DATABEHANDLERAFTALE

Standardkontraktsbestemmelser

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

Mellem

Navn
Cvr nr
Adresse
Postnummer og By
Land

herefter "den dataansvarlige"

og

Zenegy Danmark ApS
CVR-nr.: 38366041
Slotsmarken 16
2970 Hørsholm

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 ... 3
3. Den dataansvarliges rettigheder og forpligtelser ... 4
4. Databehandleren handler efter instruks ... 4
5. Fortrolighed ... 4
6. Behandlingssikkerhed ... 5
7. Anvendelse af underdatabehandlere ... 6
8. Overførsel til tredjelande eller internationale organisationer ... 7
9. Bistand til den dataansvarlige ... 8
10. Underretning om brud på persondatasikkerheden ... 9
11. Sletning og returnering af oplysninger ... 9
12. Revision, herunder inspektion ... 9
13. Parternes aftale om andre forhold ... 10
14. Ikrafttræden og ophør ... 10
15. Underskrift ... 10
16. Kontaktpersoner hos den dataansvarlige og databehandleren ... 11
Bilag A - Oplysninger om behandlingen ... 12
Bilag B - Underdatabehandlere ... 17
Bilag C - Instruks vedrørende behandling af personoplysninger ... 18
Bilag D - Parternes regulering af andre forhold ... 26
Versionshistorik ... 27

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 de tjenester, som den dataansvarlige abonnerer på, som beskrevet i de gældende vilkår og betingelser, abonnementsoplysninger på kundens konto eller en separat kommerciel aftale, vil databehandleren behandle personoplysninger på vegne af den dataansvarlige i overensstemmelse med klausulerne.

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 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.

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.

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

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

7.6. 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

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:

8.3.1. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

8.3.2. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

8.3.3. 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:

9.2.1. 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 i det land, hvor den dataansvarlige er hjemmehørende, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

9.2.2. 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

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

9.2.4. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, i det land, hvor den dataansvarlige er hjemmehørende, 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 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.

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:

10.3.1. 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

10.3.2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

10.3.3. 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 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 dataansvarlige, at oplysningerne er slettet, jf. nærmere bilag A, punkt A.5, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11.2. Den dataansvarlige har ved ophør af brug af Zenegys produkter, mulighed for at Zenegy fortsat opbevarer medarbejderens oplysninger i Zenegy Payroll i en periode op til 5 år mod et gebyr. For nogle produkter er det et lovkrav at opbevare oplysninger i mindst 5 år, se Bilag C.4.

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 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

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 A.5. and C.4, kan Bestemmelserne opsiges uden yderligere varsel af begge parter.

15. Underskrift

På vegne af databehandleren		På vegne af den dataansvarlige
Navn	Jacob Wandt	Navn
Stilling	Direktør	Stilling
Telefon	+45 70 22 22 16	Telefonnummer
E-mail	jwa@zenegy.com	E-mail
Underskrift		Underskrift



16. 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.

Hos den dataansvarlige er kontaktpersonen den i Applikationen (Zenegy), af den dataansvarlige, til enhver tid angivne kontaktperson.

Kontaktperson hos databehandleren:

Navn	Dorota Kaminska-Szczyrba
Stilling	Senior Risk Manager & DPO
Telefonnummer	+45 70 22 22 16
E-mail	compliance@zenegy.com dks@zenegy.com

Bilag A - Oplysninger om behandlingen

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

På abonnementsbasis stiller databehandleren de cloud-baserede tjenester ("Tjenester"), der er valgt af den dataansvarlige til rådighed som beskrevet i den gældende kommercielle aftale, vilkår og betingelser eller de abonnementsoplysninger, der er synlige på den dataansvarliges konto for den dataansvarlige, dennes medarbejdere og/eller dennes kunder (inkl. kundens medarbejdere).

Den dataansvarliges brug af databehandlerens cloud-baserede Tjenester sker ved den dataansvarliges eller dennes klienters selvbetjening via databehandlerens hjemmeside www.zenegy.com, og/eller via databehandlerens app.

