

# Underdatabehandleraftale



**No Problem  
Kulturen**



## Indholdsfortegnelse

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

## Underdatabehandleraftalebestemmelser

Den nærværende databehandleraftale er lavet på Datatilsynets standardkontraktbestemmelser.

Parterne er bekendte med, at der er tale om et underdatabehandlerforhold.

Den dataansvarlige IT Relation A/S (CVR 27001092) indgår nærværende aftale som databehandler i forhold til sine egne kunder, og det er således den dataansvarliges kunders personoplysninger, som databehandleren behandler på vegne af den dataansvarlige. I den forbindelse anvender Progressive A/S som databehandleren IT Relation A/S som underdatabehandler.

Parterne er således bekendte med, at når der i aftalen omtales "den dataansvarlige" skal det forstås som databehandler i forhold til kundernes egne personoplysninger.

Ligeledes er parterne bekendte med, at når der i aftalen omtales "databehandleren" skal det forstås som underdatabehandler i relation til ovennævnte databehandler.

### 1. Standardkontraktbestemmelser

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

mellem

Progressive A/S  
Lyskær 3B  
2730 Herlev  
CVR-nr.: 26107911  
(herefter "den dataansvarlige")

og

IT Relation A/S  
Dalgas Plads 7b, 1  
CVR-nr.: 27001092  
(herefter "databehandleren")

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

har 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 aftalte services ("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 90 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 databehandleraftalen. 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. 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 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 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 Torben Friedrichsen  
Stilling CTO  
Telefonnummer +45 24292477  
E-mail [tf@progressive.dk](mailto:tf@progressive.dk)

Underskrift

På vegne af databehandleren

Navn Frank Bech Jensen  
Stilling Head of Compliance and Security  
Telefonnummer +45 40906035  
E-mail [frbec@itm8.com](mailto:frbec@itm8.com)

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.

Navn Frank Bech Jensen  
Stilling Head of Compliance and Security  
Telefonnummer +45 40906035  
E-mail [frbec@itrelation.dk](mailto:frbec@itrelation.dk)

Navn Lone Skov-Madsen  
Stilling CISO  
Telefonnummer +45 24624757  
E-mail [lsm@progressive.dk](mailto:lsm@progressive.dk)

## **Bilag A – Oplysninger om behandlingen**

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

Formålet med behandlingen er at levere en eller flere af nedenstående services.

#### A.1.1 Hosting og drift

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 Services indgået mellem parterne. Herunder også specifikke opgaver bestilt af den dataansvarlige.

#### A.1.2 Service Desk

Formålet med behandlingen er levering af supportydelser 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 Konsulentytelser

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

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, genfinding, søgning, brug, sammenstilling, samkøring, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med opfyldelse af databehandlerens levering af Services til den dataansvarlige, eller når det er nødvendigt for at opfylde en konkret anmodning fra den dataansvarlige.

#### A.2.2 Service Desk

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, 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.2.3 Konsulentytelser

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**

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

Almindelige personoplysninger (jf. Databeskyttelsesforordningens 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**

Behandlingen omfatter følgende kategorier af registrerede:

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

Ansatte

Børn

Kundens egne kunder

Andre kategorier som nærmere specificeret.

**A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser ikrafttræden. 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 nedenstående underdatabehandlere. Underdatabehandleren tages i anvendelse alt efter hvilke services der aftales leveret af databehandleren.

