plandisc

Databehandleraftale

Databehandleraftale

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

mellem

CVR

herefter "den dataansvarlige"

og

Visma Plandisc A/S
CVR: 37204854
Axel Kiers Vej 5A 8270 Højbjerg
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 licens til databehandlerens løsning(er) og service(s) 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 fem 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. Bilag E indeholder en beskrivelse af databehandlerkæden.

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

12. 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 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.

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

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:

1. pseudonymisering og kryptering af personoplysninger.

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

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

4. 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 generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 10 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller

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

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

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter 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. 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 24 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. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

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

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

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 databehandlerens tjenester vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre den dataansvarlige instruerer databehandleren om andet, eller 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 nærmere 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 skriftligt varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

   Navn
   Stilling
   Underskrift

   På vegne af databehandleren

   Navn
   Stilling
   Underskrift

14. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Databehandleren kan kontaktes via nedenstående kontaktperson eller ved kommunikation til personer, der normalvis kommunikeres med i aftaleforholdet mellem den dataansvarlige og databehandleren.

2. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

3. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner. Såfremt det ikke er muligt for databehandleren at træffe den dataansvarlige ved oplyste kontaktperson, tillader den dataansvarlige at databehandleren kontakter anden person, der normalvis kommunikeres med i aftaleforholdet.

   På vegne af den dataansvarlige

   Navn
   Stilling
   E-mail

   På vegne af databehandleren

Navn	Privacy Team
Stilling	Privacy Team
E-mail	privacy.plandisc@visma.com

Bilag A Oplysninger om behandlingen

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

Behandlingen af den dataansvarliges personoplysninger sker med det formål at opfylde den mellem databehandleren og den dataansvarlige indgåede aftale om databehandlerens levering af databehandlerens digitale løsning, som er en virtuel kalenderløsning.

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

Som ejer og leverandør af løsningen behandler databehandleren ved generel drift, herunder hosting, visning, organisering, modtagelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, logning, support, fejlfinding og andre it-ydelser forbundet med databehandlerens løsning(er) og/eller service(s) til den dataansvarlige i henhold til den mellem parterne indgåede aftale.

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

Databehandleren behandler i udgangspunktet nedenstående kategorier af personoplysninger. Ved brug af løsningen er der dog mulighed for, at den dataansvarlige kan overlade behandling af alt slags data og personoplysninger til databehandleren, hvorfor databehandleren potentielt vil kunne behandle alle kategorier af personoplysninger.

- **Almindelige personoplysninger** (jf. Databeskyttelsesforordningens artikel 4, stk. 1 og artikel 6): Almindelige personoplysninger såsom navn, telefonnummer, e-mail, IP adresse

A.4. Behandlingen omfatter følgende kategorier af registrerede

Databehandleren behandler i udgangspunktet nedenstående kategorier af registrerede. Ved brug af løsningen er der dog mulighed for, at den dataansvarlige kan overlade behandling af alt slags data og personoplysninger til databehandleren, hvorfor databehandleren potentielt vil kunne behandle personoplysninger om flere kategorier af registrerede.

Kategorier af registrerede:

- Kundens slutbrugere

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 kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne ophører.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR/ VIRKSOMHEDS ID	ADRESSE OG LAND / LOKALITET FOR BEHANDLING	BESKRIVELSE AF BEHANDLING	EVENTUELT OVERFØRSELSGRUNDLAG
Amazon AWS	LU26888617	38 avenue John F. Kennedy, L-1855 Luxembourg	Amazon Web Services (AWS) lagrer kundedata sikkert via S3 Cloud Storage. Denne databehandling sker i henhold til deres standardaftale for underdatabehandlere.	AWS er certificeret under EU-U.S. Data Privacy Framework, som udgør overførselsgrundlaget for eventuelle overførsler af personoplysninger til tredjelande uden for EU/EØS
Microsoft Azure	VAT: IE8256796U	South County Business Park, Leopardstown, Dublin 18, Ireland	Microsoft Azure anvendes som hosting- og infrastrukturplatform for løsningen. Databehandlingen omfatter lagring, behandling og drift af kundedata i Microsofts svenske datacentre i overensstemmelse med Microsofts databehandleraftale.	N/A
WebHosting A/S	25674138	Naverland 2, 2600 Glostrup, Danmark	WebHosting A/S sender og modtager e-mails fra vores løsninger via SMTP-tjeneste. Databehandlingen sker i henhold til deres standardaftale for underdatabehandlere.	N/A
Ipregistry	VAT: FR13983391012	1 Chemin des Rosiers, 06800 Cagnes-sur-Mer, Frankrig	Ipregistry bruges til at slå brugernes geografiske placeringer op (IP-geolokationstjeneste). Vi bruger primært denne funktion til at blokere adgang til vores tjeneste fra sanktionerede lande, der er underlagt internationale embargoer. Denne brug sker i henhold til deres standardaftale for underdatabehandlere.	N/A
Orca Security Ltd.	13410414	Frankfurt, Germany	Orca Security Ltd. bruges til at sikre vores cloud-infrastruktur ved at analysere netværk, tjeneste- og lagerkonfigurationer, malwarescanning samt opdatering af operativsystemer, der anvendes af virtuelle maskiner, rettigheder og opsætning af multifaktor-godkendelse (MFA) for brugere med adgang til infrastrukturen osv. Databehandlingen udføres i henhold til Vismas underdatabehandleraftale med Orca Security, hvilket bl.a. sikrer, at alle data behandles inden for EU/EØS.	N/A

