

# Databehandleraftale

## 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	14
Bilag C - Instruks vedrørende behandling af personoplysninger	17
Bilag D – Parternes regulering af andre forhold	23

## Databehandleraftalebestemmelser

### 1. Standardkontraktbestemmelser

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

mellem

Kunden

(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(r) om IT-ydelser ("Serviceaftalen", "Servicen" og/eller "Services") behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser. Bestemmelserne kan dække databehandlerens behandlingsaktiviteter under flere selvstændige Serviceaftaler indgået mellem Parterne.
4. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
5. 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.
6. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
7. 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.
8. Bilag D indeholder supplerende vilkår.
9. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
10. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden ufravigelig 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 instruksens 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 Services 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. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7 og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

## 13. Parternes aftale om andre forhold

1. Parterne kan i aftale om levering af Services ("Serviceaftalen") eller i Bilag D, aftale andre bestemmelser 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 Servicen vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af Servicen vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af Services 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

Bestemmelserne anses som tiltrådt i forbindelse med underskrift af parternes aftale vedrørende levering af Services eller ved selvstændig underskrift af Bestemmelserne.

## 15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Se Kontraktens afsnit 3 for kontaktpersoner hos den dataansvarlige og databehandleren. Parterne kan kontakte hinanden via disse.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

## 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:

#### 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 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 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**

Se Aftalens afsnit 3 for typer af personoplysninger om de registrerede.

**A.4. Behandlingen omfatter følgende kategorier af registrerede**

Se Aftalens afsnit 3 for kategorier af registrerede.

**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 Services 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 Philippines Inc. 3rd Floor, 719 GM Building, Real Street Corner Luke Wright Street, Dumaguete City 6200 Negros Oriental	TIN: 739-283- 935-000	Philippines	Backup, Patch Management, 24x7 monitoring.  Where specifically agreed: Sup- port in English
itm8 s.r.o Bucharova 1281/2, Stodůlky 158 00 Praha 5 Czech Republic	CVR-no.: 07628919	European Economic Area (EEA)	Service Desk and user support, Backup and backup controls, Patch Management, Operation and Maintenance of systems and infrastructure, Virus scanning and follow up on virus alarms, Implementations and configura- tions, Monitoring and handling of monitoring alarms, Documenta- tion of assets, procedures and controls, Handling of specific cus- tomer requests and specifically agreed consultancy tasks.
B4Restore A/S Aahave Parkvej 3 8260 Viby J	CVR-no.: 27719945	European Economic Area (EEA)	Backup and restore
Microsoft Ireland Opera- tions, Ltd. Att.: Data Protection One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	SE-no.: IE8256796U	Data is stored within the EU, but support can be provided from all over the world	Microsoft O365 and Azure  This is an independent Sub-data processor, where the Customer accepts that the Sub-data pro- cessor delivers its services on its own terms, cf. Appendix D (point D.4.)
Crayon A/S Tobaksvejen 2A 2860 Søborg	CVR-no.: 29832684	European Economic Area (EEA)	Administration of Microsoft CSP licenses
Heimdal Security A/S Vestergade 2A, 3 sal 1456 København K.	CVR-no.: 35802495	European Economic Area (EEA)	Heimdal Thor products

NAVN/ADRESSE	CVR	LOKATION FOR BEHANDLING	BESKRIVELSE AF BEHANDLING
Symantec MessageLabs Ltd 350 Brook Drive, Green Park GB-RG2 6UH Berkshire	SE-no.: 3834506	Worldwide	SYMC e-mail protect
Entrust Datacard Denmark A/S Park Allé 350D 2605 Brøndby	CVR-no.: 21780340	Worldwide	SMS Passcode - 2-factor validation
J2 Global Danmark A/S Spotorno Allé 12 2630 Taastrup	CVR-no.: 28117833	European Economic Area (EEA) and article 45 countries	Vipre Spamfilter, mailbackup, Vipre Securemail
Keepit A/S Per Henrik Lings Allé 4, 4 sal 2100 København Ø	CVR-no.: 30806883	European Economic Area (EEA)	Keepit Office 365 Backup
Panorama9 A/S Flæsketorvet 26 1711 København V.	CVR-no.: 33396880	European Economic Area (EEA)  But sub-processors may transfer to 3rd countries	Panorama9 monitoring
Vibe IT HB Firmagatan 4 S-213 76 Malmö	SE-no.: 5567736672	European Economic Area (EEA)	Service Desk 24/7 in Swedish
Curanet A/S Højvængen 4 8660 Skanderborg	CVR-no.: 29412006	European Economic Area (EEA)	Remote backup
Miracle 42 A/S Borupvang 2C, st 2750 Ballerup	CVR-no.: 40111751	European Economic Area (EEA)	Ad-hoc operational support regarding Oracle tasks
FastTrack Software ApS Niels Jernes Vej 10 9220 Aalborg	CVR-no.: 31938112	Within EU	Security Services
Flexfone A/S Danmarksvej 26 8660 Skanderborg	CVR-no.: 34042985	Telephony: Within EU  Teams Integration: USA, Canada, Israel, India, Malaysia, Mexico.  Foreign numbers:	Flexfone telephony system

