Standardkontraktsbestemmelser

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

mellem

Virksomhed:
CVR-nummer:
Adresse:
Post nr. / By:
Land:

herefter "den dataansvarlige"

og

COMAsystem ApS
CVR 33 86 52 79
Øster Allé 48
2100 København Ø
Danmark

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

Indhold

1. 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 COMAsystem 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.

2. 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

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

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.

3. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

4. 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.

5. Behandlingssikkerhed

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

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

   a. Pseudonymisering og kryptering af personoplysninger

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

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

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

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

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

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

6. 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 specifik skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst én måned inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

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

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

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

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

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

7. 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.

8. Bistand til den dataansvarlige

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

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

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

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

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, Carl Jacobsens Vej 35, DK-2500 Valby, (+45) 33 19 32 00, dt@datatilsynet.dk, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

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

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

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, Carl Jacobsens Vej 35, DK-2500 Valby, (+45) 33 19 32 00, dt@datatilsynet.dk, 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.

9. 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.

10. Sletning og returnering af oplysninger

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

11. 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.

12. 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.

13. 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

   På vegne af den dataansvarlige

   Se sidste side i dette dokument

   På vegne af databehandleren

   Se sidste side i dette dokument

14. 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.

Navn	Christian Richter-Pedersen
Stilling	CEO
Telefonnummer	(+45) 69 15 99 60
E-mail	ka@comasystem.eu

Databehandlerens kontaktperson er oplyst på købsfakturaen fra COMAsystem

Bilag A Oplysninger om behandlingen

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

Databehandleren varetager opbevaring og behandling af kundens kontraktdata, som indeholder personhenførbare oplysninger.

Databehandleren behandler kundens kontraktfiler og dokumenter, herunder oplysninger indtastet i systemet af den dataansvarlige. Databehandleren udsender email notifikationer iht. de data som den dataansvarlige angiver i systemet.

Databehandleren må under ingen omstændigheder dele kundens oplysninger
med andre tredjeparter end underdatabehandlere nævnt specifikt i denne aftale, med undtagelse af eksterne retskrav, såfremt disse retskrav stammer fra EU-retten eller medlemsstaternes nationale ret, som databehandleren er underlagt.

Databehandleren må ikke bruge og/eller behandle kundens data i forhold til andre formål.

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

- Modtagelse og lagring af filer og tilstødende metadata leveret af den dataansvarlig.
- Gør det muligt for den dataansvarlige at oprette nye kontrakter og dokumenter på grundlag af de dataansvarliges leverede data.
- Generer rapporter og oversigter samlet fra dataansvarlige leveret data.

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

Personoplysninger (ikke-følsomme oplysninger)

Væsentlige sociale oplysninger	Sygedage	Eksamen	Arbejdsområde
Andre private forhold	Tjenstlige forhold	Ansøgning	Arbejdstelefon
Økonomi	Familieforhold	CV	Navn
Skat	Bolig	Ansættelsesdato	Adresse
Gæld	Bil	Stilling	Fødselsdato
og derudover			

Personoplysninger (følsomme oplysninger)

Race og etnisk oprindelse	Helbredsoplysninger oplysninger
Politisk overbevisning	Om strafbare forhold
Religiøs og filosofisk overbevisning	
Fagforeningsmæssige tilhørsforhold	
Biometriske mhp. entydig indentifikation	
Seksuelle forhold eller seksuel orientering	
Genetiske data	

Fortrolige oplysninger

CPR nummer

A.4. Behandlingen omfatter følgende kategorier af registrerede

Medarbejdere hos den dataansvarlige
Kunder
Leverandører
og derudover

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

Personoplysninger opbevares indtil enten a) aftalen om levering af ydelsen ophører eller b) Databehandleraftalen opsiges eller ophæves.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Front-Safe A/S	29631123	Spotorno Allé 12 DK-2630 Taastrup Søndervangs Alle 20 DK-8260 Viby	Backup
Addo Sign | twoday	29973334	Gærtorvet 1-5 DK-1799 København V **Data lokationer** IT Relation Nygårdsvej 5A DK-2100 København Cloud Factory Vestergade 4, DK-6800 Varde	Digital Signature

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

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:

Som beskrevet i A.1. og A.2.

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle:

At behandlingen kan omfatte personoplysninger, der er underlagt artikel 9 GDPR om "særlige kategorier af personoplysninger", hvorfor der bør 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 etableret det nødvendige (og aftalte) sikkerhedsniveau.

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

Risikovurdering
Databehandleren skal foretage en risikovurdering, og herefter gennemføre passende tekniske og organisatoriske foranstaltninger for at imødegå identificerede risici.

