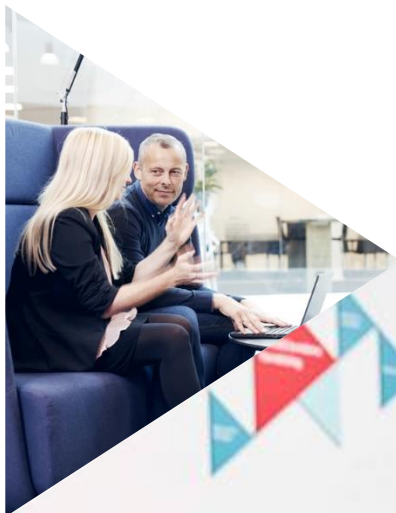


Bilag 6

Databehandleraftale

Visma IMS A/S



Indholdsfortegnelse

Databehandleraftalebestemmelser	3
1. Standardkontraktbestemmelser	3
2. Præambel	4
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	5
5. Fortrolighed	5
6. Behandlingssikkerhed	5
7. Anvendelse af underdatabehandlere	6
8. Overførsel til tredjelande eller internationale organisationer	7
9. Bistand til den dataansvarlige	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger	9
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren	10
Bilag A - Oplysninger om behandlingen	11
Bilag B - Underdatabehandlere	15
Bilag C - Instruks vedrørende behandling af personoplysninger	17
Bilag D - Parternes regulering af andre forhold	22

Denne databehandlersaftale er lavet på Datatilsynets standardkontraktbestemmelser. Parterne er bekendte med, at der er tale om et underdatabehandlerforhold.

Underdatabehandleraftalen er indgået mellem Visma IMS A/S (databehandler) og IT Relation A/S (underdatabehandler)

Parterne er bekendte med, at når der i underdatabehandleraftalen omtales "den dataansvarlige" skal det forstås som databehandler i forhold til kundernes egne personoplysninger, bortset fra i punkt 3, punkt 6.1-6.3, punkt 9.1-9.2 samt punkt 10.1, 10.2 anden linje samt punkt 10.3, hvor det fortsat skal forstås som "den dataansvarlige".

Parterne er bekendte med, at når der i aftalen omtales "databehandleren" skal det forstås som underdatabehandler, bortset fra i punkt 3, punkt 6.1-6.3, punkt 9.1-9.2 samt punkt 10.1, 10.2 anden linje samt punkt 10.3, hvor det fortsat skal forstås som "databehandleren".

Databehandleraftalebestemmelser

1. Standardkontraktbestemmelser

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

mellem

Visma IMS A/S

(herefter "den dataansvarlige")

og

IT Relation

(herefter "databehandleren"),

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

er der aftalt følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse Bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).
3. I forbindelse med leveringen af tjenester omfattet af parternes aftale om IT ydelser ("tjenesten" og/eller "tjenesterne") behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

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

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

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

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

- a. pseudonymisering og kryptering af personoplysninger.
 - b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.
 - c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.
 - d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder, som behandlingen udgør, og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren, som gør vedkommende i stand til at identificere og vurdere sådanne risici.

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

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

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dage 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 som fravigelse i bilag D.8. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser, som følger af disse Bestemmelser, er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
6. Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation.
 - b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland.
 - c. behandle personoplysningerne i et tredjeland.
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

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

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede.
- b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede.
- c. indsigtretten.
- 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 unødigt 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 det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
 - b. den dataansvarliges forpligtelse til uden unødigt 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.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3 skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger.
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden.
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, 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. 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. Procedurene 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.

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

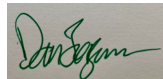
1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger 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 [Dan Thordahl Jørgensen]
Stilling [STILLING Adm. direktør]

Underskrift



På vegne af databehandleren

Navn Bo Duholm Hansen
Stilling Compliance Manager

Underskrift



15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

DEN DATAANSVARLIGE		DATABEHANDLEREN	
Navn:	[<u>Maria Høj Radmer</u>]	Navn:	Compliance and Security
Mail:	[E-mail ad mhr@ims.dk]	Mail:	gdpr@itrelation.dk
Tlf.:	[Telefon24 49 99 72]	Tlf.:	+45 70 26 29 88

Bilag A – Oplysninger om behandlingen

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

Parterne har aftalt, at databehandleren skal levere følgende ydelser:

VALGT (X)	FORMÅLET MED BEHANDLINGEN
<input checked="" type="checkbox"/>	Hosting og drift <ul style="list-style-type: none">• Angivet som Hosting, Operations, Network og Security i bilag "Services" i parternes aftale vedrørende levering af tjenesterne.
<input type="checkbox"/>	Service Desk
<input type="checkbox"/>	SEPO Secure Mail
<input type="checkbox"/>	GrantOnline
<input type="checkbox"/>	TK2 EPJ
<input type="checkbox"/>	Konsulentytelser

A.1.1 Hosting og drift

Såfremt Hosting og drift er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af hosting og drift af den dataansvarliges it-systemer herunder backup, overvågning, vedligehold og support som nærmere specificeret i aftalen vedrørende levering af tjenesterne indgået mellem parterne. Herunder også specifikke opgaver bestilt af den dataansvarlige.

