
Databehandleraftale

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

mellem

[NAVN]

CVR [CVR-NR]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

herefter "den dataansvarlige"

og

MedCom

CVR 26 91 99 91

Forskerparken 10B

5230 Odense M

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

Indholdsfortegnelse

2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	5
7. Anvendelse af underdatabehandlere	5
8. Overførsel til tredjelande eller internationale organisationer	6
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	10
15. Kontaktpersoner hos den dataansvarlige og databehandleren	11
Bilag A	Oplysninger om behandlingen12
Bilag B	Underdatabehandlere14
Bilag C	Instruks vedrørende behandling af personoplysninger15
Bilag D	Parternes regulering af andre forhold vedrørende databehandleraftalen25
Bilag E	Databehandlerkæden26

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 det Kommunale Identitetsslørings-system (KIS) 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. MedCom bliver en del af Digital Sundhed Danmark, som etableres i medfør af lov nr. 1758 af 29. december 2025 om Digital Sundhed Danmark.
Når MedComs rettigheder og pligter i medfør af loven overføres til Digital Sundhed Danmark, bliver Digital Sundhed Danmark uden videre aftalepart på nærværende aftale. Dette vil ikke herudover medføre indholdsmæssige ændringer til aftalen. Tidspunktet for overgangen fra MedCom til Digital Sundhed Danmark vil fremgå af en bekendtgørelse, som Indenrigs- og Sundhedsministeriet udsteder i medfør af lovens § 29
6. Der hører fem bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
7. 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.
8. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
9. 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.
10. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
11. Bilag E indeholder en beskrivelse af databehandlerkæden
12. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

-
13. 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 medlemsstaternes¹ nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

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

5. Fortrolighed

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

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

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 60 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
 4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

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 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 at 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, hvorved databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

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

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

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:
 - a. Arkivloven samt regler fastsat i medfør heraf kan medføre pligt til bevaring, arkivering eller aflevering af materiale, herunder personoplysninger. Hvor den dataansvarlige er underlagt arkivloven, vil databehandleren, i det omfang det er rimeligt muligt, bistå den dataansvarlige med at opfylde sine forpligtelser i henhold hertil ved efter anmodning at levere datauddrag i et af Rigsarkivet anvendt og struktureret format.
3. Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

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 aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

Navn: [NAVN]
Stilling: [STILLING]
Telefonnummer: [TELEFONNUMMER]
E-mail: [E-MAIL]

.....
Dato / Underskrift:

På vegne af databehandleren

Navn: Lars Hulbæk
Stilling: Direktør
Telefonnummer: 4036 8615
E-mail: lh@medcom.dk

.....
Dato / 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.

Kontaktperson hos den dataansvarlige:

Navn: [NAVN]
Stilling: [STILLING]
Telefonnummer: [TELEFONNUMMER]
E-mail: [E-MAIL]

Kontakt hos den dataansvarlige ved sikkerhedsbrud jf. afsnit 10:

E-mail: [E-MAIL]

Kontaktperson hos databehandleren:

Navn: Lars Hulbæk
Stilling: Direktør
Telefonnummer: 4036 8615
E-mail: lh@medcom.dk

Bilag A Oplysninger om behandlingen

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

Systemet understøtter visning og identitetssløring af sundhedsansatte i overensstemmelse med § 42 c i Sundhedsloven og regler fastsat i medfør heraf, herunder bekendtgørelse om logning og visning af logoplysninger i elektroniske sundhedssystemer.

Databehandleren er kontraktholder og fællesoffentlig systemforvalter for KIS

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

Databehandlingen består i at modtage og opbevare personoplysninger samt indsende data til sløring til den nationale sløringskomponent IDSAS.

Databehandleren hoster, drifter, vedligeholder, overvåger og supporterer KIS.

Databehandleren modtager alarmer om anomalier i overvågningen af KIS.

Databehandleren bistår Underdatabehandleren med at løse supporthenvendelser for KIS.

Som fællesoffentlig systemforvalter leverandørstyrer Databehandleren i forbindelse med leveringen af KIS til den Dataansvarlige.

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

I systemet behandles almindelige personoplysninger, herunder navn og fødselsdato, samt særlige kategorier af personoplysninger, herunder helbredsoplysninger. Der behandles desuden CPR-numre i henhold til databeskyttelseslovens § 11 samt oplysninger om strafbare forhold i henhold til databeskyttelseslovens § 10.

