Underdatabehandleraftale

mellem

Parterne

Organisationens navn:

Adresse:

Postnummer og by:

CVR-nummer:

(Herefter kaldet **Databehandleren)**

Og

MedCom

Forskerparken 10

5230 Odense M

26 91 99 91

(Herefter kaldet **Underdatabehandler**)

Er der indgået nedenstående underdatabehandleraftale (herefter **Underdatabehandleraftalen**) om Underdatabehandlerens behandling af personoplysninger for den Databehandler, der behandler personoplysninger på vegne af den Dataansvarlige.

Ved denne Underdatabehandleraftale sikrer Databehandler, at Underdatabehandler er pålagt de samme databeskyttelsesforanstaltninger som Databehandleren er, for så vidt angår Databehandlerens instruks fra Dataansvarlig om transmission af sundhedsdata i SDN.

Udarbejdet ud fra den Fælles skabelon for databehandleraftale til brug mellem sundhedsvæsenets parter

1. Definitioner

Dataansvarlig	En fysisk eller juridisk person, en offentlig myndighed, en institution eller andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den Dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret.
Databehandler	En fysisk eller juridisk person, en offentlig myndighed, en institution eller andet organ, der behandler personoplysninger på den Dataansvarliges vegne.
Hovedaftale	Den aftale eller kontrakt, der er indgået mellem parterne vedrørende udførelse af de opgaver, hvortil Underdatabehandleraftalen er knyttet.
Sikkerhedsgodkendelse	Ved sikkerhedsgodkendelse forstås en status, som en person tildeles efter en personundersøgelse, således at denne kan få adgang til klassificeret materiale eller -områder. I Danmark foretages personundersøgelser og sikkerhedsgodkendelser af Politiets Efterretningstjeneste.
Tredjelande og internationale organisationer	Et tredjeland er et land, som ikke er medlem af EU eller EØS (Island, Liechtenstein og Norge). En international organisation kan f.eks. være Røde Kors, WHO, FN, OECD m.fl. For at reglerne i forordningens kapitel V finder anvendelse på internationale organisationer, er det en forudsætning, at den internationale organisation befinder sig i et tredjeland.
Underdatabehandler	En Databehandler, som Databehandleren har overladt hele eller dele af den behandling, som Databehandleren foretager på vegne af den Dataansvarlige.

2. Generelt

2.1 Denne underdatabehandleraftale vedrører Underdatabehandlerens forpligtelse til at efterleve EUROPA-PARLAMENTETS OG RÅDETS FORORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om ophævelse af direktiv 95/46EF (generel forordning om databeskyttelse) samt lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

2.2 Principperne og anbefalingerne i ISO27001 med senere ændringer vil på alle relevante områder finde anvendelse i det omfang, andet ikke fremgår af nærværende Underdatabehandleraftale.

2.3 Underdatabehandleren skal behandle personoplysninger i overensstemmelse med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2.4 Er det i forbindelse med indgåelsen af nærværende Underdatabehandleraftale aftalt, at Underdatabehandleren forpligter sig til at gøre sig bekendt med og efterleve den Dataansvarliges informationssikkerhedspolitik eller andre sikkerhedsretningslinjer, skal dette fremgå af punkt 17.2.

2.5 Underdatabehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

3. Formål

3.1 Underdatabehandlerens opgave og formålet med databehandlingen fremgår af punkt 17.1.

3.2 Underdatabehandleren må ikke behandle oplysninger omfattet af denne Underdatabehandleraftale til egne formål.

4. Den Dataansvarliges rettigheder og forpligtelser

4.1 Den Dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

4.2 Den Dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

4.3 Den Dataansvarlige er blandet andet ansvarlig for, at der foreligger hjemmel til den behandling, som underdatabehandleren instrueres i at foretage.

5. Underdatabehandlerens generelle forpligtelser

5.1 Underdatabehandleren er Underdatabehandler for de personoplysninger, som behandles af Databehandler på vegne af den Dataansvarlige iht. Hovedaftalen og Underdatabehandleraftalen.

5.2 Underdatabehandleren handler alene efter dokumenteret instruks fra den Dataansvarlige, som videreformidlet af Databehandler og alene i det omfang, det er nødvendigt for, at Underdatabehandleren kan opfylde sine forpligtelser iht. Hovedaftalen og Underdatabehandleraftalen jf. bilag 1 Databehandlerinstruks.

5.3 Underdatabehandleren underretter omgående Databehandler, som underretter den Dataansvarlige, hvis en instruks efter Underdatabehandlerens mening er i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5.4 Underdatabehandleren har de forpligtelser, som er pålagt Underdatabehandleren i medfør af lovgivningen, jf. punkt. 2.1.

5.5 Underdatabehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor den Dataansvarliges personoplysninger opbevares, jf. punkt 17.1. Underdatabehandleren skal underrette Databehandler, der underretter den Dataansvarlige om enhver ændring.

5.6 Denne Underdatabehandleraftale frigør ikke Underdatabehandleren for de forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt Underdatabehandleren.

6. Tekniske og organisatoriske sikkerhedsforanstaltninger

6.1 Underdatabehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal

gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

6.2 Ovenstående forpligtelse indebærer, at Underdatabehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

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

6.3 Underdatabehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag 1.

6.4 Underdatabehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandling af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed iagttages.

