Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på underdatabehandlerens behandling af personoplysninger ved leverance af Infrastructure as a Service

mellem

Visma IMS A/S
CVR 25862015
Søren Frichs Vej 44D,
8230 Åbyhøj
Danmark

herefter "databehandler"

og

CLOUD FACTORY A/S
CVR.nr 35393692
VESTERGADE 4
6800 VARDE
DANMARK

herefter "underdatabehandleren"

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

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

1. Indhold

2. Præambel

1. Disse Bestemmelser fastsætter de rettigheder og forpligtelser, som finder anvendelse, når underdatabehandleren foretager behandling af personoplysninger for databehandleren og på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3-4, 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. Underdatabehandlerens behandling af personoplysninger sker i forbindelse med levering af Infrastruktur as a Service med henblik på opfyldelse af parternes allerede indgåede aftale, PARTNERAFTALE OM CLOUD-LØSNINGER af 07.06.2020

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

5. Underdatabehandleraftalen og Hovedaftalen er indbyrdes afhængige og kan ikke opsiges særskilt.

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

7. 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.

8. Bilag B indeholder den databehandlerens betingelser for underdatabehandlerens brug af underdatabehandlere i yderligere led og en liste af underdatabehandlere i yderligere led, som databehandleren har godkendt brugen af.

9. Bilag C indeholder en nærmere instruks om, hvilken behandling underdatabehandleren skal foretage på vegne af databehandleren, hvilke sikkerhedsforanstaltninger, der som minimum skal gennemføres, og hvordan der føres tilsyn med underdatabehandleren og eventuelle underdatabehandlere i yderligere led.

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

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

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel

24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Databehandleren er underlagt den dataansvarliges instruks, og den dataansvarlige har derfor over for databehandleren både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

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. Underdatabehandleren handler efter instruks

1. Underdatabehandleren må kun behandle personoplysninger efter dokumenteret instruks fra databehandleren, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som underdatabehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af databehandleren på vegne 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. Underdatabehandleren underretter omgående databehandleren, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Underdatabehandleren må kun give adgang til personoplysninger, som behandles på databehandlerens vegne, til personer, som er underlagt underdatabehandlerens 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. Underdatabehandleren skal efter anmodning fra databehandleren kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Underdatabehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, 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.

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

Underdatabehandleren 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. Underdatabehandleren bistår databehandleren og den dataansvarlige med overholdelse af forpligtelser efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for databehandleren vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som underdatabehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for databehandlerens overholdelse af sin forpligtelse efter forordningens artikel 32.

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

7. Anvendelse af underdatabehandlere i yderligere led

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

2. Underdatabehandleren må således ikke gøre brug af en underdatabehandler yderligere led til opfyldelse af disse Bestemmelser uden forudgående generel eller specifik godkendelse fra den databehandleren.

3. Underdatabehandleren har databehandlerens generelle godkendelse til brug af underdatabehandlere i yderligere led. Underdatabehandleren skal skriftligt underrette databehandleren om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere i yderligere led med mindst 30 dages varsel og derved give databehandleren mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e) i yderligere led. Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som databehandleren allerede har godkendt, fremgår af bilag B.

4. Når underdatabehandleren gør brug af en underdatabehandler i yderligere led i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af databehandleren, skal underdatabehandleren, gennem en kontrakt eller andet retligt dokument i

henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren i yderligere led de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren i yderligere led vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Underdatabehandleren er derfor ansvarlig for at kræve, at en underdatabehandler i yderligere led som minimum overholder underdatabehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) med underdatabehandlere i yderligere led og eventuelle senere ændringer hertil sendes – efter databehandlerens anmodning herom – i kopi til databehandleren, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren i yderligere led. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af en underdatabehandleraftale med en underdatabehandler i yderligere led, skal ikke sendes til databehandleren.

6. Underdatabehandleren skal i sine aftaler med underdatabehandlere i yderligere led indføje databehandleren som begunstiget tredjemand i tilfælde af underdatabehandlerens konkurs, således at databehandleren kan indtræde i underdatabehandlerens rettigheder og gøre dem gældende over for underdatabehandlere i yderligere led, som f.eks. gør databehandleren i stand til at instruere underdatabehandlere i yderligere led i at slette eller tilbagelevere personoplysningerne.

7. Hvis en underdatabehandler i yderligere led ikke opfylder sine databeskyttelsesforpligtelser, forbliver underdatabehandleren fuldt ansvarlig over for databehandleren og den dataansvarlige for opfyldelsen af underdatabehandleren i yderligere leds 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 og underdatabehandlere i yderligere led.