PERSON-OPLYSNINGER	Borger	Sundhedspersonale
Almindelige personoplysninger: (art. 6)	☒ Navn ☐ Adresse ☐ E-mail ☐ Telefonnummer ☒ Fødselsdato ☐ Medarbejder ID ☐ Billeder ☐ Andre almindelige personoplysninger: [beskriv hvilke]	☒ Navn ☐ Adresse ☐ E-mail ☐ Telefonnummer ☐ Fødselsdato ☐ Medarbejder ID ☐ Billeder ☐ Andre almindelige personoplysninger: [beskriv hvilke]
Følsomme personoplysninger: (art. 9)	☐ Race eller etnisk oprindelse ☐ Politisk, religiøs eller filosofisk overbevisning ☐ Fagforeningsmæssige tilhørsforhold ☐ Genetisk data	☐ Race eller etnisk oprindelse ☐ Politisk, religiøs eller filosofisk overbevisning ☐ Fagforeningsmæssige tilhørsforhold ☐ Genetisk data

	☐ Biometrisk data ☒ Helbredsoplysninger ☐ Seksuelle forhold eller orientering	☐ Biometrisk data ☐ Helbredsoplysninger ☐ Seksuelle forhold eller orientering
Straffedomme og lovovertrædelser (§10)	☒ Straffedomme og lovovertrædelser	☐ Straffedomme og lovovertrædelser
CPR-nummer (§11)	☒ CPR-nummer	☐ CPR-nummer
Andre fortrolige personoplysninger	☐ Væsentlige sociale forhold ☐ Væsentlige økonomiske forhold ☐ Bankoplysninger ☐ Ansøgninger og CV ☐ Andre fortrolige oplysninger: [beskriv hvilke]	☐ Væsentlige sociale forhold ☐ Væsentlige økonomiske forhold ☐ Bankoplysninger ☐ Ansøgninger og CV ☐ Andre fortrolige oplysninger: [beskriv hvilke]

A.4. Behandlingen omfatter følgende kategorier af registrerede

I KIS behandles følgende kategorier af registrerede: Sundhedspersonale og Borger.

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 kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne ophører.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR/ VIRKSOMHEDS ID	ADRESSE OG LAND	BESKRIVELSE AF BEHANDLING
MultiMed A/S	19 40 37 42	Storhaven 12 7100 Vejle, Danmark	Drift, vedligehold, hosting, support og backup, samt udvikling

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden at følge den aftalte procedure for udskiftning af underdatabehandlere – 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 indsigelse ved skift af underdatabehandlere

Databehandleren skal orientere den Dataansvarlige i tilfælde af, at der vælges en ny Underdatabehandler. Orienteringen skal ske senest 3 måneder inden den nye Underdatabehandler tages i anvendelse.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

Databehandleren behandler personoplysninger udelukkende til hosting, drift, support, vedligehold af it-løsningen, sikkerhed samt sletning/anonymisering af data, efter dokumenteret instruks fra den dataansvarlige.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle behandlingens omfang og karakter:

Behandlingen omfatter følgende antal registrerede:

- ☐ Under 1000 (1 point)
- ☒ 1000 - 10.000 (2 point)
- ☐ Over 10.000 (3 point)

Behandlingen omfatter behandling af følgende type personoplysninger:

- ☒ Almindelige personoplysninger, art. 6 (0 point)
- ☒ Særlige kategorier af personoplysninger / Følsomme personoplysninger, art. 9 (3 point)
- ☒ Andre beskyttelsesværdige / fortrolige personoplysninger, (F.eks. oplysninger om private forhold omfattet af straffelovens § 152, jf. forvaltningslovens § 27, personnumre, jf. databeskyttelseslovens § 11, samt oplysninger om strafbare forhold, jf. databeskyttelseslovens § 10) (2 point)
- ☐ Særlige behandlinger (F.eks. Overvågning, kortlægning af adfærd, profilering, automatiske behandlinger) (2 point)

Sikkerhedsniveau:

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

Aftalt sikkerhedsniveau
Grundlæggende
Betragteligt
Højt

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

Databehandleren skal understøtte den Dataansvarlige i dennes arbejde med at dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau og gennemføre de foranstaltninger, der er nødvendige for at imødegå identificerede risici.

På baggrund af det etablerede sikkerhedsniveau implementeres procedurer for revisioner i overensstemmelse med punkt C.7 og C.8.

Der henvises i øvrigt til [Datatilsynets vejledning om tilsyn](#)

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

C.2.1 Krav til pseudonymisering og kryptering af personoplysninger

Krav til pseudonymisering af personoplysninger

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

Krav til kryptering af personoplysninger

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

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

1. Databehandler foretager mindst én gang årligt en risikovurdering for hver af de behandlingssystemer og tjenester, hvori den Dataansvarliges personoplysninger behandles. Databehandler foretager loyalt og professionelt mitigerende foranstaltninger baseret på risikovurderingens resultater.
2. Databehandler foretager løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet.