6.5 Underdatabehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af den Dataansvarliges personoplysninger, om Underdatabehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. punkt 11 samt bilag 1 Underdatabehandlerinstruks.

7. Anvendelse af ad hoc arbejdspladser

7.1 Anvendelse af ad hoc arbejdspladser (fjern- eller hjemmearbejdspladser) skal være godkendt af Databehandler og den Dataansvarlige.

7.2 Såfremt Underdatabehandleren foretager databehandling fra ad hoc arbejdspladser, skal Underdatabehandleren sikre, at disse lever op til de sikkerhedsmæssige krav i denne Underdatabehandleraftale med bilag samt Datatilsynets IT-sikkerhedstekster herom.

7.2.1 I det omfang databehandlingen sker fra ad hoc arbejdspladser, skal Underdatabehandleren i punkt 17.2 beskrive

- Hvilken krypteret forbindelse, der anvendes mellem ad hoc arbejdspladsen og Underdatabehandlerens/Dataansvarliges netværk

- Anvendelse af 2-faktor-autentifikation
- Underdatabehandlerens instruks til egne medarbejdere om anvendelse af ad hoc arbejdspladser.

8. Underretningspligt og assistance

8.1 Underdatabehandleren forpligter sig til uden unødig forsinkelse og skriftligt, at orientere Databehandleren, der orienterer den Dataansvarlige om afvigelser fra kravene i Underdatabehandleraftalen, f.eks.:

- Ved enhver fravigelse fra givne instrukser
- Ved enhver afvigelse fra det aftalte om tilgængelighed
- Ved planlagte releases, opgraderinger, tests mv.
- Ved enhver mistanke om brug på fortroligheden, misbrug, fortabelse og forringelse af data mv.

8.2 Yderligere forpligter Underdatabehandleren sig til uden unødig forsinkelse og senest 24 timer efter, at denne er blevet bekendt med bruddet skriftligt at orientere Databehandleren, der orienterer den Dataansvarlige om brud på persondatasikkerheden, f.eks.:

- Ved enhver konstatering af misbrug, fortabelse og forringelse af data mv.
- Ved enhver hændelig eller uautoriseret videregivelse af eller adgang til personoplysningerne behandlet efter denne Underdatabehandleraftale

Sådan at den Dataansvarlige har mulighed for at efterleve forpligtelsen til at anmelde bruddet til tilsynsmyndigheden inden for 72 timer.

En underretning om brud på persondatasikkerheden skal indeholde følgende oplysninger:

- karakteren af bruddet på datasikkerheden og, hvis det er muligt, hvem der er omfattet, antal berørte og antal berørte registreringer af personoplysninger
- beskrivelse af de sandsynlige konsekvenser der er af bruddet
- beskrivelse af de foranstaltninger Underdatabehandleren har truffet eller foreslår truffet for at håndtere databruddet og hvad der kan gøres for at begrænse dets mulige skadevirkninger

8.3 Underdatabehandleren skal følge op på sikkerhedshændelsen og underrette Databehandleren, der underretter den Dataansvarlige om de nærmere omstændigheder, herunder udarbejde en situationsrapport samt oplyse om, hvilke personoplysninger, der er kompromitteret, samt hvilke tiltag Underdatabehandleren har iværksat eller påtænker at iværksætte.

8.4 Underdatabehandleren og dennes Underdatabehandlere må hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud uden forudgående skriftlig aftale med den

Dataansvarlige om indholdet af en sådan kommunikation, medmindre Underdatabehandleren er retligt forpligtet til sådan kommunikation.

8.5 Underdatabehandleren og dennes eventuelle Underdatabehandlere skal uden unødig forsinkelse sammen med Databehandleren bistå den Dataansvarlige med håndteringen af enhver henvendelse fra en registrerede, herunder anmodning om indsigt, berigtigelse, blokering eller sletning, hvis de relevante personoplysninger behandles af Underdatabehandleren. Underdatabehandleren og dennes eventuelle Underdatabehandlere skal ligeledes sammen med Databehandleren bistå den Dataansvarlige med at overholde øvrige forpligtelser, der måtte påhvile den Dataansvarlige efter gældende ret, hvor bistanden er forudsat, samt bistand er nødvendigt for, at den Dataansvarlige kan overholde sine forpligtelser.

9. Underdatabehandlerens brug af Underdatabehandler[1]

9.1 Underdatabehandleren må ikke uden udtrykkelig skriftligt samtykke fra Databehandler anvende andre Underdatabehandlere end dem, der er angivet i bilag 2, til at behandle personoplysninger, som den Dataansvarlige har overladt til Databehandleren, og som Databehandleren har overladt til Underdatabehandleren i medfør af Underdatabehandleraftalen og Hovedaftalen. DDatabehandleren er berettiget til at stille vilkår for et sådant samtykke.

9.2 Underdatabehandleren skal indgå en skriftlig aftale med sin Underdatabehandler, hvor det sikres, at Underdatabehandleren som minimum kan opfylde de forpligtelser, som Underdatabehandleren har påtaget sig ved denne Underdatabehandleraftale, for så vidt angår den behandling af personoplysninger, der varetages af Underdatabehandleren. Underdatabehandleren indestår for kontraktsmæssigheden og lovligheden af Underdatabehandlerens behandling af personoplysninger. Det forhold, at Underdatabehandleren indgår aftale med en Underdatabehandler, fritager ikke Underdatabehandleren for pligten til at efterleve nærværende Underdatabehandleraftale.

