**Databehandlerinstruks**

**Bilag A - Oplysninger om behandlingen**

Dette bilag udgør den Dataansvarliges instruks til Databehandleren vedrørende Databehandlerens databehandling på vegne af den Dataansvarlige i forbindelse med opfyldelse af parternes aftale af den xxx omhandlende hjemmeperitonealdialyse.

Bemærk: I tilfælde af flere behandlingsaktiviteter skal disse oplysninger fremgå for hver enkelt behandlingsaktivitet.

**A.1 Formålet med behandlingen, herunder hjemmelsgrundlag for Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige, er:**

|  |
| --- |
| Det overordnet FORMÅL med databehandlerens behandling er at opsamle og efterfølgende stille de opsamlede data til rådighed for den dataansvarlige. Ligesom formålet er, at den dataansvarlige via den teknologi, som stilles til rådighed, kan justere indstillingsværdierne individuelt for de enkelte patienter.  |

**A.2 Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker ved, at:**

Beskrivelse af dataflow, samt af hvem der gør hvad og hvordan i forbindelse med behandlingen.

|  |
| --- |
| Databehandlerens OPGAVE er at hoste, supportere, drifte og udvikle teknologien. Der sker således følgende behandlinger af data: samling, registrering, organisering, strukturering, opbevaring, tilpasning, ændring, hentning, sletning samt overførsel. Databehandlerens opgave er ved hjælp af telemedicinteknologien dagligt at opsamle behandlingsdata (personoplysninger) fra dialysemaskinen efter endt behandling hos patienten, og herefter stille de opsamlede behandlingsdata (personoplysninger) til rådighed for det kliniske personale via en WEB-portal. Det er databehandlerens opgave at udføre teknisk fejlfinding, firmware opdateringer og kvalitetssikring.  |

**A.3 Behandlingen omfatter følgende kategorier af registrerede personer:**

|  |
| --- |
| **Peritonealdialyse patienter**, der ønsker at foretage dialysebehandling i hjemmet eller på sygehuset i forbindelse med ambulatoriebesøg eller indlæggelse.**Klinisk personale,** der skal have adgang til teknologien. |

**A.4 Behandlingen omfatter følgende typer af personoplysninger:**

|  |
| --- |
| **For peritonealdialyse patienter** Navn, køn, adresse, telefonnummer, fødselsdato, ID-nummer, sprog og diabetisk statusIndstillings- og behandlingsværdier for dialysemaskinen, som for eksempel: Blodtryk, vægt, behandlingsdato, behandlingsdato, behandlingsmodus, ind- og udløbsvolumen, dialysetid, ultrafiltrationsvolumen og evt. alarmer opstået i behandlingen **For klinisk personale** Navn, e-mail, telefonnummer og afdelingsnavn, hændelsessporing (logdata) som for eksempel: indlogning, mislykket indlogning, ændring af patientinformation, visning af patientinformation, ændring af behandlingsværdier for dialysemaskinen**Herudover behandles** Data fra dialysebehandlingenIndstillinger for dialyseanordningenFejlkoder, fejlkodelister, teknisk data samt firmware opdateringer. Fejlkoder kan i visse tilfælde knyttes til patienten, hvorfor det kan være relevant for Databehandleraftalen.  |

**A.5 Lokalitet for behandling af personoplysninger og geografisk placering:**

Behandlingen af personoplysninger, omfattet af Hovedaftalen, kan ikke ske på andre lokaliteter end de følgende uden den Dataansvarliges forudgående skriftlige samtykke.

|  |
| --- |
| Data (personoplysningerne) opbevares i datacenter i EU/EØS. [*her indtastes adresserne på samtlige lokaliteter*.] |

**A.6 Ikrafttræden, varighed og ophør:**

|  |
| --- |
| Databehandleraftalen træder i kraft ved begge parters underskrift af aftalen. Jf. databehandleraftalens punkt 10. |

**A.7 Tilbagelevering og sletning af personoplysninger:**

A.7.1 Ved ophør af behandlingen af personoplysningerne omfattet af denne databehandleraftale, er Databehandleren forpligtet til at:

|  |  |
| --- | --- |
|  | Sæt kryds |
| Slette alle personoplysninger, der er blevet behandlet på vegne af den Dataansvarlige og bekræfte over for den Dataansvarlige, at oplysningerne er slettet.  | X |
| ~~Tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.~~  |  |

A.7.2 Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

|  |
| --- |
| [udfyld hvis relevant] |

Databehandleren forpligter sig alene til at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

**Bilag B - Underdatabehandlere**

Den Dataansvarlige har ved Databehandleraftalens ikrafttræden godkendt brugen af nedenstående Underdatabehandlere for den beskrevne behandlingsaktivitet.