A.1.2 Service Desk

Såfremt Service Desk er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af supportytelser til den dataansvarlige som nærmere specificeret i aftalen vedrørende levering af tjenester indgået mellem parterne. Herunder også specifikke opgaver bestilt af den dataansvarlige.

A.1.3 SEPO Secure Mail

Såfremt SEPO Secure Mail er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af sikker mailservices som nærmere specificeret i aftalen vedrørende levering af tjenester indgået mellem parterne.

A.1.4 GrantOnline

Såfremt GrantOnline er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er at opfylde parternes aftale vedrørende implementering, drift, udvikling og support af GrantOnline-løsningen.

A.1.5 TK2 EPJ

Såfremt TK2 EPJ er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af it-systemet TK2 EPJ til den dataansvarlige, hvilket omfatter f.eks. vedligehold, support og løsning af konkrete opgaver fra den dataansvarlige, som nærmere specificeret i aftalen vedrørende levering af tjenesterne indgået mellem parterne.

A.1.6 Konsulentydelse

Såfremt Konsulentydelse er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er at udføre specifikt aftalte konsulentopgaver. Formålet vil derfor variere, men altid have en sammenhæng til en aftalt konsulentopgave.

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

A.2.1 Hosting og drift

Såfremt Hosting og drift er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren yder hosting og drift af den dataansvarliges it-systemer. Det primære formål med behandlingen udgør derfor hosting, herunder opbevaring af den dataansvarliges personoplysninger, og løbende drift, herunder overvågning, backup og vedligehold af den dataansvarliges it-systemer indeholdende personoplysninger.

Behandlingen kan i de konkrete tilfælde blandt andet omfatte organisering, systematisering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, genfindning, søgning, brug, sammenstilling, samkøring, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med opfyldelse af databehandlerens levering af tjenesterne til den dataansvarlige, eller når det er nødvendigt for at opfylde en konkret anmodning fra den dataansvarlige.

A.2.2 Service Desk

Såfremt Service Desk er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren yder support til den dataansvarliges ansatte etc. Alt arbejde, som databehandleren yder som en del af supporten, og som omfatter behandling af personoplysninger på vegne af den dataansvarlige, foregår på den dataansvarliges specifikke anmodning.

Databehandleren supporterer den dataansvarlige med den dataansvarliges daglige drift af dennes it-systemer. Databehandleren kan på den dataansvarliges opfordring overtage den dataansvarliges håndtering af den dataansvarliges it-systemer på deres arbejdsplads eller servere via TeamViewer eller Remote Desktop til en konkret opgave. Derudover kan databehandleren tilgå systemer til håndtering af fejlsøgning og driftsopgaver.

Ved fejl i software eller den dataansvarliges it-systemer i øvrigt kan databehandleren hente database fra den dataansvarlige med henblik på fejlsøgning, rettelser mv. Dette sker kun efter forudgående specifik aftale.

Behandlingen kan i de konkrete tilfælde blandt andet omfatte organisering, systematisering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, genfindning, søgning, brug, sammenstilling, samkøring, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med leveringen af de aftalte tjenester, eller når det er nødvendigt for at opfylde en anmodning fra den dataansvarlige.

A.2.3 SEPO Secure Mail

Såfremt SEPO Secure Mail er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren yder support, drift, backup og applikationsvedligehold.

Tjenesten tilbyder specifikt:

- Kryptering/dekryptering/signering/videresendelse af e-mails (og evt. Digital Post/e-Boks-meddelelser) til og fra den dataansvarlige.
- Opbevaring af den dataansvarliges kryptografiske nøgle(r).

A.2.4 GrantOnline

Såfremt GrantOnline er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren yder installation, support, drift og udviklingsaktiviteter på GrantOnline-løsningen. Behandlingen omfatter desuden backup, overvågning og virusscanning.

A.2.5 TK2 EPJ

Såfremt TK2 EPJ er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren yder vedligeholdelse og support af it-systemet TK2 EPJ til den dataansvarlige. Alt arbejde, som databehandleren yder, og som omfatter behandling af personoplysninger på vegne af den dataansvarlige, foregår på den dataansvarliges specifikke anmodning.