Ekspertise og ressourcer
Databehandleren skal levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere passende tekniske og organisatoriske foranstaltninger til opfyldelse af kravene til behandling af personoplysninger i gældende databeskyttelsesret.

Informationssikkerhedspolitik
Databehandleren skal sikre, at der foreligger en ledelsesgodkendt informationssikkerhedspolitik.

Organisering af informationssikkerhed
Databehandleren skal sikre, at der er fokus på informationssikkerhed i sig selv organisationer med defineret fordeling af roller og ansvar.
Derudover skal Databehandlerens dataadgang til den Dataansvarliges data sikres igennem kontrakter, fortrolighedserklæring og sikring af adskillelse af funktioner for at minimere fejl og misbrug af data.

Medarbejdersikkerhed
Databehandleren skal have etableret en proces for medarbejdere og konsulenter kender deres ansvar i forhold til informationssikkerhed.
Databehandleren skal sikre medarbejdernes bevidsthed om forpligtelser ved beskæftigelse, og denne uddannelse skal opretholdes i hele ansættelsesforholdets varighed.
Databehandleren skal udføre awareness træning af enhver fysisk person, der udfører arbejde for databehandleren, og som får adgang til personoplysninger omfattet af disse Bestemmelser vedrørende deres forpligtelser og denne træning skal vedligeholdes under hele ansættelsesforholdet.

Databehandleren skal sikre, at enhver fysisk person, der udfører arbejde for databehandleren, og som får adgang til personoplysninger omfattet af disse Bestemmelser, kun behandler disse personoplysninger i henhold til den dataansvarliges dokumenterede instruks, medmindre anden behandling kræves i henhold til EU-retten eller national ret.

Forvaltning af aktiver
Databehandleren skal sikre ejerskab af kritiske aktiver og ajourført dokumentation.

Adgangskontrol
Databehandleren skal have en dokumenteret adgangsstyringsproces og sikre adgang kun tildeles på baggrund af et arbejdsrelateret behov.

Databehandleren skal have fastlagte procedurer for oprettelse, lukning og løbende gennemgang af tildelte rettigheder ud fra princippet om et arbejdsrelateret behov samt beslutningen om funktionsadskillelse.
Databehandleren skal have procedurer for sikker log ind for at minimere mulighederne for uautoriseret adgang til systemer og applikationer.

Kryptografi
Databehandleren skal sikre kryptering med ajourført krypteringsniveau på kommunikation over åbne netværk og mellem systemer samt sikre, at administration af nøgler foregår efter en dokumenteret proces.

Fysisk sikkerhed og miljøsikkerhed
Databehandleren skal organisere og etablere fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker på Databehandlerens fysiske placeringer. Databehandleren skal endvidere sikre beskyttelse mod uautoriseret adgang til Databehandlerens fysiske placeringer via adgangskontrolproces for alle med adgang.

Driftssikkerhed
Databehandleren skal sikre, at driftsprocedurer dokumenteres og vedligeholdes. Som som minimum skal følgende procedurer inkluderes:

- malware beskyttelse
- backup
- logning og overvågning
- styring af driftssoftware
- sårbarhedshåndtering

Kommunikationssikkerhed
Databehandleren skal sikre, at netværk administreres og kontrolleres for at beskytte Information. Databehandleren skal sikre, at den Dataansvarliges data, som kommunikeret internt og eksternt, behandlet lovmæssigt korrekt, etisk og kommercielt i løbet af informationens levetid.
Databehandleren skal sikre, at den dataansvarliges data, der kommunikeres internt og eksternt, behandles korrekt lovgivningsmæssigt, etisk og forretningsmæssigt forsvarligt i informationernes levetid. Derudover skal adgang til netværket være beskyttet.

Anskaffelse, udvikling, vedligeholdelse og bortskaffelse af systemer
Databehandleren skal sikre, at sikkerhedskrav til anskaffelse, udvikling, vedligeholdelse og bortskaffelse er integreret i løsningerne, samt kravene i databeskyttelsesforordningen databeskyttelse gennem design og standardindstillinger overholdes.

Ændringer i systemer
Databehandleren skal sikre, at ændringer i it-systemer følger en dokumenteret forandringsproces med relevante godkendelser og test.
Databehandleren skal sikre, at udvikling, test og operativsystemer holdes adskilt og at kapacitet og ydeevne overvåges og styres.

Leverandørforhold
Databehandleren skal mindst stille samme sikkerhedskrav til underdatabehandlere og andre underleverandører, der henvender sig til Databehandleren og sikrer overholdelse af disse.

