Underdatabehandleraftale

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

Mellem Databehandleren:

Organisation:
Adresse:
Postnr./By:
Land:
CVR:
Journalnummer:

Og Underdatabehandleren:

MedCom
Forskerparken 10
5230 Odense M
Danmark
CVR 26919991
Journalnummer:

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.

I henhold til databehandleraftalerne mellem Databehandleren og de tilsluttede parter i Sundhedsdatanettet (SDN), er de tilsluttede parter Dataansvarlige for behandlinger af personoplysninger i SDN, og Databehandleren er Databehandler for behandlinger af personoplysninger i SDN.

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

Indholdsfortegnelse

Indhold

1 Præambel

1. Disse Bestemmelser fastsætter Underdatabehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af Databehandleren.

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:

Tilslutning til Sundhedsdatanettet (SDN) jf. den indgåede tilslutningsaftale.

4. Underdatabehandleren behandler personoplysninger på vegne af Databehandleren i overensstemmelse med disse Bestemmelser.

5. Bestemmelserne har forrang i forhold til eventuelle tilsvarende Bestemmelser i andre aftaler mellem parterne.

6. Der hører fire 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 Databehandlerens betingelser for Underdatabehandlerens brug af Underdatabehandlere og en liste af Underdatabehandlere, som Databehandleren har godkendt brugen af.

9. Bilag C indeholder den Dataansvarliges instruks, som videreformidlet af Databehandleren for så vidt angår Underdatabehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som Underdatabehandleren som minimum skal

gennemføre, hvordan Underdatabehandleren bistår Databehandleren samt hvordan der føres tilsyn med Underdatabehandleren og eventuelle yderligere Underdatabehandlere.

10. Bilag D indeholder Bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne samt aftalte tilføjelser eller afvigelser fra Bestemmelserne.

11. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

12. Disse Bestemmelser frigør ikke Underdatabehandleren fra forpligtelser, som Underdatabehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

2 Den Dataansvarliges forpligtelser og rettigheder

1. Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

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

3. Den Dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som Underdatabehandleren instrueres i at foretage.

3 Underdatabehandleren handler efter instruks

1. Underdatabehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, som videreformidlet fra Databehandleren medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Underdatabehandleren 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. Underdatabehandleren underretter omgående Databehandleren, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

3. Parterne bør forudse og overveje eventuelle konsekvenser, der kan følge af en eventuel ulovlig instruks, som den Dataansvarlige har givet. Parterne skal, hvis det er relevant, regulere dette forhold i bilag D.

4 Fortrolighed

1. Underdatabehandleren må kun give adgang til personoplysninger, som behandles på Databehandlerens vegne, til personer, som er underlagt Underdatabehandlerens 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. Underdatabehandleren skal efter anmodning fra Databehandleren kunne påvise, at de pågældende personer, som er underlagt Underdatabehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

5 Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den Dataansvarlige, Databehandleren og Underdatabehandleren, 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 Underdatabehandleren – uafhængigt af den Dataansvarlige og Databehandleren – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal Databehandleren stille den nødvendige information fra de Dataansvarlige til rådighed for Underdatabehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal Underdatabehandleren bistå Databehandleren med vedkommendes overholdelse af Databehandlerens forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for Databehandleren vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som Underdatabehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for Databehandlerens overholdelse af sin forpligtelse efter forordningens artikel 32.
Hvis imødegåelse af de identificerede risici – efter Databehandlerens vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som Underdatabehandleren allerede har gennemført, skal Databehandleren angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

6 Anvendelse af Underdatabehandlere

1. Underdatabehandleren 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).
Underdatabehandleren må således ikke gøre brug af en anden Underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående **specifik** eller **generel skriftlig godkendelse** fra Databehandleren. Listen over Underdatabehandlere, som Databehandleren allerede har godkendt, fremgår af bilag B.

2. Underdatabehandleren skal underrette Databehandleren om evt. planlagte ændringer vedr. tilføjelse eller udskiftning af Underdatabehandlere. Ændringer skal meldes Databehandleren med passende varsel.

FORUDGÅENDE SPECIFIK GODKENDELSE	N/A	N/A
FORUDGÅENDE GENEREL GODKENDELSE	JA	Mindst 3 måneders varsel

3. Når Underdatabehandleren gør brug af en anden Underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af Databehandleren, skal Underdatabehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EUretten eller medlemsstaternes nationale ret, pålægge denne Underdatabehandler 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.

   Underdatabehandleren er derfor ansvarlig for at kræve, at en anden Underdatabehandler som minimum overholder Databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter Databehandlerens anmodning herom – i kopi til Databehandleren, 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 Databehandleren.

6. Underdatabehandleren skal i sin aftale med en anden Underdatabehandler indføje Databehandleren som begunstiget tredjemand i tilfælde af Underdatabehandlerens konkurs, således at Databehandleren kan indtræde i Underdatabehandlerens rettigheder og gøre dem gældende over for andre Underdatabehandlere, som f.eks. gør Databehandleren i stand til at instruere Underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis Underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver

Underdatabehandleren fuldt ansvarlig over for Databehandleren 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.

7 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Underdatabehandleren på baggrund af dokumenteret instruks herom fra Databehandler og den Dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Underdatabehandleren ikke er blevet instrueret i at foretage af den Dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Underdatabehandleren er underlagt, skal Underdatabehandleren underrette Databehandleren 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 Underdatabehandleren 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.