Databehandleren supporterer den dataansvarlige i Team Viewer. Databehandleren kan på den dataansvarliges opfordring overtage den dataansvarliges håndtering af systemet via Team Viewer til en konkret opgave.

Ved fejl i produktet kan databehandleren hente TK2 SQL-database fra den dataansvarlige med henblik på fejlsøgning, tilretninger mv.

Behandlingen kan i de konkrete tilfælde hermed blandt andet omfatte organisering, systematisering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, genfinding, søgning, brug, sammenstilling, samkøring, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med leveringen af de aftalte tjenester, eller når det er nødvendigt for at opfylde en anmodning fra den dataansvarlige.

A.2.6 Konsulentydelse

Såfremt Konsulentydelse er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren udfører opgaver i forbindelse med specifikke og afgrænsede opgaver. Konsulentopgaverne udføres på den dataansvarliges systemer og data, og behandlingen vil være defineret i den konkrete opgave.

Opgaverne bestilles og defineres af dataansvarlig, og databehandleren indgår i nødvendigt omfang i at sikre korrekt opgavedefinition.

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

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 4, stk. 1 og artikel 6):

Almindelige personoplysninger.

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

Racemæssig eller etnisk baggrund.

Politisk overbevisning.

Religiøs overbevisning.

Filosofisk overbevisning.

Fagforeningsmæssige tilhørsforhold.

Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.

Seksuelle forhold.

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9):

Strafbare forhold.

Væsentlige sociale problemer.

Andre rent private forhold, som ikke er nævnt ovenfor:

Andre private forhold.

Oplysninger om CPR-nummer (jf. Databeskyttelsesforordningens artikel 87):

CPR-numre.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kategorier af registrerede, identificerede eller identificerbare fysiske personer, som databehandlerens behandlinger vedrører:

Ansatte

Børn

Den dataansvarliges egne kunder

Andre kategorier som nærmere specificeret.

Specify andre kategorier

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige påbegyndes, efter parternes aftale vedrørende levering af tjenesterne træder i kraft, og indtil denne ophører.

Bilag B – Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN/ADRESSE	CVR	LOKATION FOR BEHANDLING	BESKRIVELSE AF BEHANDLING
IT Relation Prag s.r.o. Bucharova 1281/2, Stodůlky 158 00 Praha 5 Czech Republic	CVR-no.: 07628919	Europæiske Økono- misk Samarbejdsom- råde EØS	Backup. Patch Management, overvågning, konsulent ydel- ser, Fejlsøgning og installation
ServiceNow Nederland B.V. Hoekenrode 3 1102 BR Amsterdam Holland	CVR: 813457032	Europæiske Økono- misk Samarbejdsom- råde EØS	Sagshåndtering
B4Restore A/S Åhave Parkvej 31 8260 Viby J	CVR: 27719945	Europæiske Økono- misk Samarbejdsom- råde EØS	Backup

Listen over anvendte underdatabehandlere ved aftaleindgåelse er indsat i ovenstående skema og bliver reguleret ved tilkøb eller ændringer i services.

Efter Bestemmelsernes ikrafttræden må databehandleren gøre brug af andre underdatabehandlere. Den dataansvarlige vil blive informeret om ændringer i anvendte databehandlere ved tilkøb af nye services eller databehandlerens ændringer af services. Derudover kan et bilag over aktuelt anvendte underdatabehandlere leveres ved forespørgsel.

Databehandlerens meddelelse om planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere sker som beskrevet i B.2.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandlerens underretning om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere skal være den dataansvarlige i hænde minimum 30 dage, før anvendelsen eller ændringen skal træde i kraft, så vidt dette umiddelbart er muligt.

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. Sådant manglende opfyldelse kan ikke tilskrives databehandlerens misligholdelse. Databehandleren opretholder sit krav på betaling for sådanne ydelser, uanset de ikke kan leveres til den dataansvarlige.

Hvor det er særligt aftalt, at databehandleren ikke må gøre brug af underdatabehandlere uden den dataansvarliges forudgående tilladelse, accepterer den dataansvarlige, at dette kan medføre, at databehandleren kan blive afskåret fra at opfylde tjenesterne. Hvis den dataansvarlige har afslået, at der foretages ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere, vil manglende levering af tjenester derfor ikke anses for en misligholdelse af parternes aftale vedrørende levering af tjenesterne, som kan tilskrives databehandleren i de tilfælde, hvor den manglende opfyldelse kan henføres til en underdatabehandleres forhold.