NAVN/ADRESSE	CVR	LOKATION FOR BEHANDLING	BESKRIVELSE AF BEHANDLING
		USA, Hongkong, Belgium  Flexfone Test App: USA, Egypt	
XINK ApS Tuborg Boulevard 12, 3. 2900 Hellerup	CVR-no.: 32153283	Data is stored within the EU, but support can be provided from all over the world	Xink Branding and Xink Campaign
Rapid 7 120 Causeway Street Suite 400 Boston, MA 02114		European Economic Area (EEA)	Cyber Threat and Vulnerability Management Managed SIEM
Cira Apps Limited 2255 South Bascom Avenue Campbell, CA		European Economic Area (EEA)  Using Azure datacenters in Europe	CiraSync
F-Secure Danmark A/S Rued Langgaards Vej 8 2300 Copenhagen S	CVR-no.: 32559409	Inside and outside EU	Antivirus and vulnerability scan
Muninn ApS Sauntesvej 13 2820 Gentofte	CVR-no.: 37783110	European Economic Area (EEA)	Scan of network traffic
Data & More ApS Flæsketorvet 68 1711 København V	CVR-no.: 38185659	Within EU	Baseline GDPR Toolbox
CyberPilot ApS Fredens Torv 8 B 1. Sal 8000 Århus C	CVR-no.: 37435382	European Economic Area (EEA)  They use Amazon in Europe as a datacenter	System for Awareness Training and Phishing Test
Nasure A/S Rødovrevej 253C 2610 Rødovre	CVR-no.: 35472525	European Economic Area (EEA)	EDI-Portal for TK2
Improsec A/S Njalsgade 76, 4 2300 København S	CVR-no.: 37292451	European Economic Area (EEA)	Penetration test and maturity analysis

NAVN/ADRESSE	CVR	LOKATION FOR BEHANDLING	BESKRIVELSE AF BEHANDLING
Front-Safe A/S Spotorno Alle 12, 2 Høje Taastrup 2630 Taastrup	CVR-no.: 29631123	European Economic Area (EEA) and article 45 countries	Backup
Competella AB Fleminggatan 48 S-112 33 Stockholm	SE-no.: 5567815070	EU and Pakistan	Switchboard for Teams
CETA Cyber Defence ApS Lautruphøj 1-3 2750 Ballerup	CVR-no.: 40590366	European Economic Area (EEA)	DMARC Compliance
Asgot P/S Lundborgvej 18 8800 Viborg	CVR-no.: 42409847	European Economic Area (EEA)	Baseline Whistleblower - by Me'ning
Dahl Advokatpartnerselskab Lundborgvej 18 8800 Viborg	CVR-no.: 37310085	European Economic Area (EEA)	Baseline Whistleblower - by Me'ning IT Contingency Plan
Printix.net ApS Hørkær 20 2730 Herlev	CVR-no.: 36086416	European Economic Area (EEA) and UK. For e-mail notification services: U.S.A.	Printix Print Management
Omnicdocs Wilders Plads 15A 1403 Copenhagen K	CVR-no.: 35679529	Europæiske Økonomisk Samarbejdsområde EØS	Baseline Security
Uniqkey ApS Lyskær 8a, st. tv. 2730 Herlev	CVR-no.: 39004127	European Economic Area (EEA)	Password and Identity Manager

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 underdatabehandlere 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 Services. 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 Services, 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. 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 til at bruge databehandlerens kontor på Filippinerne (IT Relation Philippines Inc.) med behandlingsinstrukserne i C.1.1 Hosting og Drift og C.1.2 Service Desk.