8 Bistand til den Dataansvarlige

1. Underdatabehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt Databehandleren ved hjælp af passende tekniske og Organisatoriske foranstaltninger, med opfyldelse af de Dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.
   Dette indebærer, at Underdatabehandleren så vidt muligt skal bistå Databehandleren i forbindelse med, at de 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. den registreredes indsigtsret
   d. retten til berigtigelse
   e. retten til sletning (»retten til at blive glemt«)
   f. retten til begrænsning af behandling
   g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

2. Underdatabehandleren bistår de Dataansvarlige med at sikre overholdelse af de Dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Underdatabehandleren, jf. art 28, stk. 3, litra f.
   Dette indebærer, at Underdatabehandleren under hensyntagen til behandlingens karakter skal bistå de Dataansvarlige i forbindelse med, at den Dataansvarlige skal sikre overholdelsen af:

   a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
   b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den Dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt,

at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

c. forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
e. forpligtelsen til at høre tilsynsmyndigheden (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. Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med Underdatabehandlerens bistand til de Dataansvarlige og Databehandler vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

9 Underretning om brud på persondatasikkerheden

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

2. Underdatabehandlerens underretning til Databehandleren skal ske uden unødig forsinkelse 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. Tidsfrist for underretning af Databehandleren angives i bilag C.

3. I overensstemmelse med Bestemmelse 9.2. skal Underdatabehandleren sammen med Databehandleren bistå den Dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsyns-myndighed. Det betyder, at Underdatabehandleren 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 Underdatabehandleren skal tilvejebringe i forbindelse med sin bistand til den Dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

10 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Underdatabehandleren forpligtet til enten at slette alle personoplysninger, der er blevet behandlet på vegne af den Dataansvarlige eller at tilbagelevere alle personoplysninger og slette eksisterende kopier. Hvis der ikke foretages dataopbevaring hos Underdatabehandleren, er dette ikke relevant.

Slette alle personoplysninger

2. Eventuelle regler i EU-retten eller medlemsstaternes nationale ret, som foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedr. behandling af personoplysninger, angives i bilag D. Underdatabehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

11 Tilsyn og revision

1. Underdatabehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for Databehandleren og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af Databehandleren eller den Dataansvarlige eller en anden revisor, som er bemyndiget af Databehandleren eller den Dataansvarlige.

2. Procedurerne for Databehandlerens revisioner, herunder inspektioner, med Underdatabehandleren og andre Underdatabehandlere er nærmere angivet i Bilag C.7.

3. Underdatabehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den Dataansvarliges, Databehandlerens eller Underdatabehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til Underdatabehandlerens fysiske faciliteter mod behørig legitimation.

12 Parternes aftaler 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.

13 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 væsentlige uhensigtsmæssigheder i Bestemmelserne giver anledning hertil. Procedure for genforhandling beskrives i Bilag D, herunder evt. aftaler vedr. tidsperiode mellem genforhandlinger.

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 Databehandleren i overensstemmelse med Bestemmelse 10.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

14 Kontaktpersoner/kontaktpunkter hos Databehandleren og Underdatabehandleren vedr. Underdatabehandleraftalen

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter:

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Databehandleren:		Underdatabehandleren:	MedCom
Navn:		Navn:	Peder Illum
Stilling:		Stilling:	Sikkerhedsansvarlig
Telefon:		Telefon:	29263654
E-mail:		E-mail:	pi@medcom.dk
Afdeling:		Afdeling:	Systemforvaltning
Evt. funktionspostkasse:		Evt. funktionspostkasse:	sdn@medcom.dk

15 Underskrift

På vegne af Databehandleren:		På vegne af Underdatabehandleren:	
Navn:		Navn:	Lars Hulbæk
Stilling:		Stilling:	Direktør
Dato:		Dato:	
Underskrift:		Underskrift:	

Bilag A Oplysninger om behandlingen

BEMÆRK: I TILFÆLDE AF FLERE BEHANDLINGSAKTIVITETER, SKAL DISSE OPLYSNINGER FREMGÅ FOR HVER ENKELT BEHANDLINGSAKTIVITET.

A1. Formålet med Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren er:

Databehandlingen består i transport af personoplysninger mellem og for både offentlige og private parter i den danske sundhedssektor.

Transporten sker i Sundhedsdatanettet (SDN), et lukket, krypteret og virtuelt netværk, som består af en netværksinfrastruktur og en række støttesystemer.

Instruks for transport af personoplysninger i SDN sker gennem aftaler i støttesystemet aftalesystemet, hvori de Dataansvarlige eller Databehandleren selv forvalter og administrerer services, klienter, brugere samt aftaler om transport.

Underdatabehandleren er kontraktholder og fællesoffentlig systemforvalter for SDN.

A2. Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige drejer sig om (karakteren af behandlingen)

Underdatabehandleren hoster, drifter, vedligeholder, overvåger og supporterer SDN gennem dennes Underdatabehandlere.

Underdatabehandleren transporterer personoplysninger på baggrund af den Dataansvarliges instruks. Konfiguration af transport af personoplysninger i SDN sker automatisk i overensstemmelse med den segmentering, som indgåelsen af aftaler i aftalesystemet resulterer i.

Underdatabehandleren behandler personoplysninger om aftalesystemets brugere for, at brugerne kan være oprettet og have adgang til aftalesystemet, hvori de Dataansvarlige eller Databehandleren selv administrerer og forvalter oprettelse, nedlæggelse, vedligeholdelse og dokumentation af services, klienter og aftaler om adgange til udstillede services i SDN.

Underdatabehandleren behandler personoplysninger om aftalesystemets brugere for at understøtte sikkerheden med logning.

Underdatabehandleren behandler personoplysningerne om brugerne i aftalesystemet for udsendelse af servicemeddelelser om drift og vedligehold af SDN.

Underdatabehandleren modtager alarmer om anomalier i overvågningen af SDN.

Underdatabehandleren foretager sletning i samarbejde med dennes Underdatabehandler ved nedlæggelse af en tilslutning på SDN.

Underdatabehandler bistår dennes Underdatabehandler med at løse supporthenvendelser for SDN.

Som fællesoffentlig systemforvalter leverandørstyrer Underdatabehandleren i forbindelse med levering af SDN til den Dataansvarlige.