Databehandleren må ikke gøre brug af en Underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden Underdatabehandler til denne behandlingsaktivitet, jf. punkt B.4.

*Der udfyldes ét bilag pr. Underdatabehandler.*

**B.1. Godkendte Underdatabehandlere**

|  |  |
| --- | --- |
| Virksomhedens fulde navn CVR-nummer (eller tilsvarende). |  |
| Virksomhedens adresse (inkl. land).  |  |
| Øvrige adresser hvorfra der behandles personoplysninger.  |  |
| Hvis relevant Kontaktperson hos Underdatabehandler.  |  |
| Har Databehandleren en aftale med Underdatabehandleren, som opfylder kravene i Databehandleraftalen?  | **JA** |
| Databehandling(er), som Underdatabehandler deltager i. |  |
| Kategorier af personoplysninger som Underdatabehandler behandler.  |  |
| Lokalitet for databehandlingen. |  |

**B.2 Overførsel af personoplysninger til tredjelande (udfyldes, hvis relevant)**

|  |  |
| --- | --- |
| Foretager Underdatabehandleren behandling af personoplysninger i et tredjeland?  |  |
| Hvis ja, angiv samtlige tredjelande  |  |
| Hvis ja, angiv overførselsgrundlaget (f.eks. en EU-standardkontrakt eller Binding Corporate Rules) |  |
| Hvis ja, angiv evt. supplerende organisatoriske eller tekniske sikkerhedsforanstaltninger (herunder kryptering samt opbevaring af krypteringsnøgle) | Databehandleren skal sikre at underdatabehandleren ikke sender personoplysninger i direkte personhenførbar form, jf. bilag C, punkt C.2.  |

**B.3. Dokumentation for underdatabehandlere**

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.

**B.4. Varsel for godkendelse af underdatabehandlere**

|  |  |
| --- | --- |
|  | Sæt kryds |
| Jf. databehandleraftalens punkt 5 | X |

**Bilag C – Behandlingssikkerhed**

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

**C.1 Fastlæggelse af sikkerhedsniveau**

C.1.1 Sikkerhedsniveauet skal afspejle kategorien og mængden af personoplysninger, der indgår i behandlingen:

* Personoplysninger omfattet af databeskyttelsesforordningens artikel 6.
* Fortrolige personoplysninger omfattet af databeskyttelseslovens §§ 8 og 11.

(Oplysninger om strafbare forhold og CPR-nummer).

* Følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 9.

C.1.2 Databehandleren skal gennemføre de i databehandlerinstruksen angivne krav, medmindre andet er aftalt med den Dataansvarlige og anført i bilag D.

C.1.3 Databehandleren skal tage de nødvendige skridt til at identificere, vurdere og begrænse enhver, med rimelighed forudsigelig, intern og ekstern risiko for tilgængeligheden, fortroligheden og/eller integriteten af alle personoplysninger, der behandles i forbindelse med opfyldelsen af Hovedaftalen.

C.1.4 Databehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedspolitikker og procedurer for behandling af personoplysninger i relation til Hovedaftalens opfyldelse for at sikre, at de fornødne sikkerhedsforanstaltninger fortsat iagttages.

C.1.5 Databehandlerens sikkerhedspolitikker og procedurer i relation til Hovedaftalens opfyldelse skal som minimum beskrive:

* Medarbejdernes roller og ansvarsområder
* De tekniske og organisatoriske foranstaltninger, der er vedtaget for at sikre personoplysninger.
* Underdatabehandlere eller andre tredjeparter, der er involveret i behandlingen af personoplysninger.

C.1.6 Databehandleren skal på foranledning af dataansvarlige fremvise en samlet risikovurdering i forhold til organisatoriske, tekniske og juridiske foranstaltninger, der finder anvendelse i forbindelse med opfyldelsen af Hovedaftalen.

C.1.7 For så vidt angår overførslen mellem databehandler og en underdatabehandler i et tredjeland, forpligter databehandler sig til at udarbejde en risikovurdering for denne overførsel ved indgåelse af aftale.