8. Overførsel til tredjelande eller internationale organisationer

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

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som underdatabehandleren ikke er blevet instrueret i at foretage af databehandleren, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal underdatabehandleren underrette databehandleren 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 databehandleren kan underdatabehandleren 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 yderligere led i et tredjeland
c. behandle personoplysningerne i et tredjeland, herunder i underdatabehandlerens evt. afdelinger i tredjelande

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

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

9. Bistand til den dataansvarlige

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

   Dette indebærer, at underdatabehandleren så vidt muligt skal bistå den dataansvarlige og databehandleren 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. Underdatabehandleren bistår den dataansvarlige og databehandleren med at sikre overholdelse af den dataansvarliges og databehandlerens forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for underdatabehandleren, jf. art 28, stk. 3, litra f. Dette indebærer, at underdatabehandleren under hensynstagen til behandlingens karakter skal bistå den dataansvarlige og databehandleren i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. Forpligtelsen til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det

er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

b. 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. Forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

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

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed underdatabehandleren skal bistå den dataansvarlige og databehandleren samt i hvilket omfang og udstrækning.

10. Underretning om brud på persondatasikkerheden

1. Underdatabehandleren underretter uden unødig forsinkelse databehandleren efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden hos underdatabehandleren eller en evt. underdatabehandler i yderligere led.

2. Underdatabehandlerens underretning til databehandleren skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at databehandleren kan underrette den dataansvarlige rettidigt, og den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

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

   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. foranstaltninger der er truffet eller foreslået 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 underdatabehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige og databehandleren i dennes forpligtelse til at anmelde brud på persondatasikkerheden til Datatilsynet.

11. Sletning og tilbagelevering af oplysninger

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

12. Revision, herunder inspektion

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

2. Procedurerne for revisioner, herunder inspektioner, med underdatabehandleren og underdatabehandlere i yderligere led er nærmeret angivet i Bilag C.7. og C.8.

3. Underdatabehandleren er forpligtet til at give Datatilsynet eller tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges, databehandlerens eller underdatabehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til nævnte fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

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

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

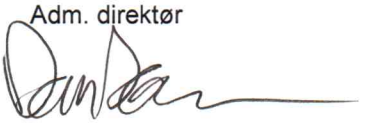
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til databehandleren i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

På vegne af databehandleren

Navn	Dan Thordahl Jørgensen
Stilling	Adm. direktør
Underskrift	



På vegne af underdatabehandleren

Navn	Mark Ringe Ibsen
Stilling	CFO
Underskrift	

15. Kontaktpersoner hos databehandleren og underdatabehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Kontaktperson hos databehandleren

Navn	Maria Høj Radmer
Stilling	Produktchef
E-mail	mhr@ims.dk
Telefonnummer	+45 24 49 99 72

Navn	Søren Skou Jessen
Stilling	Legal Counsel
E-mail	dataprivacy@firstagenda.com
Telefonnummer	+45 29 36 51 64

Kontaktperson hos underdatabehandleren

Navn	Mark Ringe Ibsen
Stilling	CFO
E-mail	mrib@cloudfactory.dk
Telefonnummer	+45 40209189

Bilag A Oplysninger om behandlingen

A.1. Formålet med underdatabehandlerens behandling af personoplysninger på vegne af databehandleren

Formålet med behandlingen er at stille virtuel datacenter kapacitet til rådighed for Databehandleren. Virtuel datacenter kapacitet består af vCPU, RAM og DISK også kaldet Infrastruktur as a Service (IaaS) som Databehandleren kan samle til Virtuelle servere, der kan anvendes i forbindelse Databehandlerens leverance og drift af IT-løsninger til dennes kunder.

Underdatabehandleren stiller derudover Cloud Factory Partner Portal, som er en Web portal, der stilles til rådighed for Databehandleren og muliggør selvbetjening ifm. provisionering af Infrastruktur as a Service produkter.

A.2. Underdatabehandlerens behandling af personoplysninger på vegne af databehandleren drejer sig primært om (karakteren af behandlingen)

Underdatabehandleren behandler personoplysninger i forbindelse med:

- Opbevaring af data i Datacenter
- Servicemeddelelser og nyhedsbreve til databehandlerens ansatte vedr. driftstatus af diverse systemer.

Underdatabehandleren behandler ikke data direkte i forbindelse med den Infrastruktur as a Service, som stilles til rådighed for Databehandleren. Underdatabehandleren stiller fysisk sikkerhed, Hardware og netværk til rådighed og sikrer at dette er forsvarligt vedligeholdt i aftaleperioden.