A3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

I SDN behandles almindelige, fortrolige og følsomme personoplysninger, herunder helbredsoplysninger.

I aftalesystemet behandles almindelige personoplysninger i form af navn, organisatorisk tilhørsforhold, mobiltelefon, arbejdsmail, logning af adfærd i aftalesystemet.

A4. Behandlingen omfatter følgende kategorier af registrerede:

I SDN behandles følgende kategorier af registrerede: Patienter, borgere og sundhedspersoner.

I aftalesystemet behandles følgende kategorier af registrerede: Brugere i aftalesystemet – dvs. teknisk og administrativt personale hos den Dataansvarlige.

A5. Underatabehandlerens behandling af personoplysninger på vegne af Databehandleren kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

Databehandlingens varighed følger den indgåede tilslutningsaftale for SDN.

Bilag B Underdatabehandlere

Ved Bestemmelsernes ikrafttræden har Databehandleren godkendt brugen af nedennævnte Underdatabehandlere for den beskrevne behandlingsaktivitet. Underdatabehandleren må ikke – uden Databehandlerens skriftlige godkendelse – gøre brug af en Underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden Underdatabehandler til denne behandlingsaktivitet.

Der udfyldes ét bilag pr. Underdatabehandler. Hvis der er mere end en underdatabehandler, bruges den skabelon til bilag B, som findes sammen med databehandlerskabelonen.

Virksomhedens fulde navn	Nuuday – TDC Erhverv A/S
CVR-nummer (eller tilsvarende)	40075291
Virksomhedens adresse (inkl. land)	Teglholmsgade 1, 2450 København SV
Øvrige adresser hvorfra der behandles personoplysninger (hvis relevant	Den præcise adresse er af sikkerhedsmæssige grunde fortrolig, men kan på anmodning til sdn@medcom.dk oplyses.
Kontaktperson hos Underdatabehandler	*dpo@nuuday.dk*
Har Underdatabehandleren en aftale med Underdatabehandleren, som opfylder kravene i Databehandleraftalen?	Ja
Databehandling(er), som Underdatabehandler deltager i	Databehandlerens opgave består i at hoste, drifte, vedligeholde, overvåge, forvalte og supportere SDN.
Kategorier af personoplysninger som Underdatabehandler behandler	Samme som under punkt A3.

Lokalitet for databehandlingen	Data behandles på lokationer på dedikerede servere beliggende inden for EU/EØS. De præcise adresser er af sikkerhedsmæssige grunde fortrolige, men kan på anmodning oplyses. Medcom kan kontaktes for nærmere oplysninger på sdn@medcom.dk.
Overførsel af personoplysninger til tredjelande (udfyldes, hvis relevant)	
Foretager Underdatabehandleren Underdatabehandler behandling af personoplysninger i et tredjeland?	SDN kan levere tilslutning af udenlandske parter, herunder i usikre tredjelande. Udenlandske parter godkendes før tilslutning i MedComs styregruppe. Transporten af personoplysninger til en udenlandske part forudsætter aftale / instruks fra den Dataansvarlige. Det påhviler den Dataansvarlige at sikre, at der er et lovligt grundlag for overførsel af personoplysninger til usikre tredjelande.
Hvis ja, angiv samtlige tredjelande	N/A
Hvis ja, angiv overførselsgrundlaget (f.eks. en EUstandardkontrakt eller Binding Corporate Rules)	N/A
Hvis ja, angiv evt. supplerende organisatoriske eller tekniske sikkerhedsforanstaltninger (herunder kryptering samt opbevaring af krypteringsnøgle)	N/A

Databehandleren fremsender aftaler med Underdatabehandler(e) og yderligere relevant dokumentation, f.eks. dokumentation på pre-audit jf. Artikel 28 (1) på anmodning fra den Dataansvarlige.

Virksomhedens fulde navn	Netic A/S
CVR-nummer (eller tilsvarende)	CVR: 26762642
Virksomhedens adresse (inkl. land)	Alfred Nobels Vej 27, 9220 Aalborg Ø, Danmark
Øvrige adresser hvorfra der behandles personoplysninger (hvis relevant	Den præcise adresse er af sikkerhedsmæssige grunde fortrolig, men kan på anmodning til sdn@medcom.dk oplyses.
Kontaktperson hos Underdatabehandler	DPO@netic.dk
Har Databehandleren en aftale med Underdatabehandleren, som opfylder kravene i Databehandleraftalen?	Ja
Databehandling(er), som Underdatabehandler deltager i	Underdatabehandlerens opgave består i at hoste, drifte, vedligeholde, overvåge og supportere SDN.
Kategorier af personoplysninger som Underdatabehandler behandler	Samme som under punkt A3.
Lokalitet for databehandlingen	Data behandles på lokationer på dedikerede servere beliggende inden for EU/EØS. De præcise adresser er af sikkerhedsmæssige grunde fortrolige, men kan på anmodning oplyses. Medcom kan kontaktes for nærmere oplysninger på sdn@medcom.dk.
Overførsel af personoplysninger til tredjelande (udfyldes, hvis relevant)	
Foretager Underdatabehandleren behandling af personoplysninger i et tredjeland?	SDN kan levere tilslutning af udenlandske parter, herunder i usikre tredjelande. Udenlandske parter godkendes før tilslutning i MedComs styregruppe.

	Transporten af personoplysninger til en udenlandske part forudsætter aftale / instruks fra den Dataansvarlige. Det påhviler den Dataansvarlige at sikre, at der er et lovligt grundlag for overførsel af personoplysninger til usikre tredjelande.
Hvis ja, angiv samtlige tredjelande	N/A
Hvis ja, angiv overførselsgrundlaget (f.eks. en EUstandardkontrakt eller Binding Corporate Rules)	N/A
Hvis ja, angiv evt. supplerende organisatoriske eller tekniske sikkerhedsforanstaltninger (herunder kryptering samt opbevaring af krypteringsnøgle)	N/A

Databehandleren fremsender aftaler med Underdatabehandler(e) og yderligere relevant dokumentation, f.eks. dokumentation på pre-audit jf. Artikel 28 (1) på anmodning fra den Dataansvarlige.