Bilag C - Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker i henhold til de indgåede aftaler mellem den dataansvarlige og databehandleren.

Databehandleren baserer sit ledelsessystem for informationssikkerhed på principperne i ISO 27001 sikkerhedsframework og har implementeret de relevante kontroller, standarden definerer. Derudover har databehandleren implementeret et ledelsessystem for sikker behandling af persondata.

Kontrollerne styres i et ISMS-system for ISO 27001 og PIMS-system for GDPR. Herved dokumenteres kontroller løbende, og findings fra interne audits anvendes til løbende forbedringer.

Databehandleren revideres desuden en gang årligt, hvor der udarbejdes en ISAE 3402 erklæring for drift, hosting og support, samt en ISAE 3000 erklæring, som dokumenterer overholdelse af databehandlerens generelle databehandleraftaler og kontroller. Derudover opretholder og vedligeholder databehandleren løbende en ISO 27001:2013-certificering.

Seneste erklæringer og certifikat ligger altid tilgængelig på databehandlerens hjemmeside.

Den dataansvarlige har instrueret databehandleren i at behandle data ud fra de Services, der er indgået aftale om og ud fra nedenstående instrukser.

C.1.1 Hosting og drift

Såfremt Hosting og drift er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Opbevaring og backup samt de dertil knyttede behandlingsaktiviteter, som er nødvendige i forbindelse med leveringen af de aftalte tjenester, eller som er nødvendige for at opfylde en anmodning eller instruks fra den dataansvarlige. Behandlinger, som foretages af databehandleren omfatter:

- Backup og backupkontroller.
- Patch Management.
- Drift og vedligehold af systemer og infrastruktur.
- Virusscanning og opfølgning på virusalarmer.
- Installationer og konfigurationer.
- 24x7-overvågning og håndtering af overvågningsalarmer.
- Dokumentation af assets, procedurer og kontroller.

C.1.2 Service Desk

Såfremt Service Desk er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandling foretages i overensstemmelse med ydelser forbundet med de supportydelser, parternes aftale vedrørende levering af tjenesterne indeholder eller specifikke sager, den dataansvarlige igangsætter.

C.1.3 SEPO Secure Mail

Såfremt SEPO Secure Mail er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker som led i udførelse af de aftalte ydelser for SEPO Secure Mail, herunder:

- Backup.
- Support.
- Drift og vedligehold.
- Udførelse af projekter.
- Dokumentation.
- Kryptering/dekryptering/signering af e-mails.
- Videreudsendelse af e-mails til og fra andre e-mailmodtagere og den dataansvarlige evt. Digital Post/e-Boks.

og dertil knyttede behandlingsaktiviteter, som er nødvendige i forbindelse med leveringen af tjenesterne, eller som er nødvendige for at opfylde en anmodning eller instruks fra den dataansvarlige.

C.1.4 GrantOnline

Såfremt GrantOnline er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren udfører udelukkende behandling efter dokumenteret instruks, medmindre behandlingen kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som leverandøren er underlagt. I sådanne tilfælde underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. Databeskyttelsesforordningens art 28, stk. 3, litra a.

C.1.5 TK2 EPJ

Såfremt TK2 EPJ er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker som led i udførelse af tjenesterne under parternes særskilte aftale herom, herunder:

- Support.
- Vedligehold.
- Udførelse af projekter.
- Dokumentation.
- Andre opgaver på anmodning fra den dataansvarlige, som kan kræve adgang til den dataansvarliges systemer eller behandling af personoplysninger på vegne af den dataansvarlige.

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

- Support på it-system TK2 EPJ.

C.1.6 Konsulentydelse

Såfremt Konsulentydelse er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandling må udelukkende foretages på baggrund af konkret aftalte konsulentopgaver.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle et generelt højt sikkerhedsniveau, som afspejler de typer af data, der behandles. Tekniske og organisatoriske foranstaltninger er implementeret i henhold til ISO 27001-standarden, og kontroller fra ISO 27002 er implementeret og efterleves.

Derudover skal sikkerhedsniveauet afspejle de specifikke aftalte ydelser i parternes aftale vedrørende levering af tjenesterne.

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

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

På aftaleindgåelsestidspunktet indebærer forpligtelsen for databehandleren til at gennemføre sikkerhedsforanstaltninger, at databehandleren skal implementere og opretholde det sikkerhedsniveau, der er beskrevet i dokumenterne "Organisatoriske og tekniske foranstaltninger" og "Fysisk og logisk sikkerhed". Dokumenterne er tilgængelige på www.itrelation.dk/gdpr-dokumenter. Disse krav til sikkerhed udgør den dataansvarliges samlede krav til sikkerhedsforhold hos databehandleren ud fra den dataansvarliges egen risikovurdering.