Databehandlerens kontor på Filippinerne består af et professionelt og engageret leveranceteam, som medvirker til at levere den bedst mulige service til databehandlerens kunder. Teamet indgår i det samlede organisationsdiagram, som en afdeling i Managed Service, på samme måde som de danske afdelinger. Desuden er teamet under lokal dansk ledelse, for at sikre at den samme kvalitet opretholdes, som når ydelsen leveres fra Danmark. På den måde er IT Relation Philippines Inc. en naturlig del af leverancen indenfor de 2 tjenester "Hosting og drift" og "Service Desk". Med det filippinske kontor styrker databehandleren de samlede kompetencer og sikrer en bred bemanning på Service Desk og driftsydelser hele døgnet året rundt. IT Relation Philippines Inc. indgår ikke i leverancen af øvrige Services.

IT Relation Philippines Inc. er desuden fuldt integreret og arbejder ud fra samme sikkerhedsretningslinjer, politikker og procedurer som den danske organisation, ligesom de er inkluderet i databehandlerens ISO 27001-certificering og ISAE 3402-erklæring.

I forhold til databehandlerens filippinske kontor skal det bemærkes, at der aldrig foregår opbevaring på eller transmission af data til Filippinerne. Medarbejderne kan kun tilgå kunders systemer og behandle data gennem en Citrix-løsning i Danmark. Der transmitteres således kun skærbilleder i krypteret form til Filippinerne.

Med ovenstående opnår databehandleren derfor præcis samme sikkerhedsniveau, uanset om arbejdet udføres fra Filippinerne eller fra Danmark.

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 Services indeholder eller specifikke sager, den dataansvarlige igangsætter.

### C.1.3 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.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 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

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 Services 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. Derudover kan der udføres remote arbejde i overensstemmelse med databehandlerens politik for remote arbejde.

#### 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
IT Relation Philippines Inc. 3rd Floor, 719 GM Building, Real Street Corner Luke Wright Street, Dumaguete City 6200 Negros Oriental	TIN: 739-283- 935-000	Processing specified in C.1, C.1.1 and C.1.2	Yes Legal basis: SCC
Competella AB Fleminggatan 48 112 33 Stockholm Sverige	CVR-no.: 556781- 5070	Switchboard for Teams	Yes Legal basis: SCC  Uses subsidiary in Pakistan Uses Microsoft as subprocessor
Cira Apps Limited 2255 South Bascom Avenue Campbell, CA		Synchronizing contacts and calendars for smartphones	Yes Legal basis: SCC Uses Microsoft as subprocessor
Microsoft Ireland Operations, Ltd. South County Business Park Leopardstown	SE-no: IE8256796U	Microsoft O365 and Azure	Yes Legal basis: SCC
Crayon A/S Tobaksvejen 2A 2860 Søborg	CVR-no.: 29832684	Administration of Microsoft CSP licenses	Yes Legal basis: SCC
F-Secure A/S Rued Langgaards Vej 8 2300 Copenhagen S	CVR-no: 32559409	Antivirus and vulnerability scan	Yes Legal basis: SCC
FastTrack Software ApS Niels Jernes Vej 10 9220 Aalborg	CVR-no: 31938112	Security Services	Yes Legal basis: SCC  Uses Azure

NAVN	CVR	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND
Flexfone A/S Danmarksvej 26 8660 Skanderborg	CVR-no: 34042985	Teams integration and foreign numbers for Flexfone	Yes Legal basis: SCC
Heimdahl Security A/S Vester Farimagsgade 1, 3. 1606 København V	CVR-no: 35472525	Security Services	Yes Legal basis: SCC Uses Microsoft & Amazon as subprocessors
Panorama9 ApS Flæsketorvet 28, 1. 1711 København V	CVR-no: 33396880	Panorama9 monitoring	Yes Legal basis: SCC (not confirmed)  Uses Google, ConnectWise, Secure By Design, Intercom
Rapid 7 120 Causeway Street Suite 400 Boston, MA 02114		Cyber Threat and Vulnerability Management Managed SIEM	Yes Legal basis: SCC (not confirmed)  Uses Amazon as subprocessor
Entrust Datacard Denmark A/S Park Allé 350D 2605 Brøndby	CVR-no.: 21780340	SMS Passcode - 2-factor validation	Yes Legal basis: SCC  Uses Amazon
Wehowsky.com ApS Sauntesvej 13 2820 Gentofte	CVR-no.: 37783110	Scan of network traffic	Yes Legal basis: SCC  Uses Amazon
Printix.net ApS Hørkær 20 2730 Herlev	CVR-no: 36086416	Printix Print Management - cloud based	Yes Legal basis: SCC  Uses Microsoft, Amazon, Mailchimp, Zendesk as subprocessors
CyberPilot ApS Fredens Torv 8 B, 1. sal 8000 Århus C	CVR-no: 37435382	Awareness Training	Yes Legal basis: SCC Awareness Training via subprocessor Phishing Test directly  Uses Amazon as subprocessor