Virksomhedens fulde navn	KvalitetsIT A/S
CVR-nummer (eller tilsvarende)	38163264
Virksomhedens adresse (inkl. land)	Fiskergade 66, 1. sal, 8000 Århus C, Danmark
Øvrige adresser hvorfra der behandles personoplysninger (hvis relevant	N/A
Kontaktperson hos Underdatabehandler	peter@kvalitetsit.dk
Har Databehandleren en aftale med Underdatabehandleren, som opfylder kravene i Databehandleraftalen?	Ja
Databehandling(er), som Underdatabehandler deltager i	Underdatabehandlerens opgave består i vedligehold af programmel til aftalesystemet, herunder support og overvågning.
Kategorier af personoplysninger som Underdatabehandler behandler	I aftalesystemet behandles almindelige personoplysninger i form af navn, organisatorisk tilhørsforhold, mobiltelefon, arbejdsmail, logning af adfærd i aftalesystemet.
Lokalitet for databehandlingen	Data behandles på lokationer på dedikerede servere beliggende inden for EU/EØS. De præcise adresser er af sikkerhedsmæssige grunde fortrolige, men kan på anmodning oplyses. Medcom kan kontaktes for nærmere oplysninger på sdn@medcom.dk.
Overførsel af personoplysninger til tredjelande (udfyldes, hvis relevant)	
Foretager Underdatabehandleren behandling af personoplysninger i et tredjeland?	Nej

Hvis ja, angiv samtlige tredjelande	N/A
Hvis ja, angiv overførselsgrundlaget (f.eks. en EUstandardkontrakt eller Binding Corporate Rules)	N/A
Hvis ja, angiv evt. supplerende organisatoriske eller tekniske sikkerhedsforanstaltninger (herunder kryptering samt opbevaring af krypteringsnøgle)	N/A

Databehandleren fremsender aftaler med Underdatabehandler(e) og yderligere relevant dokumentation, f.eks. dokumentation på pre-audit jf. Artikel 28 (1) på anmodning fra den Dataansvarlige.

Bilag C Instruks vedr. behandling af personoplysninger

Hvis det aftales mellem parterne, at et eller flere af de oplistede sikkerhedskrav ikke skal efterleves eller efterleves på anden vis end beskrevet i Databehandlerinstruksen, indføjes dette i aftalens bilag D.

C.1 Behandlingens genstand/ instruks

Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren sker ved, at Underdatabehandleren udfører følgende:

Marker de databehandlinger, Underdatabehandleren varetager og beskriv den så konkret som muligt:

Databehandling	**Udføres**	**Beskrivelse af databehandling**
Indsamling		
Registrering		
Organisering/systematisering		
Opbevaring	X	Hosting, drift, vedligehold, backup
Tilpasning eller ændring	X	Tilpasning eller ændring af personoplysninger i aftalesystemet på foranledning af den Dataansvarlige.
Genfinding		
Søgning		
Brug	X	De almindelige personoplysninger i aftalesystemet bruges til support og udsendelse af servicemeddelelse om driften af SDN.
Videregivelse ved transmission	X	Hosting, drift, vedligehold
Formidling eller enhver anden form for overladelse		

Sammenstilling eller samkøring		
Begrænsning		
Sletning eller tilintetgørelse	X	Ved ophør af tilslutningsaftalen for SDN slettes personoplysningerne i aftalesystemet.
Leverandørstyring	X	Som fællesoffentlig systemforvalter leverandørstyrer Underdatabehandleren i forbindelse med levering af SDN til Databehandleren.
Support	X	De almindelige personoplysninger i aftalesystemet bruges til support.

C.2 Behandlingssikkerhed

C.2.1 Fastlæggelse af sikkerhedsniveau

C.2.1.1. Sikkerhedsniveauet skal afspejle kategorien og mængden af personoplysninger, der indgår i behandlingen:

Sikkerhedsniveauet afspejler, at der i SDN behandles følsomme og fortrolige personoplysninger.

C.2.1.2 Underdatabehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Underdatabehandleren skal evaluere og forbedre effektiviteten af sådanne forholdsregler, når det er nødvendigt.

C2.1.3 Underdatabehandleren skal understøtte Databehandleren 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.
Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

i. Pseudonymisering og kryptering af personoplysninger
ii. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester

iii. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
iv. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

C2.1.4 Databehandling omfattet af Underdatabehandleraftalen skal ske i overensstemmelse med denne instruks.

C2.1.5 Denne instruks afspejler, hvad der er gældende på tidspunkt for underskrift af Underdatabehandleraftalen. Såfremt der sker ændringer i forholdene, herunder i det af Underdatabehandleren udfyldte, skal Databehandleren orienteres.

C2.1.6 Instruksen er en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Underdatabehandleren minimum har ansvar for at gennemføre, overholde og sikre overholdelse af hos denne og dennes Underdatabehandlere. Eventuelle aftaler mellem Databehandleren og Underdatabehandleren om fravigelse eller delvis fravigelse af et eller flere af nedenstående krav dokumenteres i bilag D.

C2.1.7 Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger er nødvendige for at sikre efterlevelse af Underdatabehandleraftalens kapitel 5, skal sådanne foranstaltninger altid træffes. Supplerende sikringsforanstaltninger angives i bilag D.