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:

C.4 Opbevaringsperiode/sletterutine

Den dataansvarlige disponerer selv over personoplysninger, som databehandleren behandler på vegne af den dataansvarlige. De personoplysninger, der er overladt til databehandlerens behandling, opbevares derfor, indtil den dataansvarlige selv sletter oplysningerne eller indtil ophør af tjenesterne vedrørende behandling af personoplysninger.

Ved sletning af personoplysninger i den dataansvarliges systemer, vil disse personoplysninger blive slettet i databehandlerens backupsystem ud fra den aftalte opbevaringsperiode (backuphistorik) for hvert enkelt system.

Databehandleren bistår på den dataansvarliges anmodning med sletning eller tilbagelevering af personoplysninger som nærmere instrueret af den dataansvarlige.

C.5 Lokalt for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Behandlingen af persondata sker på databehandlerens adresser samt de anførte databehandlere og deres underdatabehandleres adresser.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjeland

Den dataansvarlige har bemyndiget og dermed instrueret databehandleren i at overføre personoplysninger til et tredjeland som nærmere specificeret nedenfor. Den dataansvarlige kan herudover ved en efterfølgende skriftlig meddelelse eller aftale angive en instruks eller konkret godkendelse vedrørende overførsel af personoplysninger til et tredjeland.

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

C.6.1 Generel godkendelse vedrørende overførsel af personoplysninger til sikre tredjelande

Den dataansvarlige giver ved Bestemmelserne sin generelle og forudgående godkendelse (instruks) til, at databehandleren kan foretage overførsel af personoplysninger til tredjelande, hvis Kommissionen har fastslået, at tredjelandet/det relevante område/den relevante sektor har et tilstrækkeligt beskyttelsesniveau.

C.6.2 Godkendelse af overførsel til specifikke modtagere af personoplysninger i tredjelande, når der er sikret for-nødne garantier

Den dataansvarlige instruerer databehandleren til at anvende nedenstående underdatabehandler(e), hvor der sker overførsel af personoplysninger til tredjelande:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND
ServiceNow Nederland B.V.	CVR: 813457032	Hoekenrode 3 1102 BR Amsterdam Holland	Sagshåndtering	Ja Overførselsgrundlag: SCC

Den dataansvarlige har ved indgåelsen af Bestemmelserne givet godkendelse til brugen af ovenstående underdatabehandler(e) samt instruks om overførelse af personoplysninger til tredjelande ved levering af tjenesterne.

Som overførselsgrundlag indgås EU-Kommissionens til enhver tid gældende Standardkontrakter (SCC). Databehandleren og ovenstående underdatabehandler(e) er bemyndiget til at indgå en SCC på vegne af den dataansvarlige. Det betyder, at den dataansvarlige skal anses som dataeksportør i forhold til indgåelse af SCC, og at den dataansvarlige i forbindelse med overførslerne af oplysninger til ovenstående underdatabehandler(e) accepterer at være bundet af de forpligtelser, som SCC pålægger dataeksportøren.

I tilfælde af at EU-Kommissionen udarbejder nye SCC'er efter aftaleindgåelsen, er databehandleren bemyndiget til at udskifte, opdatere og anvende de til enhver tid gældende SCC'er.

Indholdet af denne instruks og/eller Bestemmelserne anses ikke for at ændre indholdet af SCC.

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

Den dataansvarlige har efter databeskyttelsesforordningens art. 24 og 28 ret og pligt til at gennemføre tilsyn med databehandlerens behandling af personoplysninger på den dataansvarlige vegne. Den dataansvarliges gennemførelse af tilsyn med databehandleren kan ske ved, at den dataansvarlige udfører en af følgende handlinger:

- egenkontrol på baggrund af dokumenter, som databehandleren gør tilgængelig for den dataansvarlige,
- skriftligt tilsyn eller
- fysiske inspektioner.

C.7.1 Egenkontrol

Den dataansvarlige har på www.itrelation.dk/gdpr-dokumenter adgang til en række dokumenter til brug for gennemførelse af egenkontrol, herunder:

- Nyeste version af databehandlerens ISAE 3402-erklæring (publiceres hvert år i februar måned).
- Beskrivelse af fysisk og organisatorisk sikkerhed hos databehandleren.
- Risikovurdering – af delt infrastruktur (firewall, backup etc.).
- IT Sikkerhedspolitik.

- Beredskabsplaner hos databehandleren.