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Omnidocs Wilders Plads 15A 1403 Copenhagen K	CVR: 35679529	Europæiske Økonomisk Samarbejdsområde EØS	Generering af rapporter og dokumenter
Competella AB Fleminggatan 48 112 33 Stockholm Sverige	CVR: 556781- 5070	EU og Pakistan	Omstillingsbord til teams
Crayon A/S Tobaksvejen 2A, 3. sal 2860 Søborg	CVR: 29832684	Europæiske Økonomisk Samarbejdsområde EØS	Azure reseller og support
Curanet A/S Højvangen 4 8669 Skanderborg	CVR: 29412006	Europæiske Økonomisk Samarbejdsområde EØS	Web hosting
Data & More Flæsketorvet 68 1711 København V	CVR: 38185659	Indenfor EU	Scanning af ustrukturerede data for persondata
Entrust Datacard Denmark A/S Park Allé 350D 2605 Brøndby	CVR: 21780340	Hele verden	To faktor validering
F-Secure Danmark A/S Rued Langgaards Vej 8 2300 Copenhagen S	CVR: 32559409	Inden og udenfor EU	Antivirus og sårbarhedsscanning
FastTrack Software ApS Niels Jernes Vej 10 9220 Aalborg	CVR: 31938112	Indenfor EU	Sikkerhedsprodukter
Flexfone A/S Danmarksvej 26 8660 Skanderborg	CVR: 34042985	Telefoni: Indenfor EU	Telefoni

		<p>Teams Integration: USA, Canada, Isreal, Indien, Malaysia, Mexico.</p> <p>Udenlandske numre: USA, Hongkong, Belgien</p> <p>Flexfone Test App: USA, Egypten</p>	
<p>Front-Safe A/S Spotorno Alle 12, 2 Høje Taastrup 2630 Taastrup</p>	<p>CVR: 29631123</p>	<p>Europæiske Økonomisk Samarbejdsområde EØS, samt artikel 45 lande</p>	<p>Backup</p>
<p>Heimdal Security A/S Vester farimagsgade 1, 3 1606 København V</p>	<p>CVR: 35802495</p>	<p>Europæiske Økonomisk Samarbejdsområde EØS</p>	<p>Sikkerhedsprodukter</p>
<p>J2 Global Denmark Spotorno Alle 12 Høje Taastrup 2630 Taastrup</p>	<p>CVR: 28117833</p>	<p>Europæiske Økonomisk Samarbejdsområde EØS, samt artikel 45 lande</p>	<p>Vipre Spam filter</p>
<p>Keepit A/S Per Henrik Lings Allé 4, 4 sal 2100 København Ø</p>	<p>CVR: 30806883</p>	<p>Europæiske Økonomisk Samarbejdsområde EØS</p>	<p>Azure backup</p>
<p>Microsoft Ireland Operations, Ltd. South County Business Park Leopardstown</p>	<p>SE-nr.: IE8256796U</p>	<p>Data er lagret indenfor EU, men support sager kan blive håndteret fra hele verden.</p>	<p>Microsoft O365 og Azure</p>
<p>Miracle 42 A/S Borupvang 2C, st 2750 Ballerup</p>	<p>CVR: 40111751</p>	<p>Europæiske Økonomisk Samarbejdsområde EØS</p>	<p>Oracle</p>
<p>IT Relation Philippines Inc. 3rd Floor, 719 GM Building, Real Street Corner</p>	<p>TIN: 739- 283-935- 000</p>	<p>Filippinerne</p>	<p>Backup, Vedligehold, Patch Management, 24X7 Overvågning.</p>

Luke Wright Street, Dumaguete City 6200 Negros Oriental			Hvor specifikt aftalt: Engelsksproget support
itm8 s.r.o Bucharova 1281/2, Stodůlky 158 00 Praha 5 Tjekkiet	CVR: 07628919	Europæiske Økonomisk Samarbejdsområde EØS	Servicedesk og bruger support, Backup og backupkontroller, Patch Management, Drift og vedligehold af systemer og infrastruktur, Virusscanning og opfølgning på virusalarmer, Installationer og konfigurationer, Overvågning og håndtering af overvågningsalarmer, Dokumentation af assets, procedurer og kontroller, Håndtering af specifikke kunde forespørgsler og konkret aftalte konsulentopgaver.
Panorama9 ApS Flaesketorvet 28 1. 1711 København V	CVR: 33396880	Europæiske Økonomisk Samarbejdsområde EØS  Men underdatabehandlere må overføre til 3. lande	Overvågning
Symantec/Norton		Hele verden	
CyberPilot ApS Fredens Torv 8 B 1. Sal 8000 Aarhus C	CVR: 37435382	Europæiske Økonomisk Samarbejdsområde EØS  De bruger Amazon i Europa som datacenter	Awareness træning
Rapid 7 120 Causeway Street Suite 400 Boston, MA 02114		Europæiske Økonomisk Samarbejdsområde EØS	SIEM
B4Restore A/S Åhave Parkvej 31 8260 Viby J	CVR: 27719945	Danmark	Backup