C2.1.8 Underdatabehandleren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger og som dermed opfylder Databeskyttelsesforordningens artikel 32. Foranstaltningerne fastlægges ud fra overvejelser om:

i. Hvad der kan lade sig gøre rent teknisk
ii. Implementeringsomkostningerne
iii. Den pågældende behandlings karakter, omfang, sammenhæng og formål
iv.c Konsekvenserne for den registreredes rettigheder ved et sikkerhedsbrud
v. Den risiko, der er forbundet med behandlingerne, jf. punkt C.2.1.3

C.2.2 Pseudonymisering og kryptering

C2.2.1 Der må kun etableres eksterne kommunikationsforbindelser, hvis forbindelsen er krypteret f.eks. til webside, front-ends og loginportaler. Dette gælder også forbindelser til underleverandøren f.eks. site-to-site forbindelse eller IP-filtrering.
Ved fortrolige og følsomme personoplysninger forventes der en stærk kryptering. HTTPS og nyeste version af TLS er et krav. Efterlevelse af kravet skal f.eks. beskrives i afsnit C2.2.4 nedenfor.

C2.2.2 E-mails indeholdende fortrolige og følsomme personoplysninger skal også være beskyttet af kryptering.

C2.2.3 Hvis der er krav fra Databehandleren om kryptering af data ved lagring (data at rest) skal dette beskrives i bilag D.

C2.2.4 Databehandlerens beskrivelse af dennes efterlevelse af kravene i afsnit C2.2, hvis relevant for behandlingen af personoplysninger i henhold til Underdatabehandleraftalen:

Kryptering af transport i SDN sker med minimum TLS 1.3. Kryptering af forbindelse til aftalesystemet sker med minimum TLS 1.3. Aftalesystemet er kun tilgængeligt via SDN.

C.2.3 Uddannelse og instruktion

C2.3.1 Der stilles krav om, at alle ansatte hos Underdatabehandleren modtager den tilstrækkelig uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Underdatabehandlerens og Databehandlerens politikker og procedurer herfor.

C.2.4 Autorisation og adgangskontrol, herunder kontrol med afviste adgangsforsøg

C2.4.1 Der skal gennemføres styring af den generelle adgang til personoplysninger.

C2.4.2 Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har brug for.

C2.4.3 Der gennemføres begrænsninger i adgangen til systemer og personoplysninger, der behandles i henhold til Underdatabehandleraftalen, ved at definere brugerroller, for så vidt det er muligt og ved at tildele privilegerede adgangsrettigheder samt at udføre attestering af brugere.
Underdatabehandleren skal træffe foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, som den pågældende er autoriseret til.

C2.4.4 Der skal foreligge oversigt/dokumentation over de enkelte medarbejderes rettigheder til de individuelle systemer og personoplysninger, der behandles i henhold til Underdatabehandleraftalen

C2.4.5 Der skal gøres brug af sikre adgangskoder/passwords og autentifikation – samt multifaktorautentifikation ved adgang fra det åbne internet – eller tilsvarende sikkerhedsniveau, ved adgang til systemer eller personoplysninger, der behandles i henhold til Underdatabehandleraftalen.

C2.4.6 Underdatabehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

C2.4.7 Der skal løbende foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have. Denne kontrol kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, så det kan konstateres, om udstedte adgange og autorisationer fortsat anvendes. Frekvens for kontrollen skal fastlægges på baggrund af risikovurderingen og beskrives i punkt C2.4.13

C2.4.8 Underdatabehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for brugere, der efter en konkret vurdering ikke længere bør have disse.

C2.4.9 Der skal foretages registrering af alle afviste adgangsforsøg, når der behandles fortrolige og/eller følsomme personoplysninger. Underdatabehandleren skal løbende foretage opfølgning på afviste adgangsforsøg

C2.4.10 Hvis en risikovurdering tilsiger det, kan der fastlægges krav om blokering af forsøg på login fra samme arbejdsstation eller med samme brugeridentifikation Efter et nærmere fastlagt antal forsøg, afhængig af sikkerhedsniveau og andre sikkerhedsforanstaltninger. Evt. krav til blokering beskrives i afsnit C2.4.13.,

C2.4.11 Ved genåbning af adgange, skal der foreligge dokumentation/en beskrivelse af på hvilken baggrund genåbning er sket, og om der sendes besked til Databehandleren ved blokeret adgangsforsøg.

C2.4.12 Autoriserede personer skal kunne fremvise billed-ID ved on-site databehandling hos den Dataansvarlige.

C2.4.13 Underdatabehandlerens beskrivelse af dennes efterlevelse af kravene i afsnit C2.4, hvis relevant for behandlingen af personoplysninger i henhold til Underdatabehandleraftalen:

Databehandleren er selv ansvarlig for autorisation, oprettelse, tildeling af rettigheder og kontrol af adgang for egne medarbejdere til aftalesystemet.

Aftalesystemet stiller information til rådighed for Databehandleren for kontrol af rettigheder og anvendelse af aftalesystemet.

Underdatabehandler og dennes Underdatabehandlere er hver især ansvarlige for autorisation, oprettelse, tildeling af rettigheder og kontrol af adgang for egne medarbejdere til SDN og aftalesystemet.

Underdatabehandlerens Underdatabehandleres autoriserede brugere gennemgås på fælles driftsmøder.

Underdatabehandler og dennes Underdatabehandlere attesterer sine medarbejderes adgang hvert halve år.

Der foretages overvågning og kontrol med afviste adgangsforsøg. Adgange blokeres efter 5 fejlede loginforsøg.

Adgang sker med multifaktor-autentifikation.

C.2.5 Genoprettelse af tilgængelighed i tilfælde af fysisk eller teknisk hændelse (back up og håndtering af driftsafbrydelser)

C2.5.1 Der gælder de samme retningslinjer for backup som for al anden behandling af personoplysninger, der behandles i henhold til Underdatabehandleraftalen.

C2.5.2 Underdatabehandleren skal sikre, at der foretages regelmæssig backup af systemer og personoplysninger, der behandles i henhold til Underdatabehandleraftalen.