Databehandler sikrer endvidere, at:

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

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

Databehandler sikrer, at

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

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

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

Databehandler har til enhver tid tidssvarende procedurer for gennemførelse af:

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

C.2.5. Krav vedrørende adgang til oplysninger via internettet

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

C.2.6. Krav vedrørende beskyttelse af oplysninger under transmission

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

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

Der anvendes altid kryptering af personoplysninger ved enhver transmission af fortrolige og følsomme personoplysninger via eksterne kommunikationsforbindelser.

C.2.7. Krav vedrørende beskyttelse af oplysninger under opbevaring

Under opbevaring af personoplysninger skal der etableres tilstrækkelige sikkerhedsforanstaltninger under hensyntagen til karakteren af de behandlede personoplysninger, og risikoen for de registreredes rettigheder.

Databehandler sikrer, at personoplysningerne er krypteret i relevant omfang under opbevaring. Krypteringen skal løbende holdes opdateret, og følge de til enhver tid værende anerkendt og gældende branchestandarder.

C.2.8. Krav vedrørende beskyttelse af oplysninger i brug (in use/in motion)

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

Databehandleren sikrer, at personoplysninger er krypteret i relevant omfang under brug. Krypteringen skal holdes opdateret, og følge de til enhver tid værende anerkendt og gældende branchestandarder.

C.2.9. Krav vedrørende fysisk sikring af lokaliteter, hvor der behandles oplysninger

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

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

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

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

C.2.10. Krav vedrørende anvendelse af hjemme-/fjernarbejdspladser

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

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

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

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

C.2.11. Krav vedrørende logning

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

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

Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

Databehandleren fører løbende kontrol med, at loggen indeholder de nødvendige oplysninger, som fremgår af disse bestemmelser.

Databehandleren skal ved mistanke om misbrug eller brud på persondatasikkerheden vederlagsfrit udlevere en log over brugeraktivitet. Databehandleren skal sikre, at loggen er forståelig og indeholder de relevante aktiviteter.

C.2.12. Øvrige foranstaltninger

Opdateringer og ændringer

Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.

Awareness / kendskab til informationssikkerhed

Ansatte og eventuelle samarbejdspartnere, som har adgang til personoplysninger omfattet af disse Bestemmelser, skal gennemgå regelmæssig uddannelse vedrørende behandling af

personoplysninger, som sikrer et vedvarende kendskab til databeskyttelsesreglerne, samt procedurer for behandlingen af personoplysninger

Mobile lagringsmedier:

Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares med tilstrækkelig stærk kryptering under opsyn eller under lås, når de ikke benyttes.

Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.

Der skal føres en fortegnelse over, hvilke mobile lagringsmedier der benyttes i forbindelse med databehandlingen.

Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af mobile lagringsmedier.

Reparation, service og kassation af udstyr:

I forbindelse med reparation og service af udstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov.

Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller renses, så der sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal opbevares i den periode, databehandlingen foregår og forevises, på den Dataansvarliges anmodning.

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:

Underretning af den dataansvarlige om anmodninger fra de registrerede

Databehandleren skal uden unødigt forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes databehandlere fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren skal på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

Bistand ved sikkerhedsbrud, herunder underretning af den dataansvarlige om sikkerhedsbrud

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

Bistand i forbindelse med risikovurderinger og konsekvensanalyser

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

Sikring af tekniske og organisatoriske foranstaltninger

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

C.4 Opbevaringsperiode/sletterutine

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

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

Det er aftalt, at der som udgangspunkt skal ske sletning af personoplysninger, som er ældre end: 5 år.

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:

Virksomhedens navn og adresse	CVR eller andet virksomheds ID	Lokalitet for behandling	Eventuelt overførselsgrundlag
MultiMED Storhaven 12 7100 Vejle	19 40 37 42	Storhaven 12 7100 Vejle	

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.

Instruks og garanti, såfremt der ikke må ske overførsel og behandling udenfor EU/EØS
Databehandleren må ikke indenfor rammerne af disse Bestemmelser overføre personoplysninger til et land udenfor EU/EØS.

Alle data, herunder personoplysninger, behandles og opbevares indenfor EU, og må ikke direkte eller indirekte helt eller delvist tilgås fra lande udenfor EU/EØS.

