Databehandleraftale

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

Mellem den dataansvarlige:

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

Og Databehandleren:

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.

Indholdsfortegnelse

Indhold

1 Præambel

1. Disse Bestemmelser fastsætter Databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den Dataansvarlige.

2. Disse Bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af:

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

4. Databehandleren behandler personoplysninger på vegne af den Dataansvarlige 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 den Dataansvarliges betingelser for Databehandlerens brug af Underdatabehandlere og en liste af Underdatabehandlere, som den Dataansvarlige har godkendt brugen af.

9. Bilag C indeholder den Dataansvarliges instruks for så vidt angår Databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som Databehandleren som minimum skal gennemføre, hvordan Databehandleren bistår den

Dataansvarlige samt hvordan der føres tilsyn med Databehandleren og eventuelle 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 Databehandleren fra forpligtelser, som Databehandleren 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 Databehandleren instrueres i at foretage.

3 Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den Dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

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. Databehandleren må kun give adgang til personoplysninger, som behandles på den Dataansvarliges vegne, til personer, som er underlagt Databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de pågældende personer, som er underlagt Databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

5 Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den Dataansvarlige og Databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.
   Den Dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

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

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

6 Anvendelse af Underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden Databehandler (en Underdatabehandler).
Databehandleren må således ikke gøre brug af en Underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående **specifik** eller **generel skriftlig godkendelse** fra den Dataansvarlige. Listen over Underdatabehandlere, som den Dataansvarlige allerede har godkendt, fremgår af bilag B.

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

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

3. Når Databehandleren gør brug af en Underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den Dataansvarlige, skal Databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EUretten eller medlemsstaternes nationale ret, pålægge Underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at Underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den Dataansvarliges anmodning herom – i kopi til den Dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt Underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af Underdatabehandleraftalen, skal ikke sendes til den Dataansvarlige.

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

7. Hvis Underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af Underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den Dataansvarlige og Databehandleren, herunder Underdatabehandleren.

7 Overførsel af oplysninger til tredjelande eller internationale organisationer

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

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Databehandleren ikke er blevet instrueret i at foretage af den Dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt, skal Databehandleren underrette den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den Dataansvarlige kan Databehandleren således ikke inden for rammerne af disse Bestemmelser:
    a. overføre personoplysninger til en Dataansvarlig eller Databehandler i et tredjeland eller en international organisation
    b. overlade behandling af personoplysninger til en Underdatabehandler i et tredjeland
    c. behandle personoplysningerne i et tredjeland

4. Den Dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

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

8 Bistand til den Dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den Dataansvarlige ved hjælp af passende tekniske og Organisatoriske foranstaltninger, med opfyldelse af den Dataansvarliges forpligtelse til at besvare

anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.
Dette indebærer, at Databehandleren så vidt muligt skal bistå den Dataansvarlige i forbindelse med, at den Dataansvarlige skal sikre overholdelsen af:

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. 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. Databehandleren bistår den Dataansvarlige med at sikre overholdelse af den Dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, jf. art 28, stk. 3, litra f.
Dette indebærer, at Databehandleren under hensyntagen til behandlingens karakter skal bistå den 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 Databehandlerens bistand til den Dataansvarlige vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

9 Underretning om brud på persondatasikkerheden

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

2. Databehandlerens underretning til den Dataansvarlige skal 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 den Dataansvarlige angives i bilag C.

3. I overensstemmelse med Bestemmelse 9.2. skal Databehandleren bistå den Dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsyns-myndighed. Det betyder, at Databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
    c. de foranstaltninger, som den Dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

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

10 Sletning og tilbagelevering af oplysninger

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

2. Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med Databehandleren og Underdatabehandlere er nærmere angivet i Bilag C.7.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den Dataansvarliges eller Databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens 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 den Dataansvarlige i overensstemmelse med Bestemmelse 10.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

14 Kontaktpersoner/kontaktpunkter hos den Dataansvarlige og Databehandleren vedr. Databehandleraftalen

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

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

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

15 Underskrift

På vegne af den Dataansvarlige:		På vegne af Databehandleren:	
Navn:	*Skrivefelt*	Navn:	Lars Hulbæk
Stilling:	*Skrivefelt*	Stilling:	Direktør
Dato:	*Skrivefelt*	Dato:	*Skrivefelt*
Underskrift:	*Skrivefelt*	Underskrift:	*Skrivefelt*

Bilag A Oplysninger om behandlingen

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

A1. Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige 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 selv forvalter og administrerer services, klienter, brugere samt aftaler om transport.