9.3 Databehandleren kan til enhver tid forlange dokumentation fra Underdatabehandleren for eksistensen og indholdet af Underdatabehandleraftaler for de Underdatabehandlere, som Underdatabehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Databehandler og den Dataansvarlige.

9.4 Det er Underdatabehandlerens ansvar at sikre og dokumentere, at eventuelle Underdatabehandlere, er bekendt med og efterlever den Dataansvarliges instruks (bilag 1).

9.5 Al kommunikation mellem den Dataansvarlige og Underdatabehandlerens Underdatabehandlere skal som udgangspunkt ske via Underdatabehandleren og Databehandleren.

[1] Såfremt underunderdatabehandleren er etableret i et tredjeland, skal reglerne i kapitel 11 ligeledes iagttages.

9.6 Ved ophør af en aftale med en Underdatabehandler skal Underdatabehandleren give Databehandleren meddelelse herom. Underdatabehandleren skal i den forbindelse sikre, at Underdatabehandleren sletter data behørigt i overensstemmelse med kravene i punkt 13.

Skift af Underdatabehandler i aftaleperioden

9.7 Underdatabehandleren kan udpege en ny Underdatabehandler, såfremt den nye Underdatabehandler (1) overholder gældende love om databeskyttelse og (2) er bundet af en Underdatabehandleraftale og (3) har et sikkerhedsniveau som er mindst den samme som den nuværende Underdatabehandler.

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

9.9 Såfremt Databehandler ikke mener, at en af Underdatabehandleren udpeget Underdatabehandler lever op til et eller flere af de ovennævnte krav under punkt (1), (2) og (3), vil det blive betragtet som væsentlig misligholdelse og der henvises til punkt 14 om misligholdelse. Inden væsentlig misligholdelse gøres gældende skal Databehandler underrette Underdatabehandler om forholdet og give en passende frist til at udbedre misligholdelsen.

10. Overførsel af personoplysninger til tredjelande eller internationale organisationer

10.1 Underdatabehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Underdatabehandleren er underlagt; i så fald underretter Underdatabehandleren Databehandleren om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. databeskyttelsesforordningens art. § 28, stk. 3, litra a.

10.2 Uden den Dataansvarlige instruks eller godkendelse kan Underdatabehandleren – indenfor rammerne af Underdatabehandleraftale – derfor bl.a. ikke;

a) videregive personoplysninger til en Dataansvarlig i et tredjeland eller i en international organisation,
b) overlade behandlingen af personoplysninger til en Underdatabehandler i et tredjeland [2],

[2] Se også pkt. 9

c) lade oplysningerne behandle i en anden af Underdatabehandlerens afdelinger, som er placeret i et tredjeland.

10.3 Den Dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af dennes aftales punkt 17.2.

11. Tavshedspligt og fortrolighed

11.1 Personoplysninger omfattet af denne aftale er fortrolige.

11.2 Underdatabehandleren sikrer, at de personer, de er autoriseret til at behandle personoplysninger på vegne af den Dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

11.3 Det påhviler Underdatabehandleren og dennes eventuelle Underdatabehandlere at informere egne ansatte, samarbejdspartnere, eksterne konsulenter, vikarer m.fl. om udstrækningen af tavshedspligten og om konsekvenserne ved en eventuel overtrædelse.

11.4 Kun de personer hos Underdatabehandleren eller dennes Underdatabehandlere, der autoriseres hertil, må have adgang til de personoplysninger, der behandles og brugerne må kun autoriseres til anvendelser, de har behov for i forhold til at kunne opfylde Databehandlerens forpligtelser over for den Dataansvarlige.

11.5 Underdatabehandleren og dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

11.6 Underdatabehandlerens forpligtelser om tavshedspligt og fortrolighed gælder også efter aftalens ophør.

12. Audit og revisionserklæringer

12.1 Underdatabehandleren skal på Databehandlerens anmodning give de nødvendige oplysninger til, at de kan påse forpligtelserne i henhold til denne aftale samt at der er truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger. Endvidere skal Underdatabehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.

12.2 Såfremt den Dataansvarlige, en repræsentant for den Dataansvarlige, dennes revision

(intern eller ekstern) eller en relevant offentlig myndighed, særligt Datatilsynet, ønsker at foretage fysisk inspektion (audit) af de foranstaltninger, som Underdatabehandleren har etableret i medfør af aftalen, forpligter Underdatabehandleren sig til - med et rimeligt varsel – at stille tid og ressourcer til rådighed herfor. Underdatabehandleren forpligter sig til på samme måde at sikre, at sådanne audits kan gennemføres hos sine eventuelle Underdatabehandlere.

12.3 Som supplement eller alternativ til de overfor nævnte audits kan der indgås aftale om, at Underdatabehandleren og dennes eventuelle Underdatabehandlere for egen regning sørger for, at en uafhængig ekspert årligt udarbejder en revisionserklæring på grundlag af en anerkendt standard angående Underdatabehandlerens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Underdatabehandleraftalen. Erklæringen skal være formuleret konkret i forhold til den opgave, som Underdatabehandleren løser for den Dataansvarlige. En sådan aftale skal fremgå af punkt 17.2.

