Indledning til underdatabehandleraftale

Denne underdatabehandleraftale er udarbejdet efter Datatilsynets Standardkontraktsbestemmelser.

Underdatabehandleraftalen fastsætter de rettigheder og forpligtelser, der finder anvendelse, når det overlades til en underdatabehandler at foretage behandling af personoplysninger på vegne af en databehandler.

Underdatabehandleraftalen er udformet med henblik på parternes efterlevelse af art. 28 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), som stiller specifikke krav til indholdet af en databehandleraftale.

Underdatabehandlerens behandling af personoplysninger for databehandleren sker med henblik på opfyldelse af parternes aftale om tjenester fra underdatabehandleren til databehandleren, og som databehandleren anvender i sine leverancer ud mod kunder. Underdatabehandleren optræder dermed som en anden databehandler (underdatabehandler) i overensstemmelse med databeskyttelsesforordningen art. 28(4).

Underdatabehandleraftalen har til formål at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt i sin aftale med den dataansvarlige.

Alle anvendte begreber i denne underdatabehandleraftale skal forstås i overensstemmelse med databeskyttelsesforordningen.

Parterne er enige om, at hvor underdatabehandleraftalen referer til ”den dataansvarlige” skal det forstås som ”databehandleren” og hvor underdatabehandleraftalen refererer til ”databehandleren” skal det forstås som ”underdatabehandleren”.

Underdatabehandleraftale for Centera Security

Standardkontraktsbestemmelser

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

mellem

itm8 Holding A/S
CVR 37621285
Dalgas Plads 7B. 1. sal
7400 Herning
Danmark

herefter ”den dataansvarlige”

og

Centera Security
- en del af CETA Cyber Defence ApS
CVR 40590366
Lejrvej 15
3500 Værløse
Danmark

herefter ”databehandleren”

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

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

1. Indhold

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 **Centera IT-sikkerhedsløsninger** 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 af 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[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

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

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 specifik skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 60 dage inden anvendelsen af den pågældende underdatabehandler. 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 på-

lagt 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 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.

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

9. Bistand til den dataansvarlige

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

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

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. indsigtsretten
d. retten til berigtigelse
e. retten til sletning ("retten til at blive glemt")
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, **Datatilsynet**, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

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

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

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest **24 timer** efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

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

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

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 dataansvarlig, at oplysningerne er slettet,** 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 nærmeret 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.

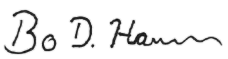
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

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 skriftlig varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

Navn	Bo Duholm Hansen
Stilling	Compliance Manager
E-mail	bdh@itm8.com
Underskrift	

   På vegne af databehandleren

Navn	Troels Lind
Stilling	Administrerende Direktør
Telefonnummer	+45 31 93 10 60
E-mail	tli@cetacyberdefence.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.

Primær Kontakt hos den Dataansvarlige:

Navn	Compliance & Security
Telefonnummer	+45 69 16 00 04
E-mail	compliance@itm8.com

Primær Kontakt hos Databehandleren:

Navn	Lennart Friberg
Stilling	Teknisk Chef
Telefonnummer	+45 31 17 81 80
E-mail	contact@centerasecurity.com

Bilag A Oplysninger om behandlingen

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

Centera email Defence
Den dataansvarlige kan anvende systemet Centera email Defence, som ejes og administreres af databehandleren, til at beskytte den dataansvarliges virksomhed imod uønskede email, derunder email indeholdende spam, phishing og skadelig kode.

Centera DMARC Compliance
Den dataansvarlige kan anvende systemet Centera DMARC Compliance, som ejes og administreres af databehandleren, til at beskytte den dataansvarliges virksomhed imod e-mail misbrug af deres domænenavne, ved at indsamle rapporter om e-mails som ikke opfylder DMARC validering fra internettet. Disse DMARC rapporter er simple data i XML standard, som modtages fra større udbydere af e-mail, som Google, facebook, yahoo mfl. Centera DMARC Compliance opsamler disse rapporter og gør dem lette at forstår og reagere på for den dataansvarlige

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

Centera email Defence
Databehandlerens system Centera email Defence scanner den dataansvarliges email, hvor email der indeholder skadeligt indhold blokeres.