NAVN	CVR	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND
J2 Global Danmark A/S Spotorno Allé 12 2630 Taastrup	CVR-no.: 28117833	Vipre Spamfilter, mailbackup, Vipre Securemail	Yes Legal basis: SCC  Uses Amazon as subprocessor
XINK ApS Tuborg Boulevard 12, 3. 2900 Hellerup	CVR-no.: 32153283	Xink Branding and Xink Campaign	Yes Legal basis: SCC  Uses Amazon as subprocessor

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

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 <https://legal.itm8.com> 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).
- Nyeste version af databehandlerens ISAE 3000-erklæring (publiceres hvert år i februar måned).
- Beskrivelse af fysisk og organisatorisk sikkerhed hos databehandleren.
- IT Sikkerhedspolitik.
- Beskrivelse af beredskab 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 anvendes nedenstående fremgangsmåde.

Procedure og rapportering for skriftligt tilsyn eller fysisk inspektion:

- Den dataansvarlige sender deres tilsynsskema til databehandleren via e-mail til [compliance@itm8.com](mailto:compliance@itm8.com) 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 fremsender eventuelle observationer fra tilsynet til [compliance@tim8.com](mailto:compliance@tim8.com).
- Databehandleren gennemgår og kommenterer på den dataansvarliges eventuelle observationer (kan gentages flere gange).
- Den dataansvarlige udfører sin endelige konklusion på tilsynet og fremsender rapporten til databehandleren.
- 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 nedenstående supplerende vilkår.

Bestemmelserne i denne aftale har forrang i forhold til eventuel tilsvarende regulering i Serviceaftaler mellem parterne vedrørende den del af databehandlerens aktiviteter og ansvar der knytter sig til databehandlingen, mens udførelsen af alle andre aktiviteter vedrørende leveringen af aftalte Services er underlagt de øvrige dele af Serviceaftalen.

Serviceaftalens øvrige vilkår, herunder ansvarsbegrænsninger m.v., er også gældende for databehandlerens opfyldelse af denne aftale.

I tilfælde af uoverensstemmelse mellem Bestemmelserne og de i dette bilag D fastsatte vilkår skal bilag D have forrang, og såfremt Serviceaftalen i øvrigt indeholder vilkår om databehandlerens behandlingsaktiviteter, vil bilag D ligeledes 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 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 Services og bilag C.2 anførte, dog under forudsætning af at sådanne alternative sikkerhedsforanstaltninger samlet set sikrer et sikkerhedsniveau på niveau med de foreskrevne sikkerhedsforanstaltninger.

### D.4 Anvendelse af Tredjepartsydelse og Public Cloud Udbydere

Uanset Bestemmelsernes punkt 7 er det aftalt, at dersom databehandleren anvender

- (a) Tredjepartsydelse, eksempelvis producenter af standardprogrammel, hardwareleverandører og øvrige leverandører af "standardydelse" såsom strøm, WAN, LAN og lignende, der ikke bidrager specifikt til Aftalens opfyldelse, men som anvendes af databehandleren som understøttende services til en flæthed af kunder, uanset at denne måtte være integreret i Services eller stillet til rådighed for dataansvarlig som en særskilt Service, eller
- (b) Public Cloud Udbydere således som disse er oplyst i en Serviceaftale (samlet kaldet "Uafhængige Underdatabehandlere"),

har databehandleren ikke ansvaret for disse Uafhængige Underdatabehandlers eventuelle behandlingsaktiviteter.

Den Uafhængige Underdatabehandlerens egne vilkår kan findes på <https://legal.itm8.com>, idet det er den dataansvarliges eget ansvar at sikre sig, at disse vilkår på tilfredsstillende vis opfylder krav til den Uafhængige Underda-

tabehandlers behandlingsaktiviteter. Den dataansvarlige er gjort bekendt med, at disse vilkår løbende kan ændres af den enkelte Uafhængige Underdatabehandler, og den dataansvarlige skal således kontinuerligt sikre sig, at disse opfylder kravene til behandlingsaktiviteterne.