13. Håndtering af data efter aftalens ophør

13.1 Underdatabehandleren og dennes eventuelle Underdatabehandlere forpligter sig til at tilbagelevere og/eller slette personoplysninger, når databehandlingen i henhold til Hovedaftalen med Databehandleren ophører medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

13.2 Databehandleren skal inden Hovedaftalens ophør skriftligt meddele Underdatabehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den Dataansvarlige. Fristen herfor aftales mellem parterne.

13.3 Underdatabehandleren er ansvarlig for, at sletning af oplysningerne sker på en sådan måde, at det ikke er muligt at genskabe oplysningerne. Underdatabehandleren er herunder ansvarlig for at oplysningerne også slettes fra backup samt hos eventuelle Underdatabehandlere.

13.4 Hvis oplysningerne tilbageleveres til den Dataansvarlige, skal Underdatabehandleren slette eventuelle kopier af oplysningerne.

13.5 Når sletningen er gennemført, skal Underdatabehandleren fremsende en skriftlig erklæring på, at data er slettet som aftalt.

13.6 Såfremt Underdatabehandleren eller dennes Underdatabehandlere i forbindelse med konkurs eller lignende ophører med at behandle personoplysninger for den Dataansvarlige, skal alle personoplysninger uden ugrundet ophold tilbageleveres på en måde, der gør det muligt for den Dataansvarlige at anvende disse fremadrettet. Underdatabehandler, dennes konkursbo e.l. er herefter forpligtet til at slette oplysninger fra deres egne systemer i overensstemmelse med pkt. 13.1-13.5.

14. Misligholdelse

14.1 Bestemmelserne i dette afsnit har forrang ift. Hovedaftalen, for så vidt angår behandlingen af personoplysninger. Såfremt dette ikke er tilfældet, angives det i pkt. 17.1.

14.2 Ved Underdatabehandlerens misligholdelse af Underdatabehandleraftalen er den Databehandleren berettiget til at gøre sædvanlige misligholdelsesbeføjelser gældende med de tilføjelser og præciseringer, som fremgår af bestemmelserne i dette afsnit.

14.3 Ved væsentlig misligholdelse af Underdatabehandleraftalen er Databehandleren berettiget til at ophæve Hovedaftalen og dermed også Underdatabehandleraftalen. Som udgangspunkt betragtes det som væsentlig misligholdelse, såfremt Underdatabehandleren ikke overholder forpligtelserne i Underdatabehandleraftalen, den til enhver tid gældende lovgivning vedrørende databeskyttelse samt kravene i de dokumenter, der udgør bilag til Underdatabehandleraftalen.

14.4 Databehandlerens ophævelse af Hovedaftalen og Underdatabehandleraftalen indebærer ikke, at Databehandleren giver afkald på sin ret til at kræve erstatning, hvis betingelserne herfor er opfyldt, jf. pkt. 14.7.

14.5 Såfremt Databehandleren vælger ikke at ophæve Hovedaftalen og Underdatabehandleraftalen i ét eller flere tilfælde, selvom Databehandleren er berettiget hertil, medfører dette ikke, at Databehandleren mister retten til at ophæve Hovedaftalen og Underdatabehandleraftalen i andre tilfælde.

14.6 Ved ophævelse af Hovedaftalen og Underdatabehandleraftalen, er Underdatabehandleren forpligtet til at levere databehandling i henhold til Hovedaftalen og denne Underdatabehandleraftale, indtil databehandlingen er sikret hos en anden Underdatabehandler. Underdatabehandleren er ligeledes forpligtet til at levere relevant ophørsassistance til Databehandleren, herunder i relation til eventuelle Underdatabehandlere, som Underdatabehandleren måtte have overladt en del af databehandlingen til.

14.7 Underdatabehandleren er erstatningsansvarlig i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af Underdatabehandleraftalen. Såfremt Databehandleren af den Dataansvarlige eller tredjemand gøres erstatningsansvarlig for Underdatabehandlerens og/eller eventuelle Underdatabehandleres manglende overholdelse af Underdatabehandleraftalen, herunder Underdatabehandleraftalens bilag, og/eller overtrædelse af gældende lovgivning vedrørende databeskyttelse, skal Underdatabehandleren holde Databehandleren skadesløs for alle omkostninger, gebyrer, erstatningsbeløb, udgifter eller tab, som den Databehandleren har afholdt eller pådraget sig som følge heraf.

14.8 Databehandleren er berettiget til at stille krav om, at Underdatabehandleren bistår med at forsvare den Dataansvarlige eller Databehandlerens interesser i en eventuel rets- eller voldgiftssag, uagtet Underdatabehandlerens eventuelle indsigelser i forhold til den

påberåbte misligholdelse, såfremt Underdatabehandlerens bistand er af væsentlig betydning for varetagelsen af den Dataansvarlige eller Databehandlerens interesser.

15. Lovvalg og værneting

15.1 Medmindre lovvalg og værneting er direkte reguleret i Hovedaftalen, finder følgende bestemmelser anvendelse:

15.1.1 Denne Underdatabehandleraftale inklusiv ethvert spørgsmål om Underdatabehandleraftalens gyldighed er undergivet dansk ret.