Databehandleren indestår for, at alle data, herunder personoplysninger, som Databehandleren via alle sine underdatabehandlere behandler på vegne af den Dataansvarlige i henhold til disse Bestemmelser ikke i nogen tilfælde, hverken af tekniske eller kommercielle grunde overføres til og behandles i tredjelande.

Databehandleren garanterer, at personoplysninger ikke overføres til tredjelande i forbindelse med brug af Databehandlerens tjeneste eller levering af Databehandlerens ydelser omfattet af denne Databehandleraftale eller underdatabehandlerens ydelser, uanset om sådan overførsel sker af tekniske eller kommercielle grunde.

På den Dataansvarliges anmodning skal Databehandleren udlevere dokumentation af såvel tjenestens overførelsesmuligheder samt de tekniske og procesmæssige foranstaltninger, som Databehandleren har fastsat for at undgå utilsigtede overførsler af personoplysninger til lande udenfor EU/EØS.

Vilkår vedrørende myndighedsanmodninger om udlevering af personoplysninger

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

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

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

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

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

Revisionserklæringen skal være af typen ISAE 3000 GDPR type 2 med høj grad af sikkerhed udarbejdet efter opbygningen i FSR standarden, dækkende kravene beskrevet i denne databehandleraftale. Revisionserklæringen fremsendes til den dataansvarlige, eller en uafhængig revisor bemyndiget af den dataansvarlige.

Den dataansvarlige kan fravige den aftalte tilsynsform, såfremt den dataansvarlige vurderer, at databehandleren på anden vis vil kunne dokumentere overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag.

Baseret på resultaterne af tilsynet er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige, eller en repræsentant bemyndiget af den dataansvarlige, har endvidere ret til at foretage inspektioner af databehandlerens fysiske faciliteter, hvor der behandles personoplysninger, samt modtage de nødvendige informationer til gennemførelse af tilsyn med den databehandlerens efterlevelse af kravene i disse Bestemmelser samt gældende databeskyttelsesret.

Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til den kompetente tilsynsmyndighed efter anmodning herom fra myndigheden.

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

Databehandleren træffer som udgangspunkt valg om, hvordan revision af underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og underdatabehandleraftalen foretages, herunder hvilken type af revisionserklæring og/eller inspektionsrapport, der indhentes. Typen og omfanget af revisionen skal afspejle karakteren af den behandling af personoplysninger, som underdatabehandleren foretager. Revisionserklæringer og/eller inspektionsrapporter fremsendes minimum 1 gang årligt til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af revisionserklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og

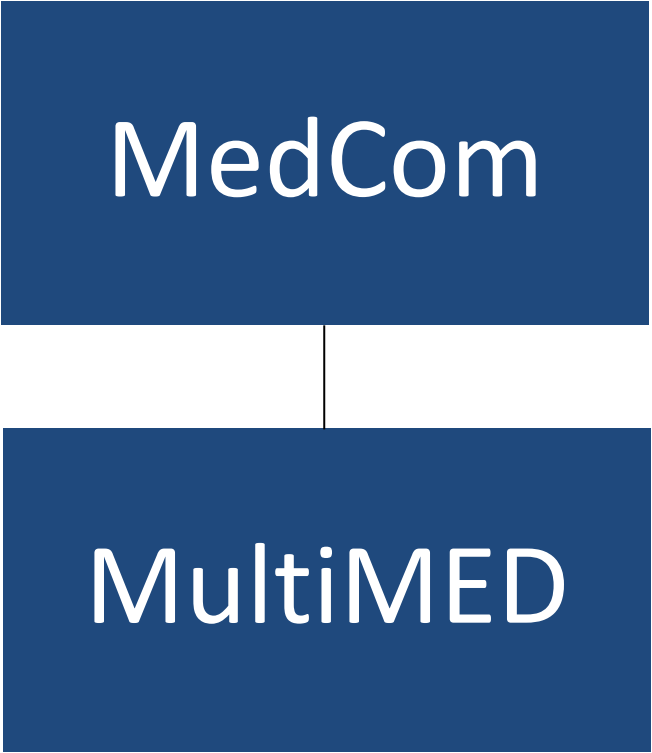
kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Den dataansvarlige kan – hvis det findes nødvendigt – vælge med rimeligt varsel at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle udgifter i forbindelse med en inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion. Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med afholdelse af et fysisk tilsyn/en inspektion hos underdatabehandleren er den dataansvarlige uvedkommende – uanset at den dataansvarlige har initieret og eventuelt deltaget på et sådant tilsyn.

Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til Datatilsynet efter anmodning herom fra Datatilsynet.



```
graph TD; MedCom[MedCom] --- MultiMED[MultiMED];
```

MedCom

MultiMED