Den dataansvarliges medarbejdere og/eller klienter (inkl. dennes medarbejdere) kan ligeledes tilgå deres egne oplysninger fra de af den dataansvarlige valgte tjenester, så som lønsedler, fraværsoversigter, ferieoversigter, udlæg, kursusoplysninger, tidsregistreringer og de dokumenter, som medarbejderen eller kunden har indlæst, eksempelvis ansættelseskontrakt.

Både den dataansvarliges, dennes medarbejderes og klienters (inkl. dennes medarbejderes) brug af tjenesten kræver et unikt bruger ID og en adgangskode.

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

Payroll: Opbevaring og foretagelse af lønadministration, HR-administration, samt bogføring/regnskab, herunder administration af løn, refusion af udlæg, kørselsregnskaber, tidsregistrering, registrering af ferie, fraværsregistrering o.lign.

Expense: Registrering af udlæg samt opbevaring af kvitteringer med henblik på korrekt håndtering og rapportering af medarbejder udlæg.

Numbers: Bogføring af udlæg, løn og andre udgifter.

Time: Registrering og opbevaring of behandling af time- og fraværs registreringer, registrering af ferie, fraværsregistrering og generering af løngrundlag til lønsystem.

Academy: Opskrivning af deltagere til, gennemførelse af, samt dokumentation af kursus.

Se også A.5.

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

De personoplysninger, som behandles af databehandleren i forbindelse med den dataansvarliges brug af databehandlerens Tjenester er forskellige alt efter hvilken kategori den registrerede tilhører, jf. følgende oversigt:

Zenegy Payroll:

KATEGORIER AF DATASUBJEKTER	PERSONOPLYSNINGER
Den dataansvarlige og/eller dennes klienter, herunder kontaktpersoner hos den dataansvarlige og/eller dennes klienter	• Kontaktpersoner hos den dataansvarlige, herunder disses kontaktoplysninger, så som telefon, email, titel, afdeling, adresse • Bankkonti til brug for Applikationen • Medlem af arbejdsgiverforening • Medlem af ferieordninger
Den dataansvarliges (eller dennes klienters) nuværende og tidligere medarbejdere	• Navn • Adresse • CPR-nummer • Kontaktoplysninger, herunder telefon, email, titel, afdeling, adresse • Navn og kontaktoplysninger for medarbejdernes pårørende • Løn • Skat og skattefradrag • Arbejdsmarkedsbidrag • ATP bidrag • Sociale bidrag • Pensionsbidrag • Fravær (f.eks. grundet sygdom, barsel, militærtjeneste, borgerligt ombud, periodiske ansættelser, o.s.v.) • Opgørelse af feriedage • Tillæg (f.eks. medarbejderens rejseudlæg, kørselsgodtgørelse, m.v.) • Fradrag (herunder den dataansvarliges udlæg, fagforeningskontingent, A-kasse bidrag, efterlønsbidrag, m.v.) • Time-/tidsregistreringer • Registrering af enheder og adgange, som er tildelt medarbejderen • Oversigt over kurser medarbejderen har deltaget i • Bankkonti til brug for lønudbetaling • Uploadede dokumenter (f.eks. ansættelseskontrakt, MUS-samtaler, straffeattest, o.s.v.)

Zenegy Expense:

KATEGORIER AF DATASUBJEKTER	PERSONOPLYSNINGER
Den dataansvarlige, herunder kontaktpersoner hos den dataansvarlige	Kontaktpersoner hos den dataansvarlige, herunder disses kontaktoplysninger, så som telefon, e-mail, titel, afdeling og adresse Bankkonti til brug for Applikationen
Den dataansvarliges nuværende og tidligere medarbejdere	Kontaktoplysninger, herunder telefon, email, titel, afdeling, adresse Medarbejderudlæg
Support af den dataansvarlige	Navn Adresse CVR-nummer Kontaktoplysninger, så som telefon, e-mail, titel, afdeling og adresse

Zenegy Numbers:

KATEGORIER AF DATASUBJEKTER	PERSONOPLYSNINGER
Den dataansvarlige, herunder kontaktpersoner hos den dataansvarlige	Kontaktpersoner hos den dataansvarlige, herunder disses kontaktoplysninger, så som telefon, e-mail, titel, afdeling og adresse Bankkonti til brug for Applikationen
Den dataansvarliges nuværende og tidligere medarbejdere	Kontaktoplysninger, herunder telefon, email, titel, afdeling, adresse Medarbejderudlæg
Support af den dataansvarlige	Navn Adresse CVR-nummer Kontaktoplysninger, så som telefon, e-mail, titel, afdeling og adresse
Den dataansvarliges kunder (alene i tilfælde hvor den dataansvarlige anvender det relevante personfølsomme data til fx fakturering)	Navn Adresse CPR nummer