15.1.2 Såfremt der opstår uoverensstemmelser mellem Parterne i forbindelse med Underdatabehandleraftalen, skal Parterne med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med henblik på at løse tvisten.

15.1.3 Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved de danske domstole ved den Dataansvarliges hjemting.

16. Ikrafttræden og varighed

16.1 Nærværende Underdatabehandleraftale indgås ved begge parters underskrift og gælder indtil behandlingen af personoplysninger i henhold til Hovedaftalen er ophørt og Underdatabehandleren har slettet data, jf. pkt. 13.

16.2 Databehandleren og Underdatabehandleren er solidariske ansvarlige for at sikre, at der foretages de nødvendige opdateringer i Underdatabehandleraftalen ved lovændringer, hvis den Dataansvarlige forpligtes til at efterkomme nye sikkerhedsstandarder eller hvis der sker ændringer af tekniske eller organisatoriske forhold hos den Dataansvarlige, Databehandleren og/eller Underdatabehandleren.

17. Specifikke forhold vedr. databehandlingen

(Såfremt Underdatabehandlerens opgave, jf. Hovedaftalen, vedrører flere forskellige databehandlinger, er der angivet kopier af nedenstående tabeller til venstre i pdf-vinduet. Disse anvendes for hver enkelt databehandling, som Underdatabehandleraftalen omfatter)

17.1 Generelle forhold

Databehandlingens navn	Sundhedsdatanettet (SDN)
ID i den Databehandlens fortegnelse over databehandlinger	
ID i Underdatabehandlerens fortegnelse	3
Hovedaftale/kontrakt (dato for indgåelse, journal-ID)	Tilslutningsaftale for SDN, den:
Databehandlingens formål	Understøtte deling via transmission af personoplysninger mellem og for parter i den danske sundhedssektor.
Generel beskrivelse af behandlingen	Aftale om deling af personoplysninger administreres og reguleres af de tilsluttede parter selv i SDNs aftalesystem som instruks for transmissionen.
Registrerede personer (kategorier af personer, der indgår i databehandlingen)	Patienter, borgere, sundhedspersoner samt teknisk / administrativt personale.

Kategorier af personoplysninger	Personoplysninger, herunder fortrolige og følsomme personoplysninger i form af helbredsoplysninger.
Evt. modtagere af oplysninger	Parter defineret i aftalen.
Sletningsfrister	Personoplysninger, der transmitteres via SDN-nettet, gemmes ikke - og der tages ikke backup. Personoplysninger i aftalesystemets brugerdatabase oprettes og slettes af den tilsluttede part selv. Aftalesystemets aftaledatabase indeholder dokumentation for, hvilke brugere fra den tilsluttede part, der har indgået aftaler. Disse personoplysninger slettes, når aftalen slettes – og senest ved nedlæggelse af partens tilslutning til SDN.
Evt. lov/bestemmelse, der hjemler databehandlingen	
Underdatabehandlerens opgave	Underdatabehandlerens opgave består i at etablere, drifte, forvalte og overvåge SDN samt yde support som nærmere angivet i Hovedaftalen.
Lokationer for databehandlingen	Data behandles hos underleverandørerne TDC NetDesign og Netic. For tilslutninger via SDN-MPLS behandles data desuden i aktivt netværksudstyr placeret hos de tilsluttede parter. De præcise adresser er af sikkerhedsmæssige grunde fortrolige, men kan på anmodning oplyses.

17.2 Særlige forhold vedr. databehandlingen (hvis ikke relevant, markeres dette)

Evt. andre lovkrav, som databehandlingen er underlagt (f.eks. krav om, at data skal opbevares i Danmark eller evt. specifikke samtykkekrav)	

Evt. andre krav, som den dataansvarlige pålægger underdatabehandleren	Skift af Underdatabehandler i SDN må imødeses jævnligt, da kontrakten er udbudspligtig og udbydes af MedCom på vegne af alle aktører i SDN. De Dataansvarlige er repræsenteret i udbudsprocessen – både i kravspecifikation og beslutning gennem brugergruppe og styregruppe. MedCom vil udbudsretlig være forpligtet af udbuddet og har ikke mulighed for herefter at give Dataansvarlig adgang til at ændre sin vurdering af en ny Underdatabehandler efter tildeling af kontrakt. Underdatabehandleraftalens afsnit 9.9 er således fraveget i denne Underdatabehandleraftale. Betingelser i SDN-tilslutningsaftalen (hovedaftalen), herunder bestemmelser om misligholdelse er vedtaget af MedComs styregruppe, og der er indgået særskilt aftale mellem MedCom og den Dataansvarlige inden for rammerne af offentlig-offentligt samarbejde. Bestemmelser om misligholdelse i denne Underdatabehandleraftale finder derfor ikke anvendelse. Underdatabehandleraftalens afsnit 14 er derfor fraveget. Hvis Dataansvarlig eller Databehandleren kræver specifikke foranstaltninger implementeret i SDN, uden at tilsvarende krav er vedtaget af MedComs styregruppe, skal sådanne foranstaltninger alene kunne implementeres på den Dataansvarlige eller Databehandlerens regning. I det omfang flere Dataansvarlige eller Databehandlere kræver de samme foranstaltninger, kan de pågældende Dataansvarlige eller Databehandler dele omkostningerne til foranstaltningerne.
Aftale mellem parterne om helt eller delvist fravigelse af krav i underdatabehandleraftalen (Beskriv aftalte fravigelser og eventuelle kompenserende sikkerhedsforanstaltninger)	Kravene til SDN fastsættes af MedComs styregruppe, og Dataansvarlig kan ikke selvstændigt stille krav til SDN. Hvis Dataansvarlig kræver specifikke foranstaltninger implementeret i SDN, uden at tilsvarende krav er vedtaget af MedComs styregruppe, skal sådanne foranstaltninger alene kunne implementeres på den Dataansvarliges regning. I det omfang flere Dataansvarlige kræver de samme foranstaltninger, kan de pågældende dataansvarlige dele omkostningerne til foranstaltningerne. Sikkerhedskrav hos MedCom baseres på ISO27001, men der kan forekomme konkrete fravigelser. MedComs aktuelle sikkerhedsforanstaltninger kan rekvireres hos MedCom.