Databehandleren er kontraktholder og fællesoffentlig systemforvalter for SDN.

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

Databehandleren hoster, drifter, vedligeholder, overvåger og supporterer SDN gennem Underdatabehandlere.

Databehandleren 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.

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

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

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

Databehandleren modtager alarmer om anomalier i overvågningen af SDN.

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

Databehandler bistår Underdatabehandleren med at løse supporthenvendelser for SDN.

Som fællesoffentlig systemforvalter leverandørstyrer Databehandleren 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. Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige 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 den Dataansvarlige godkendt brugen af nedennævnte Underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den Dataansvarliges skriftlige godkendelse – gøre brug af en Underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden Underdatabehandler til denne behandlingsaktivitet.

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	*Udfyldes med indgåelse af kontrakt med ny SDN-leverandør*
CVR-nummer (eller tilsvarende)	*Udfyldes med indgåelse af kontrakt med ny SDN-leverandør*
Virksomhedens adresse (inkl. land)	*Udfyldes med indgåelse af kontrakt med ny SDN-leverandør*
Øvrige adresser hvorfra der behandles personoplysninger (hvis relevant	*Udfyldes med indgåelse af kontrakt med ny SDN-leverandør*
Kontaktperson hos Underdatabehandler	*Udfyldes med indgåelse af kontrakt med ny SDN-leverandør*
Har Databehandleren 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 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.

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

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker ved, at Databehandleren udfører følgende:

Marker de databehandlinger, databehandleren 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 Databehandleren i forbindelse med levering af SDN til den Dataansvarlige.
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 Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal evaluere og forbedre effektiviteten af sådanne forholdsregler, når det er nødvendigt.

C2.1.3 Databehandleren skal understøtte den Dataansvarlige i dennes arbejde med at dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau og gennemføre de foranstaltninger, der er nødvendige for at imødegå identificerede risici.
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 Databehandleraftalen skal ske i overensstemmelse med denne instruks.

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

C2.1.6 Instruksen er en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren minimum har ansvar for at gennemføre, overholde og sikre overholdelse af hos denne og dennes Underdatabehandlere. Eventuelle aftaler mellem den Dataansvarlige og Databehandleren 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 Databehandleraftalens kapitel 5, skal sådanne foranstaltninger altid træffes. Supplerende sikringsforanstaltninger angives i bilag D.

C2.1.8 Databehandleren 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 den Dataansvarlige 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 Databehandleraftalen:

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 Databehandleren 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.

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 Databehandleraftalen, ved at definere brugerroller, for så vidt det er muligt og ved at tildele privilegerede adgangsrettigheder samt at udføre attestering af brugere.
Databehandleren 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 Databehandleraftalen

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 Databehandleraftalen.

C2.4.6 Databehandleren 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 Databehandleren 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. Databehandleren 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 den Dataansvarlige ved blokeret

adgangsforsøg.

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

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

Den Dataansvarlige er selv ansvarlig for autorisation, oprettelse, tildeling af rettigheder og kontrol af adgang for egne medarbejdere til aftalesystemet. Aftalesystemet stiller information til rådighed for den Dataansvarlige for kontrol af rettigheder og anvendelse af aftalesystemet. Databehandler og Underdatabehandler er hver især ansvarlige for autorisation, oprettelse, tildeling af rettigheder og kontrol af adgang for egne medarbejdere til SDN og aftalesystemet. Underdatabehandlerens autoriserede brugere gennemgås på fælles driftsmøder. Databehandler og Underdatabehandleren 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 Databehandleraftalen.