Uniqkey ApS Lyskær 8a, st, tv 2730 Herlev	CVR: 39004127	Europæiske Økonomisk Samarbejdsområde EØS  De bruger Amazon i Europa som datacenter	
Mentor IT A/S Lindevej 8 6710 Esbjerg V	CVR: 25576861	Europæiske Økonomisk Samarbejdsområde EØS	Konsulent bistand
Cira Apps Limited 2255 South Bascom Avenue Campbell, CA		Europæiske Økonomisk Samarbejdsområde EØS  De bruger Azure datacentre i Europa	Sync af kontaktpersoner og kalendere til smartphones.
Nasure A/S Rødovrevej 253C 2610 Rødovre	CVR: 35472525	Europæiske Økonomisk Samarbejdsområde EØS	EDI-Portal til TK2
Wehowsky.com ApS Sauntesvej 13 2820 Gentofte	CVR: 37783110	Europæiske Økonomisk Samarbejdsområde EØS	Muninn, Scanning af netværkstrafik
Xink ApS Tuborg Boulevard 12, 3. 2900 Hellerup "	CVR-no.: 32153283	Europæiske Økonomisk Samarbejdsområde EØS	Xink Branding and Xink Campaign
Printix.net ApS Hørkær 20 2730 Herlev	CVR: 36086416	Primært Europæiske Økonomisk Samarbejdsområde EØS og UK. For E-mail notification Services: USA	Cloud baseret print management system.
Cisco International Limited 9-11 New Square Bedfont Lakes Feltham Middlesex TW14 8HA	REG: 06640658	Europæiske Økonomisk Samarbejdsområde EØS samt USA og England	Drift, overvågning og vedligehold af netværksenheder samt analysering af netværkstrafik med henblik på at identificere og forebygge netværksnedbrud og mindske risikoen for cyber angreb.

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.

## **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 90 dage, før anvendelsen eller ændringen skal træde i kraft, så vidt dette umiddelbart er muligt.

## **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. 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

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

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

#### C.1.3 Konsulentytelser

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-standard, og kontroller fra ISO 27002 er implementeret og efterleves.

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

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 <https://legal.itm8.com>. 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:

På den dataansvarliges specifikke anmodning bistår databehandleren 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 udøvelse af de registreredes rettigheder som fastlagt i databeskyttelsesforordningen.

Hvis en registreret fremsætter anmodning om udøvelse af sine rettigheder over for databehandleren, giver databehandleren uden ugrundet ophold meddelelse herom til den dataansvarlige.

Under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, bistår databehandleren efter specifik anmodning også den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i forhold til:

- Gennemførelse af passende tekniske og organisatoriske foranstaltninger
- Sikkerhedsbrud
- Underretning om brud på persondatasikkerheden til den registrerede
- Gennemførelse af konsekvensanalyser
- Forudgående høringer fra tilsynsmyndighederne

### **C.4 Opbevaringsperiode/sletterutine**

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

### **C.5 Lokaltet for behandling**

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end et af databehandlerens datacentre.