C.7.2 Skriftligt tilsyn og fysisk inspektion

Den dataansvarlige kan vælge at gennemføre et tilsyn enten som skriftligt tilsyn eller ved fysisk inspektion. Tilsynet kan udføres af den dataansvarlige selv og/eller i samarbejde med tredjepart. Et tilsyn skal tage udgangspunkt i de sikkerhedsforanstaltninger, der er aftalt mellem parterne.

Ved anmodning om gennemførelse af skriftligt tilsyn eller fysisk inspektion skal den til enhver tid gældende formular, tilgængelig på www.itrelation.dk/gdpr-dokumenter anvendes.

Procedure og rapportering for skriftligt tilsyn eller fysisk inspektion:

- Den dataansvarlige udfylder formularen vedrørende tilsyn tilgængelig på databehandlerens www.itrelation.dk/gdpr-dokumenter.
- Den dataansvarlige kontakter databehandleren via e-mail til gdpr@itrelation.dk med udfyldt formular med ønske om gennemførelse af tilsyn og/eller inspektion.
- Databehandleren bekræfter modtagelse og oplyser endelig dato for gennemførelse af tilsynet og/eller inspektion.
- Gennemførelsen af tilsynet og/eller inspektion finder sted.
- Den dataansvarlige udarbejder en rapport, der efterfølgende fremsendes til databehandleren. Rapporten skal udarbejdes på baggrund af skabelonen tilgængelig på www.itrelation.dk/gdpr-dokumenter.
- Databehandleren gennemgår udkastet til rapporten og kommenterer evt. på den dataansvarliges eventuelle observationer (kan gentages flere gange).
- Endelig rapport konkluderes af den dataansvarlige.
- Tilsynet afsluttes.

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

Databehandleren udfører, på baggrund af databehandlerens risikovurdering og under hensyntagen til de konkrete behandlingsaktiviteter, revisioner, herunder inspektioner, med underdatabehandleres behandling af personoplysninger enten i form af egenkontrol af revisionserklæringer og tilsvarende (hvor muligt), skriftligt tilsyn eller fysisk inspektion, eller en kombination heraf.

Den dataansvarlige kan på den dataansvarliges anmodning få yderligere oplysninger om, hvilke kontrolforanstaltninger der er iværksat og gennemført over for de enkelte underdatabehandlere.

Bilag D – Parternes regulering af andre forhold

D.1 Generelt

I relation til databehandlerens behandling af personoplysninger på vegne af den dataansvarlige har parterne aftalt den nedenfor indgivne særregulering.

I tilfælde af uoverensstemmelse mellem Bestemmelserne og de i dette bilag D fastsatte vilkår skal bilag D have forrang.

D.2 Konsekvenser af den dataansvarliges ulovlige instruks

Den dataansvarlige er bekendt med, at databehandleren er afhængig af den dataansvarliges anvisninger om, i hvilket omfang databehandleren er berettiget til at anvende og behandle personoplysningerne på den dataansvarliges vegne. Databehandleren hæfter derfor ikke for krav, som udspringer af databehandlerens handlinger eller undladelser, i det omfang disse handlinger eller undladelser er en direkte databehandlingsaktivitet udøvet i overensstemmelse med den dataansvarliges instrukser.

D.3 Implementering af andre sikkerhedsforanstaltninger

Databehandleren er berettiget til at implementere og opretholde alternative sikkerhedsforanstaltninger i forhold til det i aftalen vedrørende levering af tjenesterne og bilag C.2 anførte, dog under forudsætning af at sådanne alternative sikkerhedsforanstaltninger som minimum giver samme sikkerhed som de foreskrevne sikkerhedsforanstaltninger.

D.4 Anvendelse af underdatabehandler, som leverer på standardvilkår

Uanset punkt 7 skal det understreges, at hvis databehandleren anvender en underdatabehandler, som leverer sine ydelser på egne vilkår, som databehandleren ikke har mulighed for at aftale fravigelser til, gælder underdatabehandlerens vilkår for de behandlingsaktiviteter, der overlades til udførelse hos sådan underdatabehandler. Hvor der sker behandling på en underdatabehandlers vilkår, er dette angivet ved den relevante underdatabehandler på oversigten over underdatabehandlere, som er tilgængelig på www.itrelation.dk/gdpr-dokumenter. Ved Bestemmelserne giver den dataansvarlige sin accept af og instruks om, at sådanne konkrete behandlingsaktiviteter sker på underdatabehandlerens vilkår.