Zenegy Time:

KATEGORIER AF DATASUBJEKTER	PERSONOPLYSNINGER
Den dataansvarlige, herunder kontaktpersoner(administratorer) hos den dataansvarlige	Kontaktpersoner hos den dataansvarlige, herunder disses kontaktoplysninger, så som navn, telefon, e-mail
Den dataansvarliges medarbejdere (brugere)	Kontaktoplysninger, herunder: Medarbejdernummer, Navn Email Timeregistreringer Fraværsregistreringer Kørselsregistreringer

Zenegy Academy:

KATEGORIER AF DATASUBJEKTER	PERSONOPLYSNINGER
Kursusdeltager	Kontaktoplysninger, herunder: Navn Email Stillingsbetegnelse Oplysninger om kursusgennemførelse

A.4. Behandlingen omfatter følgende kategorier af registrerede

Se oversigten i afsnit A.3.

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige fortsætter, så længe den dataansvarlige gør brug af de tjenester, der leveres af den databehandler, som den dataansvarlige abonnerer på, som beskrevet eller henvist til i den gældende kommercielle aftale, vilkår og betingelser, eller via kundens konto.

Særligt for Zenegy Payroll:

Ved ophør af abonnementsaftalen vil den dataansvarliges data blive slettet efter 7 dage. Hvis den dataansvarlige inden udløbet af 7-dages perioden fortsat ønsker, at data opbevares af databehandleren, skal den dataansvarlige genaktivere abonnementet.

Såfremt den dataansvarlige har valgt, at medarbejdere skal have adgang til Zenegy's app, har en medarbejder, hvis tilknytning til den dataansvarlige ophører, fortsat adgang til egne oplysninger indtil den dataansvarlige vælger at slette oplysningerne.

Særligt for Zenegy Expense:
Ved abonnementsaftalens ophør har den dataansvarlige mulighed for at downloade data, som herefter slettes efter 7 dage.

Særligt for Zenegy Numbers:
Uagtet at abonnementsaftalen ophører beholder Zenegy Numbers data løbende år plus fem år.

Særligt for Zenegy Time:
Ved ophør af abonnement har den dataansvarlige retten til at få data udleveret i et digitalt læsbart format. Dette sker ved at den dataansvarlige selv eksporterer data via de rapporterings og eksportværktøjer der er indbygget i applikationen.
Databehandleren har ret til at slette data 3 måneder efter abonnementsaftalen er ophørt.

Se i øvrigt C.4.

Bilag B - Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved ikrafttrædelsen af Klausulerne giver den dataansvarlige tilladelse til at benytte de underdatabehandlere, der er anført på følgende URL: https://zenegy.com/underdatabehandlere Listen udgør en integreret del af denne Databehandleraftale og kan opdateres af databehandleren i overensstemmelse med bestemmelserne heri.

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

Se Bestemmelse 7.3.

Bilag C - Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Ved den dataansvarliges brug af den cloud-baserede **Zenegy Payroll** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget lønadministrator - behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere og/eller klienter (inkl. dennes medarbejdere) i forbindelse med den dataansvarliges lønadministration, herunder lønkørsel, ferie- og fravær, kørsel og tidsregistrering, indberetning til SKAT og andre myndigheder.

Ved den dataansvarliges brug af den cloud-baserede **Zenegy HR** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator - behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere i forbindelse med den dataansvarliges HR-administration for egne medarbejdere, herunder administration af enheder og adgange tildelt den enkelte medarbejder, kursusadministration, håndtering af medarbejderen udlæg for den dataansvarlige, og lagring af dokumenter, eksempelvis ansættelseskontrakt.

Ved den dataansvarliges brug af den cloud-baserede **Zenegy Expense** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator - behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere, kunder og samarbejdspartnere i forbindelse med den dataansvarliges expense-management aktiviteter.