C2.5.3 Backup skal opbevares adskilt fra serveren i et ikke tilstødende rum for at sikre, at denne ikke går tabt. Backup skal beskyttes og opbevaring af backup skal altid ske på betryggende vis så denne ikke fortabes.

C2.5.4 Underdatabehandleren skal regelmæssigt kontrollere, at backup er læsbart. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af et systems tekniske setup.

C2.5.5 Underdatabehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.

C2.5.6 Underdatabehandleren skal regelmæssigt afprøve og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af itberedskabsøvelser. Databehandleren kan anmode om at få dokumentation for dette stillet til rådighed.

C2.5.7 Underdatabehandlerens beskrivelse af dennes efterlevelse af afsnit C2.5, hvis relevant for den af Underdatabehandleraftalen omfattede behandling af personoplysninger:

Personoplysninger, der transporteres i SDN, gemmes ikke. Der tages backup af aftalesystemet. Backuppen opbevares på en anden geografisk lokation. Den præcise adresse er af sikkerhedsmæssige grunde fortrolig, men kan på anmodning til sdn@medcom.dk oplyses.

C.2.6 Opdateringer og ændringer

C2.6.1 Underdatabehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

C2.6.2 Underdatabehandleren 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.

C.2.7 Fysisk sikring

C2.7.1 Underdatabehandleren skal sikre, at it-udstyr, der anvendes i forbindelse med databehandlingen, er fysisk sikret i henhold til gældende lovkrav.

C2.7.2 Underdatabehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Underdatabehandleren skal desuden evaluere og forbedre effektiviteten af sådanne forholdsregler, hvor det er nødvendigt.

C2.7.3 Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares med tilstrækkelig stærk kryptering under opsyn eller under lås, når de ikke benyttes.

C2.7.4 Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.

C2.7.5 Der skal føres en fortegnelse over, hvilke mobile lagringsmedier der benyttes i forbindelse med databehandlingen.

C2.7.6 Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af mobile lagringsmedier.

C2.7.7 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.

C2.7.8 Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller afmagnetiseres, 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, når den Dataansvarlige anmoder herom

C.2.8 Anvendelse af hjemme-/ad hoc-arbejdspladser

C2.8.1 Hvis Underdatabehandleren ikke må anvende ad hoc-arbejdspladser i forbindelse med databehandlingen, skal dette aftales mellem parterne og angives i bilag D.

C2.8.2 Ved anvendelse af hjemme-/Ad hoc-arbejdspladser skal der anvendes fler-faktor-login (Multifactorautentifikation) eller tilsvarende sikkerhedsniveau samt hensynstagen til time-out.

C2.8.3 Underdatabehandleren og dennes autoriserede medarbejdere må foretage databehandling fra mobile arbejdspladser, herunder med adgange til den Dataansvarliges personoplysninger over internettet, såfremt databehandlingen sker fra arbejdspladser, som er underlagt Underdatabehandlerens egne sikkerhedsregler. Databehandlingen skal endvidere ske i overensstemmelse med Underdatabehandleraftalen og denne instruks.

C2.8.4 Hjemme-/Ad hoc-arbejdspladserne skal være sikret med tekniske kontroller, der sikrer, at behandlingen af personoplysninger sker i overensstemmelse med gældende lovgivning og den Dataansvarliges, Databehandlerens og Underdatabehandlerens retningslinjer.

C2.8.5 Det skal sikres, at uvedkommende ikke får adgang til personoplysninger, der behandles ved hjemmearbejdspladser, ligesom de enkelte medarbejdere skal instrueres i, hvordan uvedkommende ikke får adgang.

C2.8.6 Underdatabehandlerens beskrivelse af dennes efterlevelse af afsnit C2.8, hvis relevant for den af Underdatabehandleraftalen omfattede behandling af personoplysninger:

Fjernadgang til SDN sker via minimum AES256-bit-krypteret VPN-adgang med multifaktor-autentifikation. Inaktive brugersessioner i aftalesystemet lukkes efter 15 minutter.

C.2.9 Logning

C2.9.1 Der skal som udgangspunkt foretages maskinel registrering (logning) ved behandling af personoplysninger. Krav til logning og indhold af loggen fastlægges på baggrund af risikovurderingen samt eventuelle lovkrav og omfang af den aftalte logning beskrives i C2.9.3

C2.9.2 Loggen skal opbevares i den periode, der aftales mellem Databehandleren og Underdatabehandleren under hensyn til eventuelle lovkrav. Aftale om opbevaringsperiode samt udlevering af logoplysninger til Databehandleren beskrives i afsnit C2.9.3

C2.9.3 Underdatabehandlerens beskrivelse af dennes efterlevelse af afsnit C2.9, hvis relevant for den af Underdatabehandleraftalen omfattede behandling af personoplysninger:

Brugerhandlinger i aftalesystemet dokumenteres i en hændelseslog, som slettes efter 2 år. Loggen er tilgængelig for Databehandleren for opfølgning på egne autoriserede medarbejderes handlinger jf. egne politikker.

Underdatabehandleren har etableret logning på alt aktivt netværksudstyr i SDN. Logningen omfatter en log over anvendelsen af privilegerede konti på aktivt netværksudstyr, herunder navn, start og slut tidspunkt samt formålet med brugen af den privilegerede konto.

Underdatabehandleren foretager overvågning af og reagerer på uautoriserede forespørgsler i loggen - samt foretager overvågning af loggen i forhold til identificering af misbrug af SDN.

Underdatabehandleren opbevarer transaktionsloggen på Underdatabehandlerens adgang til SDN i 2 år.

Driftslog uden personoplysninger opbevares i 5 år til brug ved opfølgning/undersøgelse af evt. ulovlige eller kriminelle handlinger

Alle logs er beskyttet mod uautoriseret adgang, manipulation og tekniske fejl.