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

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

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

C2.5.7 Databehandlerens beskrivelse af dennes efterlevelse af afsnit C2.5, hvis relevant for den af Databehandleraftalen 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 Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

C2.6.2 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.

C.2.7 Fysisk sikring

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

C2.7.2 Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren 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 Databehandleren 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 Databehandleren 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 Databehandlerens egne sikkerhedsregler. Databehandlingen skal endvidere ske i overensstemmelse med Databehandleraftalen 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 og Databehandlerens 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 Databehandlerens beskrivelse af dennes efterlevelse af afsnit C2.8, hvis relevant for den af Databehandleraftalen 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 den Dataansvarlige og Databehandleren under hensyn til eventuelle lovkrav. Aftale om opbevaringsperiode samt udlevering af logoplysninger til den Dataansvarlige beskrives i afsnit C2.9.3

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

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

Databehandleren har gennem Underdatabehandlere 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 Databehandleren skal føre og dokumentere et tilsyn med Databehandlerens organisations overholdelse af lovkrav, politikker, procedurer og denne Databehandleraftale med bilag.

C.2.11 Underretning

C2.11.1 Ved brud på persondatasikkerheden skal den Dataansvarlige 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 den Dataansvarlige: *Skrivefelt*

Orientering af den Dataansvarlige skal ske inden for [angiv tidsperiode]: Databehandleren underretter uden unødigt ophold Den Dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden. Databehandlerens underretning til Den Dataansvarlige 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

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

Databehandleren opretholder i sin interne organisation passende politikker og procedurer, som understøtter, at Databehandleren er i stand til at leve op til sine forpligtelser som Databehandler, herunder ift. at kunne bistå 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 den Dataansvarlige selv. Personoplysninger opbevares, så længe opbevaringen er nødvendig til opfyldelse af databehandlingens formål.

Ved ophør af tilslutning til SDN, sletter Databehandler personoplysningerne om den Dataansvarlige 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 Databehandlerens og evt. Underdatabehandlerens medarbejdere, skal opbevares i 2 år til brug ved opfølgning/undersøgelse af evt. ulovlige eller kriminelle handlinger.

Kommenterede [TGJ1]: OBS i revision

SDN-nettet ind igen med backup osv

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

C.5 Lokalitet for behandling

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

Virksomhed	**Rolle (Databehandler/Underdatabehandler)**	**Adresse**	**Typen af databehandling, virksomheden foretager**
Udfyldes med indgåelse af SDNv4-kontrakt	*Udfyldes med indgåelse af SDNv4-kontrakt*	*Udfyldes med indgåelse af SDNv4-kontrakt*	*Udfyldes med indgåelse af SDNv4-kontrakt*

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 ikke i bilag D eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må Databehandleren ikke inden for rammerne af Databehandleraftalen 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 Den Dataansvarliges tilsyn med Databehandleren 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 Databehandleren iværksætte evt. yderligere foranstaltninger, hvis dette er nødvendigt for at efterleve kravene i denne databehandleraftale.

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

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

Databehandleren 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 Databehandleren og den Dataansvarlig. Erklæringen fremsendes til den Dataansvarlig.

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

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

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 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.

D2 Sikkerhedsgodkendelse af medarbejdere

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

Eventuelle udgifter hertil vil skulle afholdes af den Dataansvarlige.

D3 Pligt til at informere den anden part

Databehandleren skal:

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

Den Dataansvarlige skal:

c) Informere Databehandleren uden unødigt ophold, hvis den Dataansvarlige bliver opmærksom på et brud på persondatasikkerheden, som Databehandleren potentielt har en rolle i.
d) Informere Databehandleren, såfremt en registreret anlægger retssag mod Databehandleren, 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. Databehandlerens ansvar efter databeskyttelsesforordningens artikel 82 over for den Dataansvarliges 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

Databehandleren sikrer gennem Underdatabehandler 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

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

D11 Ændringer

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

Godkendt i FSI 08-12-2021