Ved den dataansvarliges brug af den cloud-baserede **Zenegy Numbers** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator – behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere, kunder, leverandører og samarbejdspartnere i forbindelse med den dataansvarliges bogførings- og regnskabsmæssige aktiviteter

Ved den dataansvarliges brug af den cloud-baserede **Zenegy Time** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator – behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere eller klienter i forbindelse med den dataansvarliges administration af tidsregistreringer, herunder time registrering og fraværs registrering.

Ved den dataansvarliges brug af den cloud-baserede **Zenegy Academy** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator – behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere i forbindelse med den dataansvarliges uddannelsesmæssige aktiviteter for medarbejdere.

Den dataansvarlige og/eller dennes klienters medarbejdere indlæser selv de oplysninger, som er nødvendige for brug af Tjenesterne. Den dataansvarlige instruerer herudover databehandleren i løbende og automatisk at indhente oplysninger fra relevante myndigheder, for at sikre, at de anvendte oplysninger om medarbejdernes forhold er opdaterede, når Tjenesterne bruges.

Tjenesterne er udviklet med åbent API, som gør det muligt for andre at udvikle og tilbyde apps, der kan kommunikere med Applikationen, herunder udveksle oplysninger på tværs af programmerne ("Tredjeparts-app(s)"). I det omfang den dataansvarlige og/eller dennes klienter vælger at installere og gøre brug af Tredjeparts-apps, der kan kommunikere med Applikationen, anses det for at udgøre en instruktion til databehandleren om, at der kan ske overførsel af de i Applikationen indtastede/indlæste og de af Applikationen generede oplysninger til sådanne Tredjeparters apps.

Den dataansvarlige accepterer desuden, at dennes og/eller klienters medarbejdere har mulighed for at installere og gøre brug af Tredjeparts-apps, der kan kommunikere og udveksle den enkelte medarbejders oplysninger med Applikationen, og at sådan databehandling er omfattet af instruksen ifølge denne aftale.

Den dataansvarligere giver tilsvarende instruks om, at også den dataansvarliges og/eller klienters medarbejdere kan vælge at installere og gøre brug af Tredjeparts-apps, der kan kommunikere med Applikationen, og instruere databehandleren i, at der i så fald kan ske overførsel af de i Applikationen indtastede/indlæste og de af Applikationen generede oplysninger, som medarbejderen har adgang til, til sådanne Tredjeparters apps.

Zenegy anonymiserer de oplysninger, der er angivet i A.3., til statistiske og træningsformål, forbedring af produkter og tjenester samt behandler oplysningerne i det omfang, det kræves ved lov, herunder i forbindelse med en retsafgørelse, regulatoriske krav, den dataansvarliges konkurs, dødsfald eller lignende.

Der henvises i øvrigt til de aftalte vilkår i databehandlerens abonnementsbetingelser.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle at behandlingen af data både er normale personoplysninger, men også omfatter personoplysninger omfattet af databeskyttelsesforordningen artikel 9 om særlige kategorier af personoplysninger, hvorfor der er etableret et højt sikkerhedsniveau.

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

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

ISAE 3402
Zenegy gennemgår hvert år et audit der resulterer i en ISAE 3402 erklæring.
Denne offentliggøres på Zenegys hjemmeside under Zenegy Trust Center

Service og database lokation:
Databehandleren har fysisk adskilt sine produktions (Zenegy Produktion) og test (Zenegy Beta) databaser.

Zenegy - Beta er lokaliseret i North Europe - Dublin – Irland

Zenegy - Produktion er lokaliseret i West Europe - Amsterdam – Holland

Der henvises desuden til Bilag B.1.

Data kryptering
Data er krypteret både under transport og "at rest".

Database tilgængelighed
Data opbevares i Azure.
Adgangen er begrænset til meget få brugere.

Passwords
Passwords er SHA256 krypteret med unik salt.

Backup
Databehandleren bruger Azure til at hoste sin applikation og sit API.
Backup politikken er sat til at bevare 5 tidligere versioner af applikationen.

Databehandleren bruger Azure til at hoste sin database.
Backup politikken er sat til at tage fuld backup hver uge.

Yderligere er funktionen "Point-in-time" backup sat op således at databasen kan genskabes til et hvilket som helst tidspunkt 35 dage tilbage i tiden.