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.

Databehandleren skal opretholde en gældende liste over underdatabehandlere på databehandlerens hjemmeside, som udgør gældende bilag B. Underdatabehandleraftalerne rekvireres via hjemmesiden eller ved skriftlig anmodning til databehandleren.

B.2. Varsel for indsigelse ved skift af underdatabehandlere

Databehandlerens underretning om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere skal være offentligt tilgængelig på databehandlers hjemmeside senest 10 dage, før anvendelsen eller ændringen skal træde i kraft, så vidt dette umiddelbart er muligt jf. kontraktsbestemmelse stk. 7, 7.3.

Uanset ovenstående accepterer den dataansvarlige, at der kan være særlige tilfælde, hvor der kan opstå et konkret behov for, at ændringen vedrørende tilføjelse eller erstatning af underdatabehandlere sker med kortere varsel eller straks. I sådanne tilfælde vil databehandleren underrette den dataansvarlige om ændringen snarest muligt.

Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give databehandleren meddelelse herom inden ændringens varslede virkningstidspunkt. Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

Ved den dataansvarliges indsigelse accepterer den dataansvarlige samtidig, at databehandleren kan være forhindret i at levere hele eller dele af de aftalte tjenester. Sådan manglende opfyldelse kan ikke tilskrives databehandlerens misligholdelse. Databehandleren opretholder sit krav på betaling for sådanne ydelser, uanset de ikke kan leveres til den dataansvarlige.

.

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:

drift, herunder hosting, visning, organisering, modtagelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, logning, support, fejlfinding og andre it-ydelser forbundet med databehandlerens levering af den digitale løsning til den dataansvarlige i henhold til aftalen indgået mellem parterne om levering af databehandlerens digitale løsning.

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle: Behandlingens omfang og karakter som angivet under bilag A, A.1 og A.2, herunder nærmere angivet instruks under bilag C, C.1.

Sikkerhedsniveau:
På baggrund af de ovenfor angivne oplysninger om behandlingen, og under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål, samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder etableres følgende sikkerhedsniveau:

Aftalt sikkerhedsniveau
Højt

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 understøtte den Dataansvarlige i dennes arbejde med at dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau og gennemføre de foranstaltninger, der er nødvendige for at imødegå identificerede risici.
På baggrund af det etablerede sikkerhedsniveau implementeres procedurer for revisioner i overensstemmelse med punkt C.7 og C.8.

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:

C.2.1 Krav til pseudonymisering og kryptering af personoplysninger

Krav til pseudonymisering af personoplysninger
Databehandler foretager pseudonymisering af personoplysninger, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder

tilsiger det

Krav til kryptering af personoplysninger

Databehandler foretager kryptering af personoplysninger, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det.

Databehandleren sikrer, at denne kryptering der anvendes, er korrekt sat op og tilstrækkelig til sikring af de behandlede personoplysningers fortrolighed og integritet.

Efter instruks anvendes der altid kryptering af personoplysninger ved enhver transmission af fortrolige og følsomme personoplysninger via eksterne kommunikationsforbindelser.