	Alle afviste adgangsforsøg registreres. Gentagne adgangsforsøg blokeres ikke, da en blokering vil kunne ramme legitime logins fra samme brugerlokation hos den tilsluttede part. Gentagne adgangsforsøg udløser i stedet alarm med henblik på klarlægning af årsag. Underdatabehandleraftalens instruks punkt 5.1 er derfor fraveget.

Underdatabehandleren forpligter sig til at efterleve den dataansvarliges informationssikkerhedspolitik og/eller retningslinjer. (Angiv relevante dokumenter)	Kravene til SDN fastsættes af MedComs styregruppe, og Dataansvarlig kan ikke selvstændigt stille krav til SDN. Hvis Dataansvarlig kræver specifikke foranstaltninger implementeret i SDN, uden at tilsvarende krav er vedtaget af MedComs styregruppe, skal sådanne foranstaltninger alene kunne implementeres på den Dataansvarliges regning. I det omfang flere Dataansvarlige kræver de samme foranstaltninger, kan de pågældende Dataansvarlige dele omkostningerne til foranstaltningerne. Sikkerhedspolitik mv. for SDN kan til enhver tid rekvireres hos MedCom.
Den dataansvarlige har givet instruks om eller godkendelse af overførsel af personoplysninger til tredjeland eller international organisation (anfør også overførselsgrundlag efter databeskyttelsesforordningens kapitel 5).	SDN leverer tilslutning af udenlandske parter til SDN, herunder usikre tredjelande. Udenlandske parter godkendes før tilslutning i MedComs styregruppe. Transmissionen af personoplysninger forudsætter aftale mellem parterne i aftalesystemet, dvs. Dataansvarlig gennem Databehandleren og den udenlandske part. Det påhviler den Dataansvarlige at sikre, at der er et lovligt grundlag for overførsel af personoplysninger til usikre tredjelande.
Særlige tekniske eller organisatoriske sikkerhedsforanstaltninger, som skal etableres hos Underdatabehandleren (f.eks. sikkerhedsgodkendelse af medarbejdere)	Kravene til SDN fastsættes af MedComs styregruppe, og Dataansvarlig kan ikke selvstændigt stille krav til SDN. Hvis Dataansvarlig kræver specifikke foranstaltninger implementeret i SDN, uden at tilsvarende krav er vedtaget af MedComs styregruppe, skal sådanne foranstaltninger alene kunne implementeres på den dataansvarliges regning. I det omfang flere Dataansvarlige kræver de samme foranstaltninger, kan de pågældende Dataansvarlige dele omkostningerne til foranstaltningerne.

	Sikkerhedspolitik mv. for SDN kan til enhver tid rekvireres hos MedCom.
Beskrivelse af sikkerhedsforanstaltninger ved anvendelse af ad hoc arbejdspladser efter aftale med den Dataansvarlige	Underdatabehandlerne TDC Netdesign og Netics anvendelse af ad hoc arbejdspladser følger minimum følgende krav: Fjernadgang til SDN sker via AES256-bit-krypteret VPN-adgang med 2-faktor-autentifikation. Adgang til aftalesystemet sker via en web-brugerflade med TLS 1.2-kryptering og 2-faktor-autentifikation.
Beskrivelse af sikkerhedsforanstaltninger ved eksterne kommunikationsforbindelser	SDN-MPLS er et fully meshed privat / segmenteret netværk, som via samme VRF sikrer, at de SDN-tilsluttede parter kan kommunikere med hinanden, hvis ACL'er i det decentrale aktive netværksudstyr hos de tilsluttede parter tillader det. Sikkerheden på faste forbindelser, andre MPLS-forbindelser og VPN-forbindelser varetages af ACL'er på det centrale netværksudstyr i SDNs knudepunkt.
Uddybende beskrivelse af foranstaltninger til beskyttelse af transmission af personoplysninger over åbne netværk	Sikkerhedskrav til VPN-forbindelser fremgår af MedComs hjemmeside.
Opbevaringstid for log (hvis længere end 6 måneder, jf. punkt 5.2 i underdatabehandlerinstruksen).	Trafik på SDN logges for aggregering af monitorerings- og trafikstatistikker på tværs af de tilsluttede parter. Loggen indeholder ikke personoplysninger men kun oplysninger om den gennemførte transmission – og slettes ikke. Hændelseslog i aftalesystemet dokumenterer brugerhandlinger og slettes efter 2 år. Når en tilsluttet part nedlægges i aftalesystemet, renses hændelseslog for personoplysninger fra den tilsluttede part.

