikkerhedskopierede elementer automatisk fjernes.

C.3 Bistand til den dataansvarlige
Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Fysisk sikkerhed:
1. Databehandlerens kontorlokaler aflåses.
2. Databehandlerens udstyr er sikret bag låste døre.
3. Databehandleren og besøgende identificeres inden adgang til kontoret.
4. Databehandleren anvender nøglestyring.

Organisatorisk sikkerhed:

1. Alle medarbejdere har en fortrolighedsforpligtelse, som gælder over for alle de personoplysninger, der bliver behandlet.
2. Medarbejdernes adgang til personoplysninger i systemet er begrænset til relevante medarbejdere.
3. Medarbejdere trænes kontinuerligt i processen og de i involverede systemer, hvor persondata behandles.
4. Databehandleren skaber awareness omkring databehandling og håndtering af data hos sine medarbejdere.

C.4 Opbevaringsperiode/sletterutine
Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1.

C.5 Lokalitet for behandling
Som udgangspunkt kan behandling af de i Bestemmelserne omfattede personoplysninger ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

GoWiser ApS
Dampfærgevej 2A, 1. th
2100 København Ø
Danmark

Samt databehandlerens og underdatabehandlerens nuværende og fremtidige lokationer. Ved underdatabehandleren forstås nuværende underdatabehandlere samt eventuelle tilføjelser eller erstatninger, under hensyntagen til betingelserne for den dataansvarliges godkendelse af underdatabehandleren som angivet i Bestemmelsernes punkt 7 og bilag B.

Databehandlerens ledende medarbejdere har dog undtagelsesvis mulighed for at behandle personoplysninger uden for ovenstående lokation. Databehandlerens ledende medarbejdere har adgang til arbejdsrelateret it-udstyr stillet til rådighed af databehandleren på deres respektive private hjemmeadresser. Dette sker udelukkende med henblik på at kunne yde en fleksibel og udvidet service over for den dataansvarlige, herunder uden for databehandlerens normale åbningstider. Databehandleren forpligter sig til at sikre, at databehandlingen på disse private hjemmeadresser foregår under

iagttagelse af passende tekniske og organisatoriske sikkerhedsforanstaltninger i overensstemmelse med Bestemmelserne i denne aftale. Alle øvrige medarbejdere i databehandlerens Service Hub er ikke omfattet af reglerne om behandling af personoplysninger udenfor databehandlerens ovenstående lokation.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Ved godkendelsen af underdatabehandlerne oplistet i bilag B.1. instruerer den Dataansvarlige Databehandleren i at overføre personoplysninger til tredjelande i det omfang, det er beskrevet i bilag B.1.

Databehandleren underretter den Dataansvarlige om ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere, som fastsat i bestemmelse 7.3. Hvis ikke den Dataansvarlige gør indsigelse mod sådanne ændringer, skal den Dataansvarlige anses for at have instrueret Databehandleren i at foretage overførsel af personoplysninger til tredjelande i det omfang, det er beskrevet i forbindelse med ændringen.

Overførsel af personoplysninger til tredjelande skal ske i overensstemmelse med databeskyttelsesforordningens kapitel V, herunder de til enhver tid gældende standardkontraktbestemmelser fra EU-Kommissionen, jf. databeskyttelsesforordningens artikel 46, eller en afgørelse fra EU-Kommissionen om tilstrækkeligheden af beskyttelsesniveauet, jf. databeskyttelsesforordningens artikel 45.

De bestemmelser der gælder i henhold til det anvendte overførselsgrundlag, skal gå forud for disse Bestemmelser, men kun i relation til den behandling, der nødvendiggør overførselsgrundlaget; anden behandling er udelukkende underlagt disse Bestemmelser.

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.

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.

Den dataansvarliges tilsyn med databehandleren udføres ved blandt andet at anmode om at få udleveret relevante underdatabehandleres ISAE 3000-erklæringer eller lignende erklæringer og rapporter. Endvidere vil tilsynet udføres ved fremsendelse af et spørgeskema, som databehandleren udfylder og returnerer til den dataansvarlige uden unødig forsinkelse. Ved udfyldelsen af spørgeskemaet skal databehandleren dokumentere overholdelse af de relevante krav til databehandleren i databeskyttelsesforordningen og databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. Tilsynet skal udføres, når den dataansvarlige vurderer, at det er nødvendigt.

Databehandlerens udgifter i forbindelse med det skriftlige tilsyn afholdes af databehandleren.

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

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

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

Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende – uanset om den dataansvarlige har initieret og deltaget i en sådan inspektion.

Bilag D Parternes regulering af andre forhold