**C.2 Pseudonymisering og kryptering**

C.2.1 Databehandleren skal sikre, at der ikke må sendes personoplysninger i direkte personhenførbar form. Personoplysningerne skal opbevares og sendes krypteret eller erstattes af et kodenummer eller lignende.

C.2.2 Krypteringsnøgle, kodenøgle mv. skal opbevares forsvarligt og adskilt fra personoplysningerne.

C.2.3 Databehandleren skal sikre, at krypteringsnøgler aldrig opbevares i lande udenfor EU/EØS.

**C.3 Personalesikkerhed, Uddannelse og instruktion**

C.3.1 Databehandleren skal sikre, at Databehandlerens medarbejdere, der er involveret i behandling af personoplysninger er informeret om sikkerhedsforanstaltninger, der er relevante for deres jobfunktion. Endvidere skal medarbejderne informeres om relevante databeskyttelseskrav og relevante juridiske forpligtelser i overensstemmelse med relevant lovgivning samt Databehandlerens politikker og procedurer herfor.

C.3.2 Databehandleren skal sikre, at alle medarbejdere og underdatabehandlere eller andre tredjeparter, der er involveret i behandlingen af personoplysninger i relation til Hovedaftalen, følger fastlagte politiker og procedurer i relation til Hovedaftalens opfyldelse.

C.3.3 Databehandleren skal sikre, at kontrakter med medarbejdere og eksterne konsulenter, samarbejdspartnere, vikarer mv., der medvirker til Hovedaftalens opfyldelse, er informeret om udstrækningen af tavshedspligt og fortrolighed samt konsekvenserne ved en eventuel overtrædelse.

**C.4 Autorisation og adgangskontrol herunder kontrol med afviste adgangsforsøg**

C.4.1 Der må kun autoriseres medarbejdere, der er beskæftiget med de formål, hvortil personoplysninger i forbindelse med opfyldelsen af Hovedaftalen, behandles.

C.4.2 Der må endvidere autoriseres medarbejdere hos Databehandleren, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

C.4.3 Databehandleren skal træffe foranstaltninger til at sikre, at kun autoriserede medarbejdere kan få adgang til de personoplysninger, som den pågældende er autoriseret til.

C.4.4 Databehandleren skal kunne dokumentere hvilke medarbejdere, der har autorisation til at tilgå personoplysninger, der behandles i forbindelse med opfyldelsen af Hovedaftalen.

C.4.5 Autorisationer skal angive, i hvilket omfang den autoriserede medarbejder må forespørge, inddatere eller slette personoplysninger.

C.4.6 Der skal løbende og mindst en gang hvert halve år foretages kontrol af de adgange, som de autoriserede medarbejdere er tildelt, så det kan konstateres, om der er udstedte autorisationer, som ikke er anvendt, og som derfor eventuelt bør inddrages. Der skal i den forbindelse foretages en konkret vurdering af, om den autoriserede medarbejder fortsat har et arbejdsmæssigt behov for adgangen.

C.4.7 Databehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for medarbejdere, der ikke længere har behov for autorisationen i forbindelse med medarbejderens arbejde.

C.4.8 Den autoriserede medarbejder tildeles en personlig brugeridentifikation og et personligt password, der skal anvendes hver gang, medarbejderen får adgang til de personoplysninger, der behandles i forbindelse med opfyldelsen af Hovedaftalen.

C.4.9 Databehandleren skal definere og dokumentere en passwordpolitik. Passwordpolitikken skal som minimum indeholde oplysninger om passwordlængde, kompleksitet, gyldighedsperiode samt antal accepterede mislykkede loginforsøg. Der skal anvendes 2 faktor-autentifikation ved adgang til systemer med følsomme og fortrolige personoplysninger via internettet eller andet usikkert netværk.

C.4.10 Der skal foretages logning af alle afviste adgangsforsøg til de it-systemer, der anvendes i forbindelse med opfyldelsen af Hovedaftalen. Loggen skal overvåges med henblik på at opdage forsøg på uautoriseret adgang. Ved mistanke om forsøg på uautoriseret adgang skal der blokeres for flere forsøg. Adgangen åbnes først, når årsagen til de afviste adgangsforsøg er klarlagt.

C.4.11 Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale adgangskontrol sættes ud af kraft fx i forbindelse med systemadministration eller fejlretning.