Centera DMARC Compliance
Databehandlerens system Centera DMARC Compliance indsamler DMARC RUA rapporter for e-mails, som benytter de af den dataansvarlige angivende domæner.

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

Navn, e-mailadresse, telefonnummer, adresse og andre personoplysninger der kan optræde i emails sendt til- eller fra databehandleren.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Personer, som kommunikerer via email med den dataansvarlige.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

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

Såfremt Databehandleren ønsker at gøre brug af underdatabehandlere, skal dette forhold godkendes af den Dataansvarlige med et varsel på mindst 90 dage.

C.1. Behandlingens genstand/instruks
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Centera email Defence
Databehandlerens system Centera email Defence scanner den dataansvarliges email, hvor email der indeholder skadeligt eller uønsket indhold blokeres.

Centera DMARC Compliance
Databehandlerens system Centera DMARC Compliance indsamler fra Internettet DMARC RUA rapporter for e-mails, som benytter de af den dataansvarlige angivende domæner.

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle:

Der er tale om databehandling af emails, hvori man kan forvente personfølsomme oplysninger. Under hensyntagen til dette er der etableret et højt sikkerhedsniveau hos databehandleren.

Databehandleren anvender en risikobaseret tilgang til IT-sikkerhed og beskyttelse af de personoplysninger, vi behandler om vores kunder og vores kunders medarbejdere. Databehandleren har fastsat nedenstående tekniske og organisatoriske sikkerhedsforanstaltninger for at imødegå de risici, der er forbundet med behandling af personoplysninger i CETA Cyber Defence, som er Databehandler for den Dataansvarlige. Databehandleren vil altid som minimum iværksætte de nedenstående sikkerhedsforanstaltninger, men kan til enhver tid opgradere sikkerhedsniveauet og de dertilhørende foranstaltninger i forbindelse med en udvikling i risikoscenariet.

Fysisk sikkerhed
Databehandleren har etableret fysisk adgangssikkerhed, så kun autoriserede personer kan opnå adgang til lokaler, hvor der opbevares og behandles personoplysninger. Der foretages videoovervågning af Databehandlerens faciliteter. Der er implementeret alarmsystemer i Databehandlerens lokaler og der er kun adgang med nøgle eller adgangskort og dertilhørende kode.

Logning
Al netværkstrafik og alle serverlogs bliver overvåget og logget. Følgende logges i systemer, databaser og netværk:
• Alle adgangsforsøg,
• Alle søgninger,
• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
• Sikkerhedshændelser, herunder (i) deaktivering af logning, (ii) ændringer i systemrettigheder og (iii) mislykkede forsøg på log-on.

Databehandleren opererer ikke med fælles log-in, så det vil altid være muligt at identificere den medarbejder, der har foretaget en aktivitet. De relevante logfiler lagres og beskyttes mod manipulation og tekniske fejl. Logfilerne gennemgås løbende for at sikre normal drift og for at undersøge utilsigtede hændelser eller incidents.

Antivirus og firewalls
Al ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem en sikret firewall med en restriktiv protokol. 14 Der er etableret port- og IP-adresse filtrering

for at sikre begrænset adgang til porte og for specifikke IP-adresser. Der er installeret antivirus software og Intrusion Prevention System (IPS) på alle systemer og databaser, der anvendes til behandling af personoplysninger, for at beskytte imod fjendtlige angreb. Den anvendte antivirus software opdateres regelmæssigt. Beskyttelse mod XSS og SQL-injektioner er implementeret i alle tjenester. Databehandlerens interne netværk kan kun tilgås af dertil autoriserede personer.

Pseudonymisering og Kryptering af Personoplsyninger
Der anvendes effektiv og stærk kryptering baseret på en anerkendt algoritme ved transmission af personoplysninger via internettet og/eller e-mail. Kundens UserID (brugernavn) og password krypteres ved brug af sikre algoritmer.