C.2.10 Tilsyn

C2.10.1 Underdatabehandleren skal føre og dokumentere et tilsyn med Underdatabehandlerens organisations overholdelse af lovkrav, politikker, procedurer og denne Underdatabehandleraftale med bilag.

C.2.11 Underretning

C2.11.1 Ved brud på persondatasikkerheden skal Databehandleren uden unødig forsinkelse skriftligt orienteres på nedenstående adresse, således at den Dataansvarlige kan indberette bruddet til Datatilsynet og om nødvendigt underrette de registrerede. Underretningen skal ske til:

E-mailadresse og evt. telefonnummer til kontakt hos Databehandleren: Sikkerhedsansvarlig kontaktperson fra tilslutningsaftalen for SDNv4 *Orientering af Databehandleren skal ske inden for [angiv tidsperiode]: Underd*atabehandleren underretter uden unødigt ophold Databehandleren efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden. Underdatabehandlerens underretning til Databehandleren skal ske uden unødigt ophold dog senest 24 timer efter, at denne er blevet bekendt med bruddet, således at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed jf. Databeskyttelsesforordningens artikel 33.

C3. Bistand til den Dataansvarlige

Underdatabehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå Databehandleren og den Dataansvarlige i overensstemmelse med Underdatabehandleraftalens Bestemmelser 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Underdatabehandleren opretholder i sin interne organisation passende politikker og procedurer, som understøtter, at Underdatabehandleren er i stand til at leve op til sine forpligtelser som Underdatabehandler, herunder ift. at kunne bistå Databehandleren og den Dataansvarlige på en måde som understøtter den Dataansvarliges iagttagelse af de frister, som følger af gældende databeskyttelsesretlig lovgivning.

C4 Opbevaringsperiode og sletterutiner

Personoplysninger transporteret i SDN gemmes ikke. Personoplysninger i aftalesystemet oprettes og slettes af Databehandleren selv. Personoplysninger opbevares, så længe opbevaringen er nødvendig til opfyldelse af databehandlingens formål.

Ved ophør af tilslutning til SDN, sletter Underdatabehandler personoplysningerne om Databehandleren i aftalesystemet. Personoplysningerne vil fortsat fremgå af hændelsesloggen, som slettes efter 2 år.

Hændelseslog fra den underliggende netværksinfrastruktur i SDN, som alene indeholder persondata om Underdatabehandlerens og evt. Underdatabehandleres medarbejdere, skal opbevares i 2 år til brug ved opfølgning/undersøgelse af evt. ulovlige eller kriminelle handlinger.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal Underdatabehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med Bestemmelse 10.1, medmindre Databehandleren – efter underskriften af disse Bestemmelser – har ændret Databehandlerens oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

C.5 Lokalitet for behandling

C5.1 Behandling af personoplysninger, omfattet af Underdatabehandleraftalen, kan ikke ske på andre lokaliteter end de her listede samt, såfremt der anvendes andre Underdatabehandlere, de lokaliteter, der fremgår af Bilag B uden Databehandlerens forudgående skriftlige godkendelse:

Virksomhed	**Rolle (Underdatabehandler)**	**Adresse**	**Typen af databehandling, virksomheden foretager**
MedCom	Databehandler	Forskerparken 10, 5230 Odense M	Support.
Nuuday – TDC Erhverv A/S	Underdatabehandler	Teglholmsgade 1, 2450 København SV	Hosting, drift, vedligehold, backup, overvågning, support.
Netic A/S	Underdatabehandler	Alfred Nobels Vej 27 9220 Aalborg Ø Danmark	Hosting, drift, vedligehold, backup, overvågning, support.

KvalitetsIT ApS	Underdatabehandler	Fiskergade 66, 1.sal 8000 Århus C Danmark	Vedligehold af programmel til aftalesystemet, herunder support og overvågning.

C.6 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande

1. Godkendelse af overførsel og evt. specifik instruks vedr. overførsel af personoplysninger til tredjeland eller international organisation skal fremgå af bilag D.

2. Hvis den Dataansvarlige eller Databehandleren ikke i bilag D eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af
personoplysninger til et tredjeland, må Underdatabehandleren ikke inden for rammerne af Underdatabehandleraftalen foretage en sådan overførsel.

Anfør overførselsgrundlag efter databeskyttelsesforordningens kapitel 5 i nedenstående tabel:

	Sæt kryds
Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet (artikel 45)	
EU-standardkontrakten	
Bindende virksomhedsregler (artikel 47)	
Overførsel eller videregivelse uden hjemmel i EU-retten (artikel 48)	
Særlige forhold (Artikel 49) Angiv hvilke:	

C.7 Den Dataansvarliges tilsyn med den behandling, som foretages hos Databehandleren og Underdatabehandlere

C7.1 Databehandlerens tilsyn med Underdatabehandleren fastlægges ud fra en risikovurdering. I vurderingen af tilsynsformen skal der tages hensyn til omfanget af personoplysninger og deres følsomhed, evt. lovgivningsmæssige krav samt hvor kritisk databehandlingen er for organisationens opgaveløsning.

C7.2 Tilsynet gennemføres som udgangspunkt årligt og tidspunkt anføres nedenfor.

C7.3 Typen af tilsyn, herunder evt. typen af revisionserklæring, aftales mellem parterne og anføres nedenfor.

C7.4 Baseret på resultatet af tilsynet skal Underdatabehandleren iværksætte evt. yderligere foranstaltninger, hvis dette er nødvendigt for at efterleve kravene i denne Underdatabehandleraftale.

C7.5 Underdatabehandleren er forpligtet til at føre tilsyn med evt. andre Underdatabehandlere. Den valgte form for tilsyn med disse Underdatabehandlere skal være godkendt af Databehandleren. Efter anmodning fra Databehandleren skal dokumentation for tilsynet fremsendes til Databehandleren.