**C.5 Logning**

C.5.1 Der skal foretages logning ved al behandling af personoplysninger. Loggen skal som minimum indeholde oplysninger på følgende områder:

* Aktivitetstekst som beskriver den udførte handling på opslaget
* Aktivitetstype for den udførte handling som minimum Create, Read, Update og Delete
* Tidspunkt for systemanvendelse og specificering af systemer
* Identifikation af brugeren (brugerid), der foretager opslag i løsningen
* De konkrete data eller søgninger, der er behandlet i den sammenhæng, loggen beskriver.

C.5.2 Loggen skal opbevares i minimum 6 måneder. Logning af data indeholdende følsomme personoplysninger skal opbevares i 13 måneder, hvorefter logdata skal slettes. Undtagelser, hvor der fastsættes en længere opbevaringsperiode, anføres i bilag D herunder formål og periode.

C.5.3 Databehandleren skal beskytte logfaciliteter og logoplysninger i relation til Hovedaftalens opfyldelse mod manipulation, sletning og uautoriseret adgang.

**C.6 Backup og genetablering**

C.6.1 Databehandleren skal sikre, at backup gives et niveau af beskyttelse, der er i overensstemmelse med det niveau, der anvendes på de originale data.

C.6.2 Databehandleren skal sikre, at systemer og personoplysninger, der er omfattet af databehandleraftalen, sikkerhedskopieres regelmæssigt ud fra en risikobetragtning.

C.6.3 Backup skal opbevares krypteret, og den tilhørende krypteringsnøgle skal tilsvarende opbevares sikkert. It-systemer og de tilhørende sikkerhedskopier skal være fysisk adskilte. Sikkerhedskopier skal opbevares i sikker afstand til det primære anlæg. Adgang til diske, som indeholder backup, opbevares under fysisk såvel som logisk adgangskontrol.

C.6.4 Kun få autoriserede, betroede medarbejdere må have adgang til diske, der indeholder backup. Adgangen til backupsystemer skal begrænses til medarbejdere med et arbejdsbetinget behov.

C.6.5 Databehandleren skal sikre, at der foretages gendannelsestests af alle kritiske aktiver, og testen skal dokumenteres.

C.6.6 Databehandleren skal have en plan for gennemførsel af gendannelsestests. Planen for gendannelsestests følger et årshjul og opbygges med udgangspunkt i en risikobetragtning.

C.6.7 Backup skal testes periodisk og minimum halvårligt med henblik på at validere dels integriteten af backup-medierne, og dels at systemer og data kan genskabes, hvis det bliver nødvendigt.

C.6.8 Databehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelse

**C.7 Opdateringer og ændringer**

 C.7.1 Databehandleren skal anvende dokumenterede driftsprocedurer herunder ændringsprocedurer i it-systemer, der anvendes i forbindelse med behandlingen af personoplysninger omfattet af databehandleraftalen. Databehandleren skal regelmæssigt overvåge disse procedurer.

C.7.2 Databehandleren skal have formelle procedurer, der sikrer, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

C.7.3 Databehandleren skal have procedurer, der sikrer, at kritiske sikkerhedsopdateringer kan gennemføres inden for 48 timer.

C.7.4 Databehandleren skal sikre, at ændringer i it-miljøet ikke påvirker sikkerheden negativt. Databehandleren skal inden ændringens gennemførsel foretage og dokumentere en vurdering af påvirkningen af de konkrete eksisterende sikkerhedsforanstaltninger i forbindelse med den pågældende ændring.

C.7.5 Databehandleren skal have en proces for godkendelse af ændringer, inden disse implementeres i Databehandlerens systemer, netværk og øvrig infrastruktur eller i tilknytning til netværk og infrastruktur. Godkendelsen skal være dokumenteret, og alle påvirkede systemer, databaser og udstyr skal identificeres i dokumentationen.

C.7.6 Databehandleren skal have en nødprocedure, såfremt en ændring ikke kan gennemføres.

**C.8 Fysisk sikring**

C.8.1 Databehandleren skal have tekniske og organisatoriske foranstaltninger, som begrænser risikoen for uautoriseret fysisk adgang. Områder hvor der sker behandling af personoplysninger skal være effektivt adskilt fra områder, hvortil der er generel adgang.