C.2.2 Krav vedrørende evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

1. Databehandler foretager mindst én gang årligt en risikovurdering for hver af de behandlingssystemer og tjenester, hvori den Dataansvarliges personoplysninger behandles. Databehandler foretager loyalt og professionelt mitigerende foranstaltninger baseret på risikovurderingens resultater.
2. Databehandler foretager løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet.
3. Samme krav gælder for den dataansvarlige når de mitigerende foranstaltninger alene kan foretages af den dataansvarlige selv ved dennes brug af løsningen.

Databehandler sikrer endvidere, at:

1. Adgang til de personoplysninger, som aftalen vedrører, er begrænset til personer, der har et sagligt formål.
2. Der er tekniske og/eller organisatoriske foranstaltninger, som sikrer, at alene disse autoriserede personer, har adgang. Autorisationen omfatter også personer, som udfører konsulentopgaver eller nødvendige revisions- drifts- og systemtekniske opgaver.
3. Der skal løbende foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have.
4. Ansatte og eventuelle samarbejdspartnere skal til stadighed være bekendt med og have tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.
5. Den dataansvarlige er underlagt samme krav ift. sin egen organisation.

C.2.3 Krav vedrørende evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

Databehandler sikrer, at

1. Databehandleren skal have opdaterede og effektive beredskabsplaner og -procedurer, der sikrer genetablering af personoplysninger og adgange inden for rimelig tid i tilfælde af driftsafbrydelser.
2. Databehandleren skal sikre, at der foretages regelmæssig backup af personoplysninger, der er omfattet af aftalen.
3. Databehandleren skal regelmæssigt afprøve og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser.

C.2.4 Krav vedrørende procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden

Der skal foreligge procedurer, som sikrer, at der sker regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Databehandler har til enhver tid tidssvarende procedurer for gennemførelse af:

- Regelmæssig kontrol, vurdering, tilpasning og forbedring af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren er underlagt efter den til enhver tid gældende lovgivning, retspraksis, Datatilsynets afgørelser, anbefalinger og retningslinjer samt vilkårene i nærværende databehandleraftale.
- Kontrol af, at sikkerhedsforanstaltningerne faktisk efterleves i forhold til den til enhver tid værende risiko for de registreredes rettigheder og frihedsrettigheder.
- Kontrol af brugeradgang for medarbejdere eller andre autoriserede.
- Kontrol af at backuppen er læsbar, skrivebeskyttet, har det rette omfang og kan reetableres.
- Kontrol af at der sker korrekt kryptering, herunder at krypteringsnøglen opbevares sikkert.
- Kontrol med at sikkerhedsloggene er tilstrækkelige og relevante.
- Kontrol med at det fysiske sikkerhedsniveau er afstemt med det til enhver tid værende trusselsbillede.
- Databehandleren har formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.
- For kritiske sikkerhedsopdateringer skal Databehandleren have procedurer, der sikrer, at disse kan gennemføres uden unødig forsinkelse.
- At der føres ekstraordinære kontroller ved større ændringer af systemteknisk set-up og efter brud på persondatabeskyttelsen.

C.2.5 Krav vedrørende adgang til personoplysninger via internettet

Når der tilgås systemer indeholdende personoplysninger over internettet skal autentifikationen af brugeren ske ved flerfaktorautentificering. Der må kun oprettes forbindelse til disse personoplysninger omfattet af disse bestemmelser igennem sikre krypterede forbindelser.

C.2.6 Krav vedrørende beskyttelse af personoplysninger under transmission

Der skal anvendes tilstrækkelige sikkerhedsforanstaltninger i forbindelse med transmission af personoplysninger. Sikkerhedsforanstaltningerne skal leve op til de til enhver tid anerkendte og gældende branchestandarder for behandling af personoplysninger.

Databehandler sikrer i denne forbindelse, at personoplysninger er krypteret i forbindelse med transmissionen. Krypteringen skal løbende holdes opdateret, og følge den til enhver tid anerkendte og gældende branchestandard.

C.2.7 Krav vedrørende beskyttelse af personoplysninger under opbevaring

Under opbevaring af personoplysninger skal der etableres tilstrækkelige sikkerhedsforanstaltninger under hensyntagen til karakteren af de behandlede personoplysninger, og risikoen for de registreredes rettigheder. Databehandler sikrer, at personoplysninger er krypteret under opbevaring, og at adgang til disse kun kan ske af autoriserede personer via kontrollerede adgangsprocedurer.