Evt. aftale om udarbejdelse af revisionserklæring, herunder angivelse af type	MedCom gennemfører årligt en uafhængig it-revision af SDN, herunder VDX med henblik på overholdelse af Databeskyttelsesloven. Den Dataansvarlige eller Databehandleren skal afholde omkostningerne ved yderligere auditering, herunder omkostninger til Underdatabehandleren og dennes Underdatabehandleres medvirken hertil.

17.3 Kontaktoplysninger i forbindelse med underretning om sikkerhedshændelser

Kontaktpersoner hos Databehandleren ved almindelige afvigelser fra normal drift	
Funktion	Teknisk kontaktperson i Tilslutningsaftale for SDN
Navn	*(fremgår af tilslutningsaftale)*
E-mail	*(fremgår af tilslutningsaftale)*
Telefon	*(fremgår af tilslutningsaftale)*
Bemærkninger	
Kontaktpersoner hos Databehandleren ved kritiske fejl og sårbarheder samt ved mistanke herom	
Funktion	Sikkerhedsansvarlig og teknisk kontaktperson i Tilslutningsaftale for SDN
Navn	*(fremgår af tilslutningsaftale)*
E-mail	*(fremgår af tilslutningsaftale)*
Telefon	*(fremgår af tilslutningsaftale)*
Bemærkninger	
Kontaktpersoner hos Underdatabehandleren ved almindelige afvigelser fra normal drift	
Funktion	Sikkerhedsansvarlig
Navn	Peder Illum
E-mail	sdn@medcom.dk
Telefon	6543 2030
Bemærkninger	I praksis skal henvendelser ske til SPOC hos Underdatabehandler. Kontaktoplysninger og information findes på www.medcom.dk.
Kontaktpersoner hos Underdatabehandleren ved kritiske fejl og sårbarheder samt ved mistanke herom	
Funktion	Sikkerhedsansvarlig
Navn	Peder Illum
E-mail	sdn@medcom.dk
Telefon	6543 2030
Bemærkninger	Foruden MedCom skal henvendelser ske til SPOC hos Underdatabehandler. Kontaktoplysninger og information findes på www.medcom.dk.

18. Bilagsliste

Bilag 1: Databehandlerinstruks
Bilag 2: Underdatabehandler

Bilag 1
Databehandlerinstruks

1. Databehandlerens ansvar

Databehandling omfattet af Databehandleraftalen skal ske i overensstemmelse med denne instruks.

2. Generelt

2.1 Databehandleren skal som minimum træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysninger omfattet af Databehandleraftalen.

2.1.1 Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger, beskrevet i punkt 17.2, er nødvendige for at sikre efterlevelse af Databehandleraftalens punkt 6.1, skal sådanne mere omfattende foranstaltninger altid træffes.

2.2 Databehandleren skal udpege et fast kontaktpunkt, som over for den Dataansvarlige skal varetage ethvert forhold i relation til behandlingen af personoplysninger på vegne af den Dataansvarlige, jf. punkt 17.3

2.3 Databehandleren skal tage de nødvendige skridt til at identificere, vurdere og begrænse enhver, med rimelighed forudsigelig, intern og ekstern risiko for tilgængeligheden, fortroligheden, og/eller integriteten af alle personoplysninger omfattet af Databehandleraftalen.

3. Autorisation og adgangskontrol

3.1 Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.

3.2 Databehandleren skal sikre, at der foretages et efter omstændighederne passende baggrundstjek for alt personale, der i forbindelse med deres ansættelse vil have

adgang til personoplysninger omfattet af Databehandleraftalen, uanset i hvilket format personoplysninger måtte være tilgængelige.

3.2.1 Såfremt den Dataansvarlige stiller krav om, at personale hos Databehandleren, der har adgang til personoplysninger, skal være sikkerhedsgodkendt, skal dette fremgå af Databehandleraftalens 17.2.

3.3 Kun de personer hos Databehandleren, som autoriseres dertil, må have adgang til personoplysninger, der behandles i henhold til Databehandleraftalen. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles.

3.4 Der må endvidere autoriseres personer hos Databehandleren, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

3.5 Databehandleren skal kunne dokumentere hvilke medarbejdere, der har autorisation til at tilgå personoplysninger, der behandles i henhold til Databehandleraftalen.

3.6 Autoriserede personer hos Databehandleren udstyres med en personlig brugeridentifikation og et personligt password, der skal anvendes hver gang, der logges på systemet. Der skal anvendes 2-faktor-autentificering ved adgang til systemer med følsomme personoplysninger via internettet eller andet usikkert netværk.

3..7 Databehandleren skal sikre, at dennesmedarbejdere modtager den tilstrækkelig uddannelse og instruktioner for at sikre, , at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Databehandlerens og den Dataansvarliges politikker og procedurer herfor.

3.8 Der skal træffes foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, og at brugeren kun kan få adgang til de personoplysninger og anvendelser (behandlinger), som den pågældende er autoriseret til.