### **C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande**

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 fornødne garantier

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

NAVN	CVR	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND
Omnidocs A/S	CVR: 35679529	Wilders Plads 15A 1403 Copenhagen K	Genering af rapporter og dokumenter
Microsoft Ireland Operations, Ltd.	SE-nr.: IE8256796U	South County Business Park Leopardstown	Microsoft O365 og Azure
Crayon A/S	CVR-nr: 29832684	Tobaksvejen 2A 2860 Søborg	Azure reseller og support
Entrust Datacard Denmark A/S	CVR: 21780340	Park Allé 350D 2605 Brøndby	To faktor validering
Competella AB	CVR: 556781-5070	Fleminggatan 48 112 33 Stockholm Sverige	Omstillingsbord til teams
F-Secure A/S	CVR-nr: 32559409	Rued Langgaards Vej 8 2300 Copenhagen S	Antivirus og sårbarhedsscanning
FastTrack Software ApS	CVR-nr: 31938112	Software ApS Niels Jernes Vej 10 9220 Aalborg	Sikkerhedsprodukter
Flexfone A/S	CVR: 34042985	Danmarksvej 26 8660 Skanderborg	Teams integration og udenlandske numre til Flexfone

NAVN	CVR	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND
Heimdal Security A/S	CVR: 35802495	Vester farimagsgade 1, 3 1606 København V	Sikkerhedsprodukter
IT Relation Philippines Inc.	TIN: 739-283-935-000	3rd Floor, 719 GM Building, Real Street Corner Luke Wright Street, Dumaguete City 6200 Negros Oriental	Behandlinger specificeret i C.1, C.1.1 og C.1.2
Panorama9 ApS	CVR: 33396880	Flaesketorvet 28 1. 1711 København V	
CyberPilot ApS	CVR: 37435382	Fredens Torv 8 B 1. Sal 8000 Aarhus C	Awareness træning
Cira Apps Limited		2255 South Bascom Avenue Campbell, CA	
Wehowsky.com ApS	CVR: 37783110	Saantesvej 13 2820 Gentofte	Skanning af netværkstrafik
Printix.net ApS	CVR: 36086416	Hørkær 20 2730 Herlev	Cloud baseret print management system.
Rapid 7		120 Causeway Street Suite 400 Boston, MA 02114	SIEM log management og sårbarhedsstyring
Cisco International Limited	REG: 06640658	9-11 New Square Bedfont Lakes Feltham Middlesex TW14 8HA	Drift, overvågning og vedligehold af netværksenheder samt analysering af netværkstrafik med henblik på at identificere og forebygge netværksnedbrud og mindske risikoen for cyber angreb.

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 Services.

Såfremt EU-Kommissionens standardkontrakter ("SCC") for overførelse af personoplysninger til et tredjeland anvendes som overførselsgrundlag, er databehandleren og/eller evt. underdatabehandleren berettiget til at indgå disse SCC'er med den relevante underdatabehandler.

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**

Databehandleren skal for egen regning indhente en revisionsrapport af typen ISAE 3402 type 2 eller tilsvarende fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser

Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i Databehandleraftalen, til rådighed for den dataansvarlige. Databehandleren giver herunder mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

Udføres revision af en anden end den dataansvarlige selv, skal denne anden revisor være uafhængig og ikke-konkurrerende i forhold til databehandleren og i øvrigt være underlagt fortroligheds- og tavshedspligt enten som følge af lov eller som følge af en fortrolighedsaftale, hvorpå Databehandleren kan støtte ret direkte over for den pågældende anden revisor.

Databehandleren underretter omgående den dataansvarlige, hvis en instruks om at stille oplysninger til rådighed eller give mulighed for revisioner og inspektioner efter databehandlerens mening er i strid med persondataforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller national ret.

### **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 i overensstemmelse med proceduren beskrevet ovenfor i punkt C.7.

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 Bestemmelser om begunstiget tredjemand ift. underdatabehandlere**

Parterne har aftalt, at Bestemmelsernes punkt 7.6 (som udfærdiget nedenfor) ikke skal finde anvendelse mellem parterne.

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