Håndtering af brud på informationssikkerheden
Databehandleren skal registrere, og risikovurderer informationssikkerhedshændelser og

indberette disse til den dataansvarlige uden unødig forsinkelse. Databehandleren skal udarbejde procedurer for indsamling af beviser i tilfælde af informationssikkerhedshændelser.

Informationssikkerhedsaspekter af nød-, beredskabs- og genopretningsstyring
Databehandleren skal have udarbejdet beredskabsplaner, der definerer hvordan systemer eller tjenester genetableres rettidigt. Disse beredskabsplaner skal testes årligt eller kl store ændringer.

Overholdelse (Compliance)
Databehandleren skal løbende kontrollere, om systemer og tjenester opfylder kravene Databehandlerens sikkerhedskrav samt effektiviteten og kapaciteten af sikkerhedskravene at sikre løbende fortrolighed, integritet, tilgængelighed og robusthed af systemer og tjenester.
Databehandleren leverer en årlig ISAE 3000 type II revisorerklæring.

C.3 Bistand til den dataansvarlige
Databehandleren skal sikre, at den dataansvarlige uden unødig forsinkelse modtager underretning om enhver anmodning fra en registreret om udøvelse af dennes rettigheder, modtaget af databehandleren. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret omkring udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret.

Databehandleren yder den dataansvarlige den assistance som påkrævet i overensstemmelse med Bestemmelse 9.1 og 9.2 uden modtagelse af vederlag for databehandlerens medgået tid.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares så længe den dataansvarlige har sin individuelle konto i det leverede system. Ved sletning af enhver enhed vil dataene eksistere i databehandlerens backup i op til 180 dage, hvorefter de slettes automatisk og uigenkaldeligt.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

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

Global Connect :
Datacenter co-location
Høreskætten 3
2630 Taastrup

Front-Safe :
Spotorno Allé 12
DK-2630 Taastrup

Søndervangs Alle 20
DK-8260 Viby

Visma ADDO (Twoday) :

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Databehandleren er ikke instrueret i at overføre personoplysninger til tredjelande eller internationale organisationer.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

Databehandler anvender ikke overførsler til tredjelande ifm. behandlingen.

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

Databehandleren skal årligt for databehandlerens regning indhente en ISAE 3000 type II 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 Revisionserklæring kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE 3000 type II for COMAsystem ApS

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

Baseret på resultaterne af revisionserklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.
Den dataansvarliges eventuelle udgifter i forbindelse med en 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. Databehandlerens eventuelle udgifter i forbindelse med en inspektion afholdes af databehandleren selv og er den dataansvarlige uvedkommende.

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

Databehandleren eller en repræsentant for databehandleren foretager inspektion ved enten (i) at gennemgå revisionserklæringer, (ii) at fremsende spørgeskema til underdatabehandleren, som underdatabehandleren skal besvare, og/eller (iii) foretager en planlagt 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 den planlagte inspektion, kan databehandleren gennemføre en uplanlagt inspektion hos underdatabehandleren, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for og resultaterne af 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.

Baseret på resultaterne af inspektionen, er den dataansvarlige berettiget til 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 – hvis det findes nødvendigt – 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.

Den dataansvarliges eventuelle udgifter i forbindelse med en inspektion afholdes af den dataansvarlige selv. Databehandleren og underdatabehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion. Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med en inspektion afholdes af databehandleren og underdatabehandleren selv og er den dataansvarlige uvedkommende

Bilag D Parternes regulering af andre forhold

D.1 Roller

Den dataansvarlige kan være dataansvarlig såvel som databehandler for de personoplysninger, som databehandleren skal behandle i henhold til disse Bestemmelser. Såfremt den dataansvarlige agerer som databehandler, agerer databehandleren som underdatabehandler. Dette ændrer dog ikke ved parternes rettigheder og forpligtelser efter denne databehandleraftale.

D.2 Overholdelse af databeskyttelsesregler

Databehandlerens behandling af personoplysninger i medfør af disse Bestemmelser skal overholde reglerne i den til enhver tid gældende danske og europæiske databeskyttelsesret, herunder men ikke begrænset til Lov 2018-05-23 nr. 502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (*Databeskyttelsesloven*).

D.3 Sikkerhedsforanstaltninger

Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver manglende overholdelse af databehandlerens sikkerhedsforpligtelser, der fremgår af disse Bestemmelser, uanset om dette beror på manglende overholdelse hos databehandleren eller dennes eventuelle underleverandører.

D.4 Sikkerhedsbrud

Databehandleren må ikke udsætte sådan underretning om brud på persondatasikkerheden (eller mistanken herom) som følge af, at databehandleren endnu ikke har fyldestgørende informationer til rådighed. I sådanne tilfælde skal databehandleren give sådanne informationer, som er tilgængelige.

Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud eller manglende overholdelse af disse Bestemmelser uden forudgående skriftlig aftale med den dataansvarlige om indholdet af en sådan kommunikation, medmindre databehandleren er forpligtet til en sådan kommunikation efter lovgivningen.

D.5 Datatilsynet og andre offentlige myndigheder

Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver henvendelse rettet til databehandleren eller dennes eventuelle underleverandører fra i) Datatilsynet vedrørende behandling af personoplysninger omfattet af disse Bestemmelser, eller ii) fra en myndighed om videregivelse af personoplysninger omfattet af disse Bestemmelser, medmindre orientering af den Dataansvarlige er forbudt i henhold til EU-retten eller lovgivningen i en medlemsstat.

Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til Bilag C, pkt. C.7 og C.8 til Datatilsynet (eller andre relevante myndigheder), efter anmodning herom fra Datatilsynet (eller andre relevante myndigheder).

D.6 Vederlag

Databehandlerens forpligtelser i henhold til disse Bestemmelser medfører ikke krav på særskilt betaling til databehandleren. Databehandlerens udgifter vedrørende databehandlerens underleverandører er endvidere den dataansvarlige uvedkommende.

D.7 Ansvar

Uanset hvad der måtte fremgå af andre aftaler indgået mellem parterne, skal databehandleren skadesløsholde den dataansvarlige, såfremt den dataansvarlige bliver mødt med krav fra tredjemand, som følge af, at databehandleren i sin rolle som databehandler eller databehandlerens eventuelle underleverandører i deres rolle som underdatabehandlere har overtrådt den til enhver tid gældende databeskyttelseslovgivning. Databehandleren hæfter kun for skader, hvis databehandleren eller dennes eventuelle underleverandører ikke har opfyldt sine forpligtelser som databehandler og/eller underdatabehandlere, som det følger af den til enhver tid gældende lovgivning, eller hvis databehandleren som databehandler eller dennes eventuelle underleverandører som underdatabehandlere har undladt at følge eller handlet i strid med den dataansvarliges lovlige og dokumenterede instruks. Forpligtelsen til at skadesløsholde den dataansvarlige er ikke omfattet af en eventuelt aftalt erstatningsmaksimering i

andre aftaler indgået mellem parterne. Databehandlerens forpligtelse til at skadesløsholde den dataansvarlige gælder dog ikke for bøder pålagt den dataansvarlige i medfør af databeskyttelsesforordningens artikel 83 eller sanktioner fastlagt i Danmark i overensstemmelse med databeskyttelsesforordningens artikel 84.

Den Dataansvarlige skadesløsholde databehandleren, såfremt databehandleren bliver mødt med krav fra tredjemand som følge af, at den dataansvarlige i sin rolle som dataansvarlig har overtrådt den til enhver tid gældende persondataretlige lovgivning. Den dataansvarlige hæfter kun for skader, hvis den dataansvarlige ikke har opfyldt sine forpligtelser som dataansvarlig, som det følger af den til enhver tid gældende lovgivning. Forpligtelsen til at skadesløsholde databehandleren er ikke omfattet af en evt. aftalt erstatningsmaksimering i andre aftaler mellem parterne. Den dataansvarliges forpligtelse til at skadesløsholde databehandleren efter nærværende afsnit gælder ikke for bøder pålagt databehandleren i medfør af databeskyttelsesforordningens artikel 83 eller sanktioner fastlagt i Danmark i overensstemmelse med databeskyttelsesforordningens artikel 84.

D.8 Opsigelse

I det omfang den dataansvarlige gør indsigelse mod planlagte ændringer vedrørende tilføjelse eller udskiftning af en underdatabehandler og databehandleren fastholder den planlagte ændring, er den dataansvarlige berettiget til at opsige aftalen, som defineret under disse Bestemmelsers pkt. 2.3 samt disse Bestemmelser med virkning fra udløbet af det varsel på mindst 3 måneder, som databehandleren er forpligtet til at give den dataansvarlige, jf. disse Bestemmelsers pkt. 7.3.

Opsigelsen i henhold til dette punkt, medfører ikke krav på særskilt betaling til databehandleren.

D.9 Forrang

I tilfælde af uoverensstemmelse mellem disse Bestemmelser og bestemmelserne i andre skriftlige eller mundtlige aftaler indgået mellem parterne, skal disse Bestemmelser have forrang, medmindre strengere krav til behandlingssikkerheden er fastsat i andre skriftlige eller mundtlige aftaler indgået mellem parterne