D.5 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.6 Vederlag

D.6.1 Bistand

Databehandleren er berettiget til vederlag for bistand efter de i Bestemmelsernes punkt 9 aftalte bistandsydelser. Vederlaget opgøres på baggrund af den forbrugte arbejdstid og de aftalte timesatser i aftalen vedrørende levering af tjenesterne, og hvor der ikke er aftalt timesatser heri, da efter databehandlerens gældende timesatser samt med tillæg af eventuelt afholdte positive omkostninger, herunder også omkostninger der skal afholdes af databehandleren for underdatabehandleres bistand.

Fører databehandlerens bistand til krav om skærpelse af de sikkerhedsforanstaltninger, der skal iagttages i forhold til det aftalte i aftalen vedrørende leveringen af tjenesterne og Bilag C, gennemfører databehandleren, så vidt det er muligt, sådanne yderligere sikkerhedsforanstaltninger efter nærmere aftale med den dataansvarlige, forudsat databehandleren modtager betaling herfor.

D.6.2 Implementering af øvrige sikkerhedsforanstaltninger

Fører den dataansvarliges krav eller databehandlerens løbende vurderinger til skærpelse af kravene til sikkerhedsforanstaltninger i forhold til det aftalte, implementerer og gennemfører databehandleren sådanne yderligere sikkerhedsforanstaltninger efter nærmere aftale med den dataansvarlige, forudsat databehandleren modtager betaling herfor.

Den dataansvarlige kan anmode om databehandlerens assistance i forbindelse med sletning af personoplysninger.

D.6.3 Tilsyn og revision

Databehandleren er berettiget til vederlag for den dataansvarliges udøvelse af tilsyn og revision. Vederlaget opgøres på baggrund af den forbrugte arbejdstid og de aftalte timesatser i aftalen vedrørende levering af tjenester, og hvor der ikke er aftalt timesatser heri, da efter databehandlerens gældende timesatser samt med tillæg af eventuelt afholdte positive omkostninger, herunder også omkostninger der skal afholdes af databehandleren for underdatabehandleres bistand.

D.7 Ansvar og misligholdelse

En eventuel misligholdelse af Bestemmelserne reguleres og behandles i overensstemmelse med parternes aftale vedrørende levering af tjenesterne.

I tilfælde hvor databehandleren har udredt beløb til registrerede i overensstemmelse med Databeskyttelsesforordningens artikel 82 eller erstatningsansvarsloven § 26, har databehandleren fuld regres mod den dataansvarlige for det udredte beløb, som beløbsmæssigt overstiger den aftalte ansvarsbegrænsning i parternes aftale vedrørende levering af tjenesterne. Parterne har hermed aftalemæssigt fraveget Databeskyttelsesforordningens artikel 82, stk. 5 og erstatningsansvarsloven § 26.

Uanset databeskyttelsesforordningen art 82, stk. 5 kan en part, der har udredt erstatningsbeløb til en skadelidt, der ikke svarer til fuld erstatning, gøre regres efter princippet i art. 82, stk. 5.

I forhold til anden godtgørelse for ikke-økonomiske tab til de registrerede skal princippet i art. 82 ligeledes finde anvendelse, for så vidt angår den interne endelige ansvarsfordeling mellem databehandleren og den dataansvarlige.

Parterne kan ikke gøre regres eller erstatningskrav gældende overfor den anden part for bøder eller anden straf, der er pålagt i medfør af databeskyttelsesloven § 41 samt for bødeforelæg accepteret efter databeskyttelsesloven § 42.

D.8 Fravigelser

Parterne har aftalt følgende fravigelser til Bestemmelserne samt nærværende bilag:

BESTEMMELSERNE/AFSNIT	FRAVIGELSE TIL BESTEMMELSERNE
Afsnit 7.6	<p>Parterne har aftalt, at Bestemmelsernes punkt 7.6 (som udfærdiget nedenfor) ikke skal finde anvendelse mellem parterne.</p> <p>Følgende tekst udgår derfor af Bestemmelserne: "Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredje-mand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlerne, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne."</p>

BILAG/AFSNIT	FRAVIGELSE TIL BILAGENE
A.1	<p>Bilag A.1 omskrives til:</p> <p><u>A.1.1 Hosting og drift</u> Såfremt Hosting og drift er valgt som ydelse i skemaet i bilag A.1. gælder følgende:</p> <p>Formålet med behandlingen er levering af hosting og drift af den dataansvarliges it-systemer herunder backup, overvågning, vedligehold og support som nærmere specificeret i aftalen vedrørende levering af tjenesterne indgået mellem parterne. Herunder også specifikke opgaver bestilt af den dataansvarlige.</p> <p><u>A.1.6 Konsulentydelse</u> Såfremt Konsulentydelse er valgt som ydelse i skemaet i bilag A.1. gælder følgende:</p> <p>Formålet med behandlingen er at udføre specifikt aftalte konsulentopgaver. Formålet vil derfor variere, men altid have en sammenhæng til en aftalt konsulentopgave.</p>
A.2	<p>Bilag A.2 omskrives til:</p> <p><u>A.2.1 Hosting og drift</u> Såfremt Hosting og drift er valgt som ydelse i skemaet i bilag A.1. gælder følgende:</p> <p>Databehandleren yder hosting og drift af den dataansvarliges it-systemer. Det primære formål med behandlingen udgør derfor hosting, herunder opbevaring af den</p>