C.2.8 Krav vedrørende fysisk sikring af lokaliteter, hvor der behandles personoplysninger

Databehandler sikrer, at der er passende sikkerhedsforanstaltninger mod enhver uautoriseret adgang til lokationer, hvor den Dataansvarliges data behandles.

Sikkerhedsforanstaltninger skal være afstemt med det aktuelle trusselsbillede samt den følsomhed og mængde af personoplysninger, som Databehandler behandler for den Dataansvarlige.

Behandlingen foregår fra lokationer, som er beskyttet mod skader forårsaget af fysiske forhold, herunder, men ikke begrænset til, brand, overophedning, vandskade, magnetisme, forsyningssvigt, tyveri og hærværk.

Databehandleren skal sikre, at alt anvendt udstyr, der anvendes i forbindelse med behandlingen af personoplysninger, er underlagt passende tekniske foranstaltninger.

C.2.9 Krav vedrørende anvendelse af hjemme-/fjernarbejdspladser

Hjemme-/fjernarbejdspladser skal være sikret med tekniske kontroller, der sikrer, at behandlingen af personoplysninger sker i overensstemmelse med gældende lovgivning og den indgåede aftale.

Det skal sikres, at uvedkommende ikke får adgang til personoplysninger, der behandles ved hjemmearbejdspladser, ligesom de enkelte medarbejdere skal instrueres i, hvordan uvedkommende ikke får adgang.

Databehandler sikrer, at der anvendes kryptering af kommunikationsforbindelser. Fjernadgange skal være sikret af en VPN-løsning eller anden sikkerhedsteknologi, så det kun er autoriserede personer, som kan få adgang til personoplysninger.

Autentifikation af personer som får adgang til personoplysninger skal være baseret på multifaktorautentifikation eller tilsvarende sikkerhedsforanstaltninger.

C.2.10 Krav vedrørende logning

Databehandleren skal føre log over brugernes adgang og anvendelse af Løsningen i det omfang, det er nødvendigt for at kunne dokumentere databehandlingen og efterleve gældende databeskyttelseslovgivning. Loggen skal som minimum indeholde relevante oplysninger til identifikation af anvendelsens karakter og formål.

Der skal foretages maskinel registrering (logning) ved al behandling af personoplysninger.

Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvender søgekriterium.

Logoplysninger opbevares i en periode, der står i rimeligt forhold til formålet med logningen og slettes herefter, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode af hensyn til at kunne anvende den som værktøj til brug ved efterforskning. På tidspunktet for aftalens indgåelse er den fastsatte opbevaringsperiode 12 måneder, men perioden kan justeres af databehandleren i overensstemmelse med gældende sikkerheds- og driftsmæssige krav.

Databehandleren skal løbende kontrollere, at loggen indeholder de nødvendige oplysninger, som fremgår af disse bestemmelser. Ved mistanke om misbrug eller brud på persondatasikkerheden skal Databehandleren uden vederlag udlevere relevante logoplysninger, herunder tidspunkt, bruger, type af adgang eller ændring samt den anvendte funktionalitet og sikre, at loggen præsenteres i en forståelig og brugbar form.

C.3 Bistand til den dataansvarlige

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

<u>Underretning af den dataansvarlige om anmodninger fra de registrerede</u>
Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes underdatabehandlere fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret.

Databehandleren skal på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

Bistand ved sikkerhedsbrud, herunder underretning af den dataansvarlige om sikkerhedsbrud
Databehandlerens bistand i forbindelse med den dataansvarliges forpligtelser efter databeskyttelsesforordningens artikel 33 og 34 sker ved, at databehandleren indgiver de oplysninger, der følger af Bestemmelse 10.3, til den dataansvarlige inden for den frist, der følger af Bestemmelse 10.2. Databehandleren skal efterfølgende bistå den dataansvarlige ved på den dataansvarliges anmodning at stille de oplysninger til rådighed, som er nødvendige for, at den dataansvarlige kan foretage anmeldelse af brud på persondatasikkerheden til den kompetente tilsynsmyndighed eller som er nødvendige for, at den dataansvarlige kan underrette den registrerede herom.