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

Al data overladt til databehandleren på vegne af den dataansvarlige. Dermed kan alle kategorier af personoplysninger potentielt blive behandlet af underdatabehandleren.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Den dataansvarliges brugere, kunder og/eller medarbejdere

A.5. Underdatabehandlerens behandling af personoplysninger på vegne af databehandleren kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer indtil aftalen mellem parterne om levering af underdatabehandlerens digitale løsning til databehandleren opsiges eller ophæves af parterne.

Bilag B Betingelser for underdatabehandlerens brug af underdatabehandlere i yderligere led og liste over godkendte underdatabehandlere i yderligere led

B.1. Godkendte underdatabehandlere i yderligere led

Ved Bestemmelsernes ikrafttræden har databehandleren godkendt brugen af følgende underdatabehandlere i yderligere led:

Underdatabehandleren benytter ikke underdatabehandlere i yderligere led i forbindelse med behandlingsaktiviteten.

Ved Bestemmelsernes ikrafttræden har databehandleren godkendt brugen af ovennævnte underdatabehandlere i yderligere led for den beskrevne behandlingsaktivitet. Underdatabehandleren må ikke – uden databehandlerens skriftlige godkendelse – gøre brug af en underdatabehandler i yderligere led til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler i yderligere led til denne behandlingsaktivitet.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Underdatabehandlerens behandling af personoplysninger på vegne af databehandleren sker ved, at underdatabehandleren udfører følgende:

Drifter og vedligeholder en teknisk platform, herunder fysiske server, lagringskapacitet, netværk osv., der muliggør oprettelse af de virtuelle servere, som databehandler stiller til rådighed for sine services og/eller dataansvarlige.

C.2. Behandlingssikkerhed

Underdatabehandleren har ikke adgang til opbevarede persondata for databehandleren. Databehandleren kan dog i enkelte tilfælde, midlertidigt give underdatabehandleren adgang til de Hostede virtuelle servere, i forbindelse med support, hvorfor det er vurderet, at der som minimum etableres et sikkerhedsniveau jf. dette Bilag C.

Underdatabehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne.
Underdatabehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

ORGANISERING AF INFORMATIONSSIKKERHEDEN

- Underdatabehandleren skal træffe de fornødne tekniske og organisatoriske foranstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen.
- Underdatabehandleren skal nærmere præcist træffe de tekniske og organisatoriske foranstaltninger, som fremgår af nærværende Bilag C.

INTERNE SIKKERHEDSRETNINGSLINJER

- Underdatabehandleren skal fastsætte og gennemføre interne risikobaserede retningslinjer for sikker behandling af personoplysninger i overensstemmelse med den til enhver tid gældende lovgivning om behandling af personoplysninger.
- Underdatabehandleren skal endvidere implementere en databeskyttelsespolitik i overensstemmelse med databeskyttelsesforordningens artikel 24(2).
- Underdatabehandlerens relevante interne retningslinjer skal gennemgås mindst én gang om året med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold.

MEDARBEJDERSIKKERHED

- Alle personoplysninger skal behandles fortroligt. I overensstemmelse med Aftalens afsnit 5 har medarbejdere hos underdatabehandleren tavshedspligt om alle de personoplysninger, som de får adgang til i forbindelse med databehandlingen.
- Databehandleren kan til enhver tid forlange en udtrykkelig liste over de af underdatabehandlerens medarbejdere, som er godkendt og autoriseret til at tilgå eller modtage databehandlerens informationer.
-

FYSISK SIKKERHED

- Der skal træffes sikkerhedsforanstaltninger til hindring af uvedkommendes adgang til personoplysninger, som underdatabehandleren behandler i medfør af nærværende Aftale.

IT-SIKKERHED

- Underdatabehandlerens udstyr, der benyttes ved behandling af personoplysninger, skal være omfattet af dokumenterede processer for opdatering og sårbarhedsstyring.

- Underdatabehandlerens udstyr, der benyttes ved behandling af personoplysninger, skal være omfattet af dokumenterede processer for malwarebeskyttelse og opdatering af dette.
- Såfremt Underdatabehandlerens ansatte anvender hjemmearbejdsplads til behandling af personoplysninger, skal Leverandøren indestå for, at de interne sikkerhedsforanstaltninger overholdes inden for rammerne af Datatilsynets retningslinjer om anvendelse af hjemmearbejdspladser.

SIKRING AF UDSTYR

- I forbindelse med reparation, service eller destruktion af udstyr og medier, som indeholder personoplysninger omfattet af nærværende Aftale, skal det sikres, at uvedkommende ikke får adgang til personoplysningerne.