dataansvarliges personoplysninger, og løbende drift, herunder overvågning, backup og vedligehold af den dataansvarliges it-systemer indeholdende personoplysninger.

Behandlingen kan i de konkrete tilfælde blandt andet omfatte organisering, systematisering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, genfindning, søgning, brug, sammenstilling, samkøring, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med opfyldelse af databehandlerens levering af tjenesterne til den dataansvarlige, eller når det er nødvendigt for at opfylde en konkret anmodning fra den dataansvarlige.

A.2.6 Konsulentydelse

Såfremt Konsulentydelse er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren udfører opgaver i forbindelse med specifikke og afgrænsede opgaver. Konsulentopgaverne udføres på den dataansvarliges systemer og data, og behandlingen vil være defineret i den konkrete opgave.

Opgaverne bestilles og defineres af dataansvarlig, og databehandleren indgår i nødvendigt omfang i at sikre korrekt opgavedefinition.

C.1

Bilag C.1 omskrives til:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker i henhold til de indgåede aftaler mellem den dataansvarlige og databehandleren.

Databehandleren baserer sit ledelsessystem for informationssikkerhed på principperne i ISO 27001 sikkerheds-framework og har implementeret de relevante kontroller, standarden definerer. Derudover har databehandleren implementeret et ledelsessystem for sikker behandling af persondata.

Kontrollerne styres i et ISMS-system for ISO 27001 og PIMS-system for GDPR. Herved dokumenteres kontroller løbende, og findings fra interne audits anvendes til løbende forbedringer.

Databehandleren revideres desuden en gang årligt, hvor der udarbejdes en ISAE 3402 erklæring for drift, hosting og support, samt en ISAE 3000 erklæring, som dokumenterer overholdelse af databehandlerens generelle databehandleraftaler og kontroller. Derudover opretholder og vedligeholder databehandleren løbende en ISO 27001:2013-certificering.

Seneste erklæringer og certifikat ligger altid tilgængelig på databehandlerens hjemmeside.

Den dataansvarlige har instrueret databehandleren i at behandle data ud fra de Services, der er indgået aftale om og ud fra nedenstående instrukser.

C.1.1 Hosting og drift

Såfremt Hosting og drift er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Opbevaring og backup samt de dertil knyttede behandlingsaktiviteter, som er nødvendige i forbindelse med leveringen af de aftalte tjenester, eller som er nødvendige for at opfylde en anmodning eller instruks fra den dataansvarlige. Behandlinger, som foretages af databehandleren omfatter:

- Backup og backupkontroller.
- Patch Management.
- Drift og vedligehold af systemer og infrastruktur.
- Virusscanning og opfølgning på virusalarmer.
- Installationer og konfigurationer.
- 24x7-overvågning og håndtering af overvågningsalarmer.
- Dokumentation af assets, procedurer og kontroller.

C.1.6 Konsulenttydelser

Såfremt Konsulenttydelser er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandling må udelukkende foretages på baggrund af konkret aftalte konsulentopgaver.

C.3

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

Registreredes rettigheder, jf. pkt. 9.1.

- Databehandleren skal bistå med at iagttage de registreredes rettigheder ved bl.a. at kunne give indsigt i, slette, begrænse og berigtige oplysninger samt sørge for at dette også sker hos underdatabehandlerne
- Databehandleren skal bistå med at opfylde de registreredes rettigheder uden unødigt forsinkelse

Databehandleren skal have udarbejdet en procedure for, hvordan de behandler anmodninger fra en registreret om deres rettigheder

Brud og hændelser, jf. pkt. 9.2. Informationer som skal sendes:

- 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.3

Databehandleren bistår, uden særskilt vederlag, i overensstemmelse med Bestemmelse 9.1 og 9.2 såfremt dette er krævet under Databeskyttelsesforordningen og nationalt implementeret databeskyttelseslov. Såfremt henvendelsen relaterer direkte til

en evt tilkøbt User Management service, anerkender den dataansvarlige at databehandleren kan kræve særskilt vederlag herfor.