Bistand i forbindelse med risikovurderinger og konsekvensanalyser
Databehandleren skal bistå den dataansvarlige ved at stille de nødvendige oplysninger til rådighed, så den dataansvarlige kan gennemføre de nødvendige risikovurderinger. Såfremt den dataansvarlige vurderer, at behandlingen sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder, skal databehandleren på anmodning fra den dataansvarlige bistå den dataansvarlige i forbindelse med dennes forpligtelser efter databeskyttelsesforordningens artikel 35 og 36 ved at indgive de oplysninger til den dataansvarlige, der er nødvendige for, at den dataansvarlige kan foretage en konsekvensanalyse i overensstemmelse med artikel 35 og foretage en forudgående høring af den kompetente tilsynsmyndighed i overensstemmelse med artikel 36.

Sikring af tekniske og organisatoriske foranstaltninger
Databehandleren skal endelig sikre, at dennes tekniske og organisatoriske foranstaltninger gør det muligt for den dataansvarlige at overholde sine forpligtelser efter databeskyttelsesforordningens artikel 33-36, herunder f.eks. gennem de foranstaltninger vedrørende styring af sikkerhedsbrud, styring af aktiver, logning mv., der følger af bilag C.

C.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

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

Det er aftalt, at der skal ske sletning af personoplysninger, som den dataansvarlige har foretaget en egenvurdering til sletning (uanset tidsramme), samt at databehandleren understøtter den dataansvarliges sletning af disse personoplysninger. Udover ovenstående skal databehandler kunne foretage sletning af personoplysninger efter konkret anmodning fra den dataansvarlige.

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 de, som følger af nærværende databehandleraftale og de adresser som fremgår af anvendte underdatabehandlere, samt underdatabehandlere i yderligere led, som nærmere beskrevet i gældende bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler, medmindre en sådan overførsel sker til en af de autoriseret underdatabehandlere 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.

Vilkår vedrørende myndighedsanmodninger om udlevering af personoplysninger

Databehandleren skal underrette den Dataansvarlige om enhver henvendelse, som Databehandleren eller dennes underdatabehandlere modtager fra en myndighed i et tredjeland om videregivelse af personoplysninger omfattet af disse Bestemmelser.

Såfremt Databehandleren, direkte eller indirekte, modtager en anmodning om at udlevere oplysninger omfattet af disse Bestemmelser, herunder personoplysninger, til en modtager, der geografisk er placeret uden for EU/EØS, er Databehandleren til enhver tid forpligtet til at modsætte sig en sådan anmodning om udlevering, så vidt det er muligt for Databehandleren i henhold til EU-ret eller medlemsstaternes nationale ret.

Databehandleren skal, eventuelt i fællesskab med den pågældende underdatabehandler, udtømme enhver mulighed for at påklage anmodninger om videregivelse af personoplysninger omfattet af disse Bestemmelser, hvis der er tale om generelle anmodninger eller anmodninger, der ikke er i overensstemmelse med EU-retten, herunder databeskyttelsesforordningen, samt øvrig national lovgivning, som supplerer databeskyttelsesforordningen. Databehandleren skal, i det omfang det er muligt, give den Dataansvarlige mulighed for at indtræde i klage- og retssager, med henblik på at give den Dataansvarlige mulighed for at varetage sine egne interesser.

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

Databehandleren skal én gang årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisionserklæringen skal være af typen ISAE 3000 revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser, med høj grad af sikkerhed og udarbejdet efter opbygningen i FSR-standarden, dækkende kravene beskrevet i denne databehandleraftale

Den dataansvarlige kan fravige den aftalte tilsynsform, såfremt den dataansvarlige vurderer, at databehandleren på anden vis vil kunne dokumentere overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag. Databehandleren er berettiget til særskilt vederlag herfor, såfremt Databehandleren anmodes om en anden tilsynsform end aftalt ovenfor.

Revisionserklæringen og/eller inspektionsrapport fremsendes uden unødig forsinkelse til den dataansvarlige til orientering, såfremt denne eller disse ikke allerede er tilgængelig på databehandlerens hjemmeside. den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen/inspektionsrapporten og kan i sådanne tilfælde anmode om en ny revisionserklæring/

inspektionsrapport under andre rammer og/eller under anvendelse af anden metode mod betaling.

Baseret på resultaterne af tilsynet 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 bemyndiget af den dataansvarlige, har endvidere ret til at foretage inspektioner af databehandlerens egne fysiske faciliteter, hvor der behandles personoplysninger, samt modtage de nødvendige informationer til gennemførelse af tilsyn med den databehandlerens efterlevelse af kravene i disse Bestemmelser samt gældende databeskyttelsesret.Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til den kompetente tilsynsmyndighed efter anmodning herom fra myndigheden.