Ved Bestemmelserne giver den dataansvarlige sin accept af og instruks til, at sådanne konkrete behandlingsaktiviteter sker på den Uafhængige 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.

Sletningspligten omfatter ikke (i) kopier af elektronisk udvekslede personoplysninger opbevaret som led i automatiserede backup funktioner, forudsat at adgangen hertil er begrænset til IT- eller compliancepersonale samt at alle sådanne oplysninger behandles i overensstemmelse med Aftalens bestemmelser, og (ii) personoplysninger som skal opbevares af databehandleren ifølge ufravigelig lovgivning.

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 - generelt

Medmindre databehandleren som led i aftalte Services og indenfor det faste vederlag for sådanne Services har påtaget sig at opfylde bestemmelserne, vil Databehandleren være berettiget til vederlag for bistand efter de i Bestemmelsernes, herunder punkt 9, aftalte bistandsydelse.

Vederlaget opgøres på baggrund af den forbrugte arbejdstid og de aftalte timesatser i Serviceaftale vedrørende levering af Services, og hvor der ikke er aftalt timesatser heri, da efter databehandlerens gældende timesatser.

Eventuelt afholdte eksterne omkostninger, herunder også omkostninger der skal afholdes af databehandleren for underdatabehandleres bistand, faktureres den dataansvarlige.

### D.6.2 Implementering af øvrige sikkerhedsforanstaltninger

Såfremt den dataansvarliges instruks m.v., samt databehandlerens løbende vurderinger i øvrigt, medfører skærpede krav til de i en Serviceaftale indeholdte krav til sikkerhedsforanstaltninger vedrørende leveringen af Services eller til bilag C, vil databehandleren loyalt søge at imødekomme sådanne krav såfremt dette teknisk muligt og foreneligt med opfyldelsen af øvrige krav til de berørte Services.

Databehandleren er berettiget til vederlag og omkostningsdækning efter samme principper som ovenfor.

#### 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 Serviceaftale vedrørende levering af tjenester, og hvor der ikke er aftalt timesatser heri, da efter databehandlerens gældende timesatser.

Eventuelt afholdte eksterne omkostninger, herunder også omkostninger der skal afholdes af databehandleren for underdatabehandleres bistand, faktureres den dataansvarlige.

### **D.7 Ansvar og misligholdelse**

En eventuel misligholdelse af Bestemmelserne reguleres og behandles i overensstemmelse med parternes Serviceaftale vedrørende levering af Services, med følgende tillæg;

- a) 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 Serviceaftale vedrørende levering af Services. Parterne har hermed aftalemæssigt fraveget databeskyttelsesforordningens artikel 82, stk. 5 og erstatningsansvarsloven § 26.
- b) Uanset databeskyttelsesforordningen art 82, stk. 5 kan databehandleren, dersom denne har udredt erstatningsbeløb til en skadelidt, der ikke svarer til fuld erstatning, gøre regres efter princippet i art. 82, stk. 5.
- c) 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.
- d) 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.
- e) Databehandlerens samlede erstatningsansvar ved misligholdelse af Bestemmelserne er omfattet af den beløbsmæssige begrænsning (og indregnes ved erstatningsmaksimeringen) der eventuelt følger af parternes Serviceaftale. Ansvar (inklusive sådan erstatning eller anden økonomisk kompensation der måtte være indrømmet den dataansvarlige under Serviceaftalen) begrænses til et beløb lavere end 150% af det beløb databehandleren har modtaget i de foregående 12 måneder forud for den skadegørende handling. Såfremt en 12 måneders periode ikke er gået, beregnes ansvarsbegrænsningen som gennemsnittet af modtagne beløb i de måneder, som er gået, ganget med 12.
- f) Databehandlerens erstatningsansvar ved misligholdelse af Bestemmelserne omfatter ikke indirekte tab, herunder driftstab, følgeskader eller andet indirekte tab.
- g) Databehandleren er ikke ansvarlig for misligholdelse af Bestemmelserne forårsaget af computervirus, cyberkriminalitet eller andre former for tredjemands uberettigede indgreb i den dataansvarlige eller databehandlerens IT-systemer, medmindre tabet er direkte relateret til manglende opfyldelse af aftalte krav til sikkerhed i parternes Serviceaftale.

## D.8 Fravigelser

Parterne har aftalt følgende fravigelser til Bestemmelserne samt nærværende bilag:

BESTEMMEL- SERNE/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>