Der kan læses mere om Azure continuity her:
https://azure.microsoft.com/en-us/updates/point-in-time-restore-retention-for-standard-edition-extended-to-35-days/

Backup af databasen har det formål at kunne rekonstruere hele databasen og miljøet. Backup har således ikke det formål at kunne genetablere enkelt kunders data.

Tredjepart og leverandør risikovurdering
Databehandleren gennemfører årlige reviews af sine leverandører og tredjepartere.

Det sker konkret ved gennemgang af databehandleraftaler for de enkelte leverandører, samt verifikation af om aktiviteter følger databehandleraftalen og behandlingsgrundlaget.

For alle leverandører der behandler data udføres der en risikovurdering.
Denne vurdering tager udgangspunkt i datasubjektet og er baseret på en risiko matrix.

Brugers adgang til data via browser
Adgang til Applikationen sker via internettet via en webbrowser der understøtter SSL / https.

Databehandleren har implementeret mulighed for dataansvarlige for at implementere stærke adgangskoder der skifter hver 90. dag.

Databehandleren har implementeret mulighed for dataansvarlige for at implementere Multi Faktor Adgang.

Alle Databehandlerens interne brugere tilgår Applikationen med alle sikkerhedsfunktioner slået til.

Brugers adgang til data via API
Databehandleren stiller et REST API til rådighed. Det er udelukkende dataansvarlige som kan give adgang til dataansvarliges data i Applikationen.

Adgang administreres på flere niveauer.

- En bruger af API'et kan ikke få adgang til mere end den rolle som brugeren har i Applikationen.
- Databehandleren bruger industristandarden OAuth 2.0.
- Apps er begrænset af den uri som er lagt ind ved oprettelse.
- Apps kan kun tilgå dataansvarliges data via https
- Apps kan have yderligere begrænsninger i form af Scopes som oprettes samtidig med Appen.

Der kan læses mere om REST API'et her:
https://developers.zenegy.com/

Der kan læses mere om OAuth 2.0 her:
https://aaronparecki.com/oauth-2-simplified/

Fysisk adgang til databehandlerens **faciliteter**
Databehandleren opererer som en lukket facilitet selv om der ikke behandles oplysninger fysisk.

Alle besøgende logges.

Databehandleren bruger et adgangskort baseret system.

Kort opgøres løbende i et system i forbindelse med opsigelse og ansættelser samt ved årlig kontrol.

Hjemmearbejdspladser
Databehandlerens medarbejdere har mulighed for at arbejde hjemmefra.
Alle computere er krypterede og adgangskodebeskyttet.
Systemer er kodeords og/eller Multi Faktor beskyttet.

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 sådanne tekniske og organisatoriske foranstaltninger, som kan bidrage til den dataansvarliges mulighed for at besvare anmodninger om udøvelsen af de registreredes rettigheder.

C.4 Opbevaringsperiode/sletterutine

Data opbevares så længe den dataansvarlige finder, at det opfylder det formål som den dataansvarlige har. Databehandleren stiller funktioner til rådighed for den dataansvarlige, således at den dataansvarlige kan leve op til de formål.

Såfremt den dataansvarlige opsiger sin aftale med Databehandleren, har Databehandleren bygget funktionalitet der muliggør eksport og sletning af data.
Databehandleren pakker al data digitalt, således at den dataansvarlige har mulighed for at downloade og overføre data til andet system.

Særligt for Zenegy Payroll:

Hvis den dataansvarlige opsiger sin abonnementsaftale med Zenegy, har Zenegy etableret funktionalitet, der muliggør eksport og sletning af data inden for 7 dage.

Særligt for Zenegy Expense

Eksport af data:
Applikationen har indbygget funktionalitet der muliggør at dataansvarlig ved egen kraft kan eksportere data, herunder kassekladde, posteringer inklusive bilag, betalingskort, leverandører og lister med alle udgifter.

Sletning af data:
Den data ansvarlige kan vælge at slette sine data via indbygget funktionalitet i Applikationen.
Når den dataansvarlige har valgt at slette data starter en periode hvor konto'en er låst på 7 dage. I denne periode kan dataansvarlige fortryde sin sletning. Herefter slettes data uigenkaldeligt.