3.9 Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

3.10 Der skal mindst en gang hvert halve år foretages kontrol af, at brugerne kun er tildelt de adgange, som de har behov for. Denne kontrol kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, således at det kan konstateres, om der er udstedte autorisationer, som ikke er anvendt, og som derfor eventuelt bør inddrages. Ved anvendelse af en sådan statistisk opfølgning vil der fortsat være behov for en konkret vurdering af, om medarbejderen har et fortsat arbejdsmæssigt behov for adgang.

3.11 Databehandleren skal uden unødig forsinkelse inddrage autorisationer (og herunder adgange) for brugere, der ikke længere har behov for autorisationen i forbindelse med brugerens arbejde.

4. Fysisk sikring

4.1 Databehandleren skal sikre, at it-udstyr, der anvendes i forbindelse med databehandlingen, er fysisk sikret i henhold til gældende lovkrav

4.2 Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler.

4.3 Ved reparation og service af udstyr, skal Databehandleren sikre, at reparations- og servicepersonalet behandler eventuelle personoplysninger, de bliver bekendt med under deres arbejde, fortroligt.

4.4 Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller afmagnetiseres, såder sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal forevises, når den Dataansvarlige anmoder herom.

5. Kontrol med afviste adgangsforsøg og logning

5.1 Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret højst 35 på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Adgangen åbnes først, når årsagen til de afviste adgangsforsøg er klarlagt.

5.2 Der skal foretages maskinel registrering (logning) af ved al behandling af personhenførbare oplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, med mindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode af hensyn til at kunne anvende loggen som værktøj til brug for efterforskning.

5.2.1 Aftales der en længere opbevaringstid for loggen, skal dette fremgå af Databehandleraftalens punkt 17.2.

5.3 Databehandleren skal efter ønske fra den dataansvarlige stille nødvendige loginformationer til rådighed for den Dataansvarlige til brug for gennemførelse af periodisk audit eller til undersøgelse af misbrug eller mistanke om misbrug.

6. Håndtering af ind- og uddatamateriale indeholdende personoplysninger

6.1 Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddateringen. Inddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, der er indeholdt heri.

6.2 Når det ikke længere er nødvendigt at bevare inddatamaterialet, skal Databehandleren slette eller tilintetgøre inddatamaterialet. Fremgangsmåden herfor skal ske efter best practice.

6.3 Punkt 6.2 gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser i henhold til anden lovgivning, eller hvis journaliseret materiale behandles efter de almindelige arkiv bestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver.

6.4 Uddatamaterialeer omfattet af samme instrukser som inddatamateriale..

6.5 Udover bestemmelsen i punkt 6.4 må uddatamateriale kun anvendes af personer, der er beskæftiger med de formål, til hvilke behandlingen af personoplysninger foretages, samt i forbindelse med revision, teknisk vedligeholdelse, driftsovervågning og fejlretning mv.

7. Mobile lagringsenheder

7.1 Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares krypteret under opsyn eller under lås, når de ikke benyttes.

7.2 Mobile lagringsmedier med personoplysninger må kun udleverestil autoriserede personermed henblik på revision eller drifts- og systemtekniske opgaver

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

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

7.5 I forbindelse med reparation og service af dataudstyr, 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. Dette skal ske efter best practice.

8. Sikkerhedskopier

8.1 Der gælder de samme retningslinjer for sikkerhedskopier som for al anden behandling af personoplysninger i medfør af denne aftale.

8.2 Databehandleren skal sikre, at systemer og personoplysninger sikkerhedskopieres regelmæssigt. Sikkerhedskopierne skal opbevares adskilt fra serverne i et ikke tilstødende rum for at sikre, at disse ikke går tabt f.eks. som følge af brand eller oversvømmelse. Opbevaring af sikkerhedskopier skal altid ske på betryggende vis så de ikke fortabes.

8.3 Databehandleren skal regelmæssigt kontrollere, at sikkerhedskopier er læsbare. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af system teknisk setup.

9. Opdateringer og ændringer

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

9.1.1 For kritiske sikkerhedsopdateringer skal Databehandleren have procedurer, der sikrer at disse kan gennemføres inden for 48 timer.

9.2 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.

10. Eksterne kommunikationsforbindelser

10.1 Der må kun etableres eksterne it-kommunikationsforbindelser med tilladelse fra den Dataansvarlige og der træffes foranstaltninger til at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

10.1.1 Der skal træffes foranstaltninger til beskyttelse af personoplysninger, der transmitteres over åbne net. Eventuelle uddybende beskrivelser af foranstaltningerne skal fremgå af Databehandleraftalens punkt 17.2.

11. IT-beredskab

11.1 Databehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimeligtid i tilfælde af driftsafbrydelser.

12. Underretning om sikkerhedshændelser og assistance ved håndteringen

12.1 Databehandlerens skal have en procedure for håndtering og opfølgning på sikkerhedsbrud i overensstemmelse med kravene i ISO27001.

12.2 Databehandleren skal dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau.

12.3 Oversigt over kontaktpersoner i forbindelse med underretning om sikkerhedshændelser skal fremgå af Databehandleraftalens punkt 17.3.

For Databehandleren

Dato:

Navn:

_____

For Underdatabehandleren

Dato:

Navn:

_____