TRANSMISSION AF OPLYSNINGER OVER INTERNETTET

- Ved tilslutning til internet eller andre åbne net skal der træffes foranstaltninger, som sikrer imod, at uvedkommende får adgang til underdatabehandlerens interne net.
- Ved transmission af personoplysninger over det åbne internet (f.eks. e-mail) skal underdatabehandleren efterleve følgende minimumskrav:
    - Transmission af fortrolige personoplysninger samt følsomme personoplysninger efter databeskyttelsesforordningens artikel 9 og 10 skal ske ved forsvarlig kryptering baseret på en anerkendt algoritme (AES eller tilsvarende).

SLETNING AF PERSONOPLYSNINGER

- Papirdokumentation skal makuleres, når der ikke længere er behov for at opbevare personoplysningerne. Personoplysninger, der opbevares digitalt, skal slettes på en anerkendt måde, når der ligeledes ikke er behov for opbevaring af oplysningerne.

LOGNING

- Alle transaktioner med følsomme personoplysninger efter databeskyttelsesforordningens artikel 9 og 10, skal logges, og loggen skal indeholde oplysninger om,
    - Tidspunkt,
    - Bruger,
    - Type af anvendelse,
    - Angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.
- Loggen skal opbevares i seks måneder, hvorefter den skal slettes.
- Underdatabehandleren er ligeledes forpligtet til at udlevere udskrifter/give databehandleren adgang til logs, efter anmodning fra den øverste sikkerhedsansvarlige hos databehandleren.

ADGANGSSTYRING

- Kun de personer hos underdatabehandleren, som er autoriseret hertil, må have adgang til personoplysningerne. Der må ikke gives adgangsrettigheder til personoplysningerne i videre omfang, end de pågældende har behov for i forhold til deres jobfunktion.
- Brugeradgange til følsomme personoplysninger skal revurderes årligt.
- Medarbejderens adgangskoder skal være tilstrækkeligt komplekse.
- Underdatabehandleren skal sikre, at der er en passwordpolitik, samt at denne er systemunderstøttet ved autorisation på systemer, der giver adgang til personoplysninger.
- Der skal føres kontrol med afviste adgangsforsøg, og der skal blokeres for yderligere forsøg efter flere på hinanden følgende adgangsforsøg inden for den fastsatte, almindelige arbejdsdag.
- Underdatabehandleren må ikke anvende software, programmel og hardwarekonfigurationer med kendte svagheder og sårbarheder, som kan udnyttes til at få adgang til personoplysningerne.

C.3 Bistand til den dataansvarlige og databehandleren

Underdatabehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige og databehandleren i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

I forbindelse med at iagttage de registreredes rettigheder, jf. pkt. 9.1. bistår underdatabehandleren databehandler med:

- at give indsigt i, slette, begrænse og berigtige oplysninger samt sørge for at dette også sker hos underdatabehandlere i yderligere led, såfremt det er muligt
- at opfylde de registreredes rettigheder uden unødig forsinkelse
- alle henvendelser fra evt. registrerede henvises til databehandler

I forbindelse med brud og hændelser, jf. pkt. 9.2. sendes følgende informationer, såfremt det er muligt, til databehandler:

- Fakta om det konstaterede brud (tid, sted, årsag)
- Hvornår bruddet startede, hvornår det blev opdaget og hvornår bruddet er standset
- Karakteren af bruddet på persondatasikkerheden, herunder om der er sket brud på fortrolighed, integritet og tilgængelighed
- Kategorierne og det omtrentlige antal berørte registrerede hvis dette er muligt
- Kategorierne af personoplysninger hvis dette er muligt
- Navn og kontaktoplysninger til kontaktpunkt hvor yderligere oplysninger kan indhentes
- Beskrivelse af de sandsynlige konsekvenser af bruddet
- Beskrivelse af foranstaltninger der er truffet eller foreslået truffet som led i håndteringen af bruddet og dets mulige skadevirkninger

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i perioden for parternes aftale om underdatabehandlerens levering af underdatabehandlerens værktøjer og services til databehandleren, eller i henhold til særskilt skriftlig aftale, hvorefter de slettes hos underdatabehandleren. Ved sletning eller tilbagelevering af Infrastruktur as a Service opbevares data i henhold til underdatabehandlerens Disaster Recovery retention, som er 30 dage, hvorefter data automatisk slettes.