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

Databehandleren træffer som udgangspunkt valg om, hvordan revision af underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og underdatabehandleraftalen foretages, herunder hvilken type af revisionserklæring og/eller inspektionsrapport, der indhentes. Typen og omfanget af revisionen skal afspejle karakteren af den behandling af personoplysninger, som underdatabehandleren foretager.

Resultaterne af revisionserklæringer og/eller inspektionsrapporter fremgår minimum 1 gang årligt via den tilsynsform som den dataansvarlige har tilvalgt under C.7. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode mod betaling.

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 mod betaling.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren finder det nødvendigt. Den dataansvarlige kan ligeledes anmode om sådanne inspektioner når denne finder det nødvendigt, dog mod vederlag til databehandleren.

Dokumentation for sådanne inspektioner fremgår af tilsynsformen som valgt under bilag C, C.7. 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 mod betaling.

Den dataansvarlige kan – hvis det findes nødvendigt – vælge med rimeligt varsel 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. Dette sker mod betaling til både databehandleren og den udvalgte

underdatabehandler.

Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Databehandlerens ansvar omfatter alene de databeskyttelsesretlige forpligtelser i relation til personoplysningerne. Databehandleren hæfter ikke for underdatabehandlerens øvrige forhold eller mangler i underleverancen, som ikke vedrører overholdelsen af databeskyttelseslovgivningen

Den dataansvarliges eventuelle udgifter i forbindelse med en inspektion afholdes af den dataansvarlige selv. Databehandleren er forpligtet til at afsætte den tid og de ressourcer, der med rimelighed er nødvendige for at muliggøre inspektionen. Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til Datatilsynet efter anmodning herom fra Datatilsynet.

Bilag D Parternes regulering af andre forhold

D.1 Ansvar og misligholdelse

Parternes aftale om erstatningsansvar og ansvarsbegrænsning fremgår af Aftalen indgået mellem databehandleren og den dataansvarlige om databehandlerens levering af digitale løsning til den dataansvarlige, så længe denne ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

D.2 Sletning og returnering af oplysninger

Det er mellem parterne aftalt, at den dataansvarlige instruerer om databehandlerens sletning og returnering af personoplysninger i forbindelse med Bestemmelsernes ophør.

Den dataansvarlige skal, senest 30 dage efter at behandlingen af personoplysninger er ophørt, meddele databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige. I det tilfælde hvor personoplysninger skal tilbageleveres til den dataansvarlige, skal databehandleren ligeledes slette eventuelle kopier. Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever meddelelsen fra den dataansvarlige.

Såfremt databehandleren ikke har modtaget meddelelse fra den dataansvarlige, inden 30 dage efter behandlingen af personoplysninger er ophørt, fremsender databehandleren en rykker til den dataansvarlige. Hvis den dataansvarlige herefter ikke meddeler databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige, er databehandleren uden yderligere varsel berettiget til at slette personoplysninger.

Databehandleren er berettiget til vederlag for dennes behandlingsaktiviteter frem til det tidspunkt, hvor den dataansvarlige meddeler databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige.

D.3 Krav om vederlag

Medmindre andet er udtrykkeligt aftalt i denne databehandleraftale, udfører Databehandleren sine forpligtelser uden særskilt vederlag. Såfremt den dataansvarliges anmodninger medfører et merarbejde, der overstiger et rimeligt tidsforbrug (5 timer), kan Databehandleren opkræve betaling for den medgåede tid efter nærmere aftale mellem Parterne.

Eksempelvis er den dataansvarlige uden unødig forsinkelse blevet underrettet af databehandleren om et brud på persondatasikkerheden i overensstemmelse med Bestemmelse 10, og skyldes bruddet alene den dataansvarliges forhold, er databehandleren berettiget til særskilt vederlag for tid brugt på underretningen.

Bilag E Databehandlerkæden

Databehandleren forpligter sig til at opretholde en opdateret og tilgængelig oversigt over samtlige underdatabehandlere Den dataansvarlige kan løbende orientere sig herom. Databehandleren forpligter sig desuden til at følge den kommende harmonisering af et fælles europæisk "standardiseret format" for angivelse af databehandlerkæder og vil implementere et sådant straks ved vedtagelse og offentliggørelse i EU-regi

Databehandler:	Visma Plandisc A/S	CVR. nr.:	37204854
Systemnavn:	**Plandisc**		

.