C7.6 Databehandleren kan beslutte, at der som supplement skal være adgang for Databehandleren eller en repræsentant at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra Underdatabehandleren eller evt. Andre Underdatabehandlere foretager behandling af personoplysninger.

Underdatabehandleren vil årligt på eget initiativ og regning få gennemført en ISAE3000-erklæring af uafhængig revisor for at kunne dokumentere overholdelse af Databeskyttelsesloven og GDPR. Erklæringen dokumenterer desuden overholdelse af udvalgte relevante sikkerhedskrav til SDN og aftalesystemet. Erklæringen er møntet på det specifikke forhold mellem Underdatabehandleren og Databehandleren. Erklæringen fremsendes til Databehandleren.

Det er Databehandlerens ansvar at vurdere, om erklæringen er tilstrækkelig til at opfylde Databehandleren og den Dataansvarliges tilsynsbehov.

Underdatabehandleren vil årligt og på eget initiativ indhente og behandle erklæringer fra andre Underdatabehandlere.

Databehandleren eller den Dataansvarlige skal selv afholde omkostningerne ved yderligere auditering, herunder Underdatabehandleres medvirken – med undtagelse af, hvis en auditering kommer på baggrund af brud på persondatasikkerheden, anmærkninger i revisionserklæringer eller andre objektivt konstaterbare forhold.

Bilag D Parternes regulering af andre forhold

D1 Governance

Kravene til SDN fastsættes af MedComs styregruppe, og Databehandleren kan ikke selvstændigt stille krav til SDN. Hvis Databehandleren kræver specifikke foranstaltninger implementeret i SDN, uden at tilsvarende krav er vedtaget af MedComs styregruppe, skal sådanne foranstaltninger alene kunne implementeres på Databehandlerens regning.

I det omfang flere Databehandlere og/eller Dataansvarlige kræver de samme foranstaltninger, kan de pågældende Databehandlere og/eller Dataansvarlige dele omkostningerne til foranstaltningerne.

Sikkerhedspolitik mv. for SDN kan til enhver tid rekvireres hos MedCom.

D2 Sikkerhedsgodkendelse af medarbejdere

Databehandleren vil kunne kræve sikkerhedsgodkendelser af medarbejdere hos Underdatabehandleren eller dennes Underdatabehandlere. Underdatabehandleren eller dennes Underdatabehandlere skal stille sig til rådighed herfor.

Eventuelle udgifter hertil vil skulle afholdes af Databehandleren.

D3 Pligt til at informere den anden part

Underdatabehandleren skal:

a) Informere Databehandleren uden unødigt ophold om overvågnings-aktiviteter og foranstaltninger iværksat overfor Underdatabehandleren vedrørende oplysninger behandlet på vegne af Databehandleren i henhold til gældende lovgivning medmindre sådan lovgivning forbyder Underdatabehandleren at informere Databehandleren.
b) Informere Databehandleren, såfremt en registreret anlægger retssag mod Underdatabehandleren, jf. databeskyttelsesforordningens artikel 79.

Databehandleren:

c) Informere Underdatabehandleren uden unødigt ophold, hvis Databehandleren bliver opmærksom på et brud på persondatasikkerheden, som Underdatabehandleren potentielt har en rolle i.
d) Informere Underdatabehandleren, såfremt en registreret anlægger retssag mod Underdatabehandleren, jf. databeskyttelsesforordningens artikel 79.

D4 Lovvalg og værneting

Enhver tvist og ethvert krav, som måtte udspringe af disse Bestemmelser skal afgøres i overensstemmelse med bestemmelser om lovvalg og værneting i tilslutningsaftalen for SDN.

D5 Erstatningsansvar

Tilslutningsaftalens regulering om begrænsning af erstatningsansvar og skadesløsholdelse finder anvendelse på disse Bestemmelser - og intet i disse Bestemmelser skal tolkes som en udvidelse af erstatningsansvaret og skadesløsholdelsespligterne i tilslutningsaftalen for SDN. Underdatabehandlerens ansvar efter databeskyttelsesforordningens artikel 82 over for Databehandlerens eventuelle regreskrav, er tilsvarende begrænset i overensstemmelse med Tilslutningsaftalens regulering om skadesløsholdelse og begrænsning af ansvar.

D6 Regulering fra tilslutningsaftalen for SDN efter tilslutningsaftalens ophør

Hvis tilslutningsaftalen for SDN ophører før disse Bestemmelser, skal de følgende reguleringstemaer fra tilslutningsaftalen fortsat være gældende i relation til disse Bestemmelser, så længe Bestemmelserne gælder:

- Erstatningsansvar og begrænsning heraf
- Tilsyn/kontrol og compliance
- Økonomisk regulering, herunder ift. priser
- Roller og ansvar i relation til tredjeparter
- Fortrolighed
- Lovvalg og værneting
- Opsigelse og ophør

D7 Særligt vedrørende backups

Efter, at der er sket sletning i aftalesystemet i overensstemmelse med Kontrakten og punkt 10 i Bestemmelserne, vil sletning i backups ske ved udløbet af den fastsatte retention-periode for den pågældende backup. Denne vil fremgå af driftshåndbogen.

D8 Sikker konfiguration og beskyttelse mod malware

Underdatabehandleren sikrer gennem dennes Underdatabehandlere vedligeholdelse af software/firmware og konfigurationer - samt i relevant omfang vedligeholdelse af anti-malware og antivirus.

D9 Netværkssikkerhed

Der anvendes IDS/IPS-funktionalitet i SDN, og der gennemføres månedlige sårbarhedsskanninger.

D10 Overvågning

Underdatabehandleren overvåger SDN gennem dennes Underdatabehandlere, så de kan reagere på afbrydelser af og forhindre afbrydelser, på baggrund af overskridelse af grænseværdier.

D11 Ændringer

Genforhandling af vilkårene i Underdatabehandleraftalen sker i den governance, der er aftalt for SDN.