Ved ophør skal underdatabehandleren således enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre databehandleren – efter underskriften af disse Bestemmelser – har ændret databehandlerens 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 databehandlerens forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- **Danmark**

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis databehandleren ikke i disse Bestemmelser eller efterfølgende giver dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er underdatabehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler,

medmindre en sådan overførsel sker til en af de autoriseret underdatabehandlere i yderligere led nævnt i bilag B. Overførselsgrundlag anvendes i henhold til Databeskyttelsesforordningens Kapitel V om overførsler af personoplysninger til tredjelande eller internationale organisationer. De specifikke overførselsgrundlag følger af gældende bilag B.

C.7 Procedurer for databehandlerens revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandleren

Underdatabehandleren skal én gang årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart angående underdatabehandlerens overholdelse af denne databehandleraftale med tilhørende bilag.

Der er mellem parterne enighed om, at der kan anvendes følgende typer af revisionserklæringer:

- ISAE 3402 type 2
- ISAE 3000

Revisionserklæringen sendes snarest muligt efter indhentelsen, dog senest 12 måneder efter aftalens indgåelse, til databehandleren til orientering.
En repræsentant for databehandleren har herudover adgang til at føre tilsyn, herunder fysisk tilsyn, hos underdatabehandleren, når der efter databehandlerens vurdering opstår et behov herfor.
Databehandlerens eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af databehandleren selv. Underdatabehandleren er dog forpligtet til at afsætte de ressourcer (hovedsagligt den tid), der er nødvendig for, at databehandleren kan gennemføre sit tilsyn. Underdatabehandleren er i dette tilfælde berettiget til at modtage særskilt vederlag herfor efter princippet om dokumenteret medgået tid.

Bilag D Parternes regulering af andre forhold

D.1. Misligholdelse og tvistigheder

Misligholdelse og tvistigheder er reguleret i Hovedaftalen. I tilfælde af, at Hovedaftalen ikke tager stilling hertil, skal gældende rets almindelige misligholdelsesbeføjelser finde anvendelse på Bestemmelserne i denne aftale.

Regulering af tvistløsning, inklusive lovvalg og værneting i Hovedaftalen finder også anvendelse for Bestemmelserne, som om Bestemmelserne var en integreret del heraf. I tilfælde af at Hovedaftalen ikke tager stilling hertil skal nedenstående bestemmelser finde anvendelse på Bestemmelserne. Værneting er Retten i Aarhus.

Aftalen er underlagt dansk ret med undtagelse af:

a) Regler der fører til anvendelse af anden lov end dansk lov samt
b) FN-Konventionen om internationale løsørekøb (CISG)

Opstår der uoverensstemmelser i forbindelse med Bestemmelserne eller deres gennemførelse, skal parterne med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med en mediator med henblik på at løse tvisten. Om nødvendigt skal forhandlingerne søges løftet op på direktionsniveau i parternes organisationer.

Kan parterne ikke opnå en løsning ved forhandling, er parterne berettiget til at kræve tvisten afgjort endeligt ved retssag ved de almindelige domstole. Retten i Esbjerg er valgt som værneting. Retsplejelovens henvisningsregler til Landsret og Sø- og Handelsret skal dog fortsat finde anvendelse.

Såfremt databehandleren ikke mener, at en af underdatabehandleren udpeget Underdatabehandler i yderligere led lever op til et eller flere af de ovennævnte krav under punkt (7), vil det blive betragtet som væsentlig misligholdelse. Inden væsentlig misligholdelse gøres gældende skal den databehandleren underrette underdatabehandleren om forholdet og give en passende frist til at udbedre misligholdelsen.

Som udgangspunkt betragtes det som væsentlig misligholdelse, såfremt underdatabehandleren ikke overholder forpligtelserne i denne Databehandleraftale, den til enhver tid gældende lovgivning vedrørende databeskyttelse samt kravene i de dokumenter, der udgør bilag til Databehandleraftalen.

D.2. Erstatning og forsikring

Erstatnings- og forsikringsspørgsmål er reguleret i Hovedaftalen. I tilfælde, at Hovedaftalen ikke tager stilling hertil, er underdatabehandleren erstatningsansvarlig i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af Bestemmelserne. Såfremt databehandleren af tredjemand gøres erstatningsansvarlig for underdatabehandlerens og/eller eventuelle underdatabehandlere i yderligere leds manglende overholdelse af Bestemmelserne, herunder bilagene, og/eller overtrædelse af gældende lovgivning vedrørende databeskyttelse, skal underdatabehandleren holde databehandleren skadesløs for alle omkostninger, gebyrer, erstatningsbeløb, udgifter eller tab, som databehandleren har afholdt eller pådraget sig som følge heraf.