Særligt for Zenegy Numbers:

Såfremt den dataansvarlige opsiger sin aftale med Zenegy, er Zenegy forpligtet til at opbevare data i 5 år efter aftales ophør.

Særligt for Zenegy Time:

Se Bilag A.5.

Særligt for Zenegy Academy:

For Zenegy Academy gælder, at ved den dataansvarliges opsigelse af Academy abonnement, slettes data senest 30 dage efter udløb af abonnementsperioden.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan med den dataansvarliges forudgående generelle godkendelse jf. C.1 og C.6 samt forudgående varsel til den dataansvarlige jf. 7.3, ske på andre lokaliteter end følgende:

Se B.1. Godkendte underdatabehandlere.

Se C.2. Behandlingssikkerhed - Service og database sikkerhed.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige er bekendt med – og er forpligtet til at gøre sine medarbejdere bekendt med - at databehandlerens Tjenester stilles til rådighed via en cloud-baseret løsning, hvor databehandleren blandt andet gør brug af software og IT-systemer, herunder servere, der stilles til rådighed af tredjeparter.

I det omfang databehandlerens Ydelser gør brug af eller er baseret på ydelser leveret af underdatabehandlere i tredjelande, instruerer og bemyndiger den dataansvarlige hermed databehandleren til at overføre personoplysninger til databehandlerens underdatabehandlere i sådanne tredjelande med henblik på levering af tjenester, som den dataansvarlige abonnerer på, som angivet i den gældende kommercielle aftale, vilkår og betingelser eller via kundens konto.

Brugen af underdatabehandlere i tredjelande skal være underlagt tilsvarende bestemmelser som de Bestemmelser, der er aftalt mellem den dataansvarlige og databehandleren, ligesom databehandleren er forpligtet til at sikre, at overførslen og databehandlingen sker i henhold til kravene i databeskyttelsesforordningen Kapitel V (Overførsel af personoplysninger til tredjelande eller internationale organisationer).

Ved Databehandlerens konkurs, opretholdees Underdatabehandleres forpligtelser til at behandle data sikkert og i overenstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[2] nationale ret og disse Bestemmelser

Overførslen til tredjelande sker i henhold til (i) EU-U.S. Data Privacy Framework, (ii) EU-Kommissionens standardbestemmelser om databeskyttelse, (iii) en adequacy beslutning fra EU-Kommissionen (Fx EU-US Data Privacy Framework) eller (iv) databeskyttelsesforordningens artikel 47, hvor overførslen sker til ét eller flere medlemmer af en koncern underlagt retligt bindende virksomhedsregler (Binding Corporate Rules).

Se tillægsaftale om EU Standardkontraktbestemmelser (Modul 3).

Se oversigt over virksomheder med godkendte bindende virksomhedsregler (pre-GDPR).

Se oversigt over virksomheder med godkendte bindende virksomhedsregler (post-GDPR).

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.

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

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

Databehandleren skal i perioden juli til oktober hvert år 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 3402

Revisionserklæringen gøres uden unødig forsinkelse offentligt tilgængelig på databehandlerens hjemmeside, www.zenegy.com, under Zenegy Trust Center, til den dataansvarlige til orientering.

Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde for egen regning og risiko anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

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.

Databehandler stiller muligheden til rådighed for den dataansvarlige eller en repræsentant for den dataansvarlige for at foretage en årlig inspektion, herunder fysisk inspektion, af 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 inspektion afholdes af den dataansvarlige selv.

Databehandleren er 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 kan foretage årligt en fysisk inspektion af lokaliteterne, hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske 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 planlagte tilsyn, kan databehandleren gennemføre en inspektion med underdatabehandleren, når databehandleren 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 for egen regning og risiko anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til 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 for egen regning og risiko vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker I overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandlerens og underdatabehandlerens udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende, medmindre inspektionen er initieret af den dataansvarlige, der er for dataansvarliges egen regning og risiko.

Bilag D - Parternes regulering af andre forhold

Som supplement til Bestemmelserne har Parterne aftalt følgende:

Vedr. Bestemmelse 4.2:

Uanset Bestemmelse 4.2, er databehandleren ikke forpligtet til aktivt at efterprøve eller undersøge lovligheden af den dataansvarliges instrukser.