Back-up og tilgængelighed
De tekniske foranstaltninger og Databehandlerens systemer testes løbende ved sårbarhedsscanninger og penetrationstests. Alle ændringer til systemer, databaser og netværk følger fastlagte Change Management procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches. Der foretages systemovervågning af alle systemer, hvori der behandles personoplysninger. Datamiljøet overvåges for sårbarheder og eventuelle identificerede problemer afhjælpes. Der foretages back-up, så det sikres at alle systemer og data, herunder personoplysninger, kan genoprettes, hvis de går tabt eller ændres.

Autorisation, adgangsbegrænsninger og sikkerhed
Det er kun medarbejdere med et arbejdsbetinget behov, der får adgang til personoplysninger. Alle vurderinger af en medarbejders arbejdsbetingede behov foretages ud fra en "need-to-have" tilgang, for at sikre overholdelse af princippet om dataminimering. Medarbejdernes adgang revurderes regelmæssigt. Der gennemføres løbende awareness-træning af medarbejdere i relation til IT-sikkerhed og behandlingssikkerhed for personoplysninger. Alle medarbejdere informeres om den af ledelsen godkendte skriftlige informationssikkerhedspolitik. Der foretages screening af alle nye medarbejdere. Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver nye medarbejdere introduceret til informationssikkerhedspolitikken og procedurer for behandling af de personoplysninger, der ligger indenfor medarbejderens arbejdsområde. Der er fastsat procedurer for at sikre, at fratrædende medarbejdere bliver frataget deres tildelte brugerrettigheder. 15 Databehandleren har implementeret en passwordpolitik, der er med til at sikre at medarbejderes adgangskoder ikke kommer uvedkommende til hænde, samt at der kun godkendes adgangskoder, der er tilstrækkeligt komplicerede og at adgangskoder skiftes regelmæssigt. Der er etableret beskyttelse af flytbare enheder. Medarbejderes laptop computere er bl.a. beskyttet med anerkendt kryptering og passwords på harddiskdrev-niveau. Der anvendes desuden VPN-forbindelse og to-faktor autentificering ved fjernadgang. Eksterne personer, der færdes på Databehandlerens lokationer, hvor der potentielt er adgang personoplysninger, informeres om Databehandlerens sikkerhedsregler og underskriver en fortrolighedserklæring.

Kontroller
Databehandleren udfører intern revision og kontrol af de fastsatte tekniske og organisatoriske sikkerhedsforanstaltninger baseret på kontrollerne i den anerkendte
ISAE 3000 standard.

C.3 Bistand til den dataansvarlige
Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

C.4 Opbevaringsperiode/sletterutine
Personoplysningerne opbevares i op til 90 dage hvorefter de slettes hos databehandleren.

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 Lokalitet for behandling

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

Behandling af personoplysninger sker på en eller flere af følgende adresser:

- Databehandlerens adresser.
- Datacentre databehandleren benytter.
- Underdatabehandlere, samt 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
Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

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

Den dataansvarlige kan uden omkostninger og maksimalt en gang årligt sende et tilsynsspørgeskema til databehandleren, så den dataansvarlige kan demonstrere at der er ført tilsyn med databehandleren og sikre, at databehandleren overholder nærværende aftale.

Den dataansvarlige eller en repræsentant for den dataansvarlige har mulighed for at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, i det omfang den dataansvarlige finder det nød

vendigt."

Alle eventuelle omkostninger for inspektioner og ekstraordinær dokumentation hos Databehandleren, afregnes den Dataansvarlige som angivet under Bilag D - Parternes regulering af andre forhold.

Bilag D Parternes regulering af andre forhold

D.1. Aftale om vederlæggelse i forbindelse med Databehandlerens bistand til den Dataansvarlige.

Al bistand fra databehandleren, til opgaver der stilles af dataansvarlige og som måtte ligge udenfor den dataansvarliges lovbestemte rettigheder i relation til Databeskyttelsesforordningen, afregnes til en takst af DKK 1.490,00 pr time for medgået tid indenfor normal kontortid og DKK 2.350,00 pr time udenfor normal kontortid.