Den dataansvarlige er bekendt med, at databehandleren er afhængig af den dataansvarliges anvisninger om, i hvilket omfang databehandleren er berettiget til at anvende og behandle personoplysningerne på den dataansvarliges vegne.

Databehandleren hæfter derfor ikke for krav, der udspringer af databehandlerens handlinger eller undladelser, i det omfang disse handlinger eller undladelser er en direkte databehandlingsaktivitet udøvet i overensstemmelse med den dataansvarliges instrukser.

Vedr. Bestemmelse 7.3:
Den dataansvarlige anerkender, at databehandlerens Tjenester er standardiserede, cloud-baserede abonnementsydelser, der stilles til rådighed for et stort antal kunder, og at databehandleren derfor ikke har mulighed for at indrette de tilbudte systemer således, at hver kunde kan stille krav om, at databehandleren ikke må gøre brug af bestemte underdatabehandlere, som databehandleren i øvrigt har godkendt.

På den baggrund anerkender den dataansvarlige, at såfremt denne har indsigelser mod databehandlerens ændring eller valg af nye underdatabehandlere, og databehandleren ikke imødekommer sådan indsigelse, er den dataansvarliges eneste beføjelse at opsige abonnementsaftalen med databehandleren. Opsigelsen kan ske med øjeblikkelig virkning, og ingen af parterne har nogen krav mod hinanden i anledning heraf.

Vedr. Bestemmelse 9.2:
I det omfang den dataansvarlige ønsker databehandlerens bistand til de ydelser, der er beskrevet under Bestemmelse 9.2.3 og 9.2.4, er den dataansvarlige forpligtet til at vederlægge databehandleren for den herved anvendte tid i henhold til de til enhver tid anvendte timesatser som kan oplyses ved henve.

Vedr. Bestemmelse 12.1:

Databehandleren er forpligtet til at afsætte de ressourcer, der er nødvendig(e) for, at den dataansvarlige eller dennes rådgiver/repræsentant kan gennemføre sin inspektion og/eller revision hos databehandleren eller dennes underdatabehandlere. "Databehandlerens udgifter i forbindelse med en fysisk inspektion og/eller en på vegne den dataansvarlige udført revision hos databehandleren eller dennes underdatabehandlere, afholdes af den dataansvarlige. Databehandlerens og/eller dennes underdatabehandleres tid godtgøres med de af databehandleren til enhver tid anvendte timsatser.

Vedr. Bestemmelse 13.1:
Databehandlerens ansvar overfor den dataansvarlige er begrænset til det i abonnementsbetingelserne anførte, ligesom de i abonnementsbetingelserne i øvrigt anførte bestemmelser finder anvendelse mellem den dataansvarlige og databehandleren, bortset fra i det omfang de forringer den registreredes grundlæggende rettigheder og frihedsrettigheder ifølge databeskyttelsesforordningen.

Klausul om ældre referencer

For klarhedens skyld skal eventuelle henvisninger i tidligere versioner af denne aftale til 'Bilag E' nu fortolkes som henvisning til beskrivelsen af tjenester, der er beskrevet i den gældende kommercielle aftale, vilkårene og betingelserne eller i kundens kontoabonnementsoplysninger.

Versionshistorik

Version	Ændringer
2023-09-v-1.0	Generelt
2024-09-30-v 1.1	- Første version – konsolidering af samtlige DPA'er for enkelt-produkter leveret af Zenegy. - Tilføjelse af typer af personfølsomme data som Zenegy behandler i forbindelse med Zenegy Numbers, fjernelse af underdatabehandlere som ikke længere anvendes, mindre redaktionelle justeringer.
2025-01-20-v 1.2	- Version 1.2 - kontaktoplysninger opdateret i punkt 16.
2025-04-29- v 1.3	- Version 1.3 - ændring i underdatabehandlere
2025-10-06 - v 1.4	- Version 1.4 – liste over godkendte underdatabehandlere (bilag B1) flyttet til hjemmesiden, bilag E fjernet, opdaterede behandlingsaktiviteter for Microsoft og Horaizon.
2026- 04-14- v. 1.5	- Version 1.5 – opdateret Bilag C; opdateret opbevaringsperiode og sletteprocedurer