C.8.2 Databehandleren skal sikre, at fysiske områder, der anvendes til Hovedaftalens opfyldelse, og hvor uautoriserede personer kan komme ind, kontrolleres fx ved fremvisning af adgangs- eller gæstekort.

C.8.3 Databehandleren skal føre en log over al adgang til de områder, der anvendes til Hovedaftalens opfyldelse.

C.8.4 Databehandleren skal ud fra en risikobaseret tilgang have effektiv sikring mod miljømæssige hændelser, herunder brand, vandindtrængen, eksplosion og tilsvarende påvirkninger af serverrum, krydsfelter og tilsvarende områder.

C.8.5 Databehandleren skal endvidere sikre, at:

|  |  |
| --- | --- |
|  | Sæt kryds |
| Kritiske informationsaktiver, herunder servere, sikres med nødstrøm, herunder f.eks. UPS (Uninterruptible Power Supplies) og generatorer. | (x) |
| Kabler til elektricitet og kommunikation sikres mod indtrængen og sabotage, dvs. at kabler skal være skærmede, eller at føringsveje skal være utilgængelige. | (x) |
| Der på lokationer, hvor kritiske informationsaktiver opbevares, er etableret en plan for brugen af nødstrømsanlæg, som periodisk afprøves og kontrolleres. | (x) |
| Kritiske informationsbærende aktiver overvåges, og driftsområdet tilsluttes alarm, der advarer ved uautoriseret indtrængen, brand, indtrængende vand samt ændringer i temperatur og luftfugtighed. | (x) |
| Kritiske informationsbærende aktiver er beskyttet af et automatisk brandslukningsanlæg. | (x) |
| It-systemer og infrastruktur er beskyttet mod lyn og overspændinger. | (x) |
| Kabler og udstyr til datakommunikation beskyttes mod aflytning, interferens og skader. | (x) |
| Kabelføring dokumenteres og opdateres, når kabelføringen ændres. | (x) |
| Der er etableret alternative kommunikationsforbindelser til systemer med væsentlig betydning for regionen. | (x) |
| Væsentligt it-udstyr beskyttes mod tyveri. | (x) |

**C.9 Anvendelse af fjern- og hjemmearbejdspladser og mobilt udstyr**

C.9.1 Anvendelse af fjern- eller hjemmearbejdspladser skal være godkendt af den Dataansvarlige, og angives i bilag D.

C.9.2 Såfremt Databehandleren foretager behandling af personoplysninger fra fjern- eller hjemmearbejdspladser, skal Databehandleren sikre, at disse minimum lever op til nedenstående sikkerhedsmæssige krav:

* Forbindelsen mellem fjern- eller hjemmearbejdspladsen og Databehandlerens/Dataansvarliges netværk, skal være krypteret.
* Der skal anvendes 2-faktor-autentifikation.
* Databehandleren skal have en instruks for sikker anvendelse af fjern- og hjemmearbejdspladser.
* Databehandleren skal instruere Databehandlerens medarbejdere i sikkerheden for anvendelsen af fjern- eller hjemmearbejdspladser.

C.9.3 Mobilt udstyr, der anvendes til Hovedaftalens opfyldelse, skal være mærket og krypteret, og skal opbevares under opsyn eller under lås, når de ikke benyttes.

C.9.4 Mobilt udstyr med adgang til personoplysninger må kun udleveres til autoriserede personer med henblik på revisions- eller drifts- og systemtekniske opgaver.

C.9.5 Der skal føres en fortegnelse over, hvilket mobilt udstyr der benyttes i forbindelse med Hovedaftalens opfyldelse.

C.9.6 Ved reparation og service af mobilt udstyr skal Databehandleren sikre, at servicepersonalet behandler eventuelle personoplysninger, de bliver bekendt med under deres arbejde, fortroligt.

C.9.7 Ved kassation af mobilt udstyr, der indeholder lagringsmidler, skal der ske effektiv sletning af personoplysningerne. Dokumentation for, at kassation er sket i overensstemmelse med ovenstående, skal forevises på den Dataansvarliges anmodning.

**C.10 Kommunikationssikkerhed**

C.10.1 Databehandleren skal sikre, at alle former for transmission, der foretages via internettet krypteres i overensstemmelse med den Dataansvarliges krav stillet i forbindelse med aftaleindgåelsen.

C.10.2 Databehandleren skal sikre, at der:

* Benyttes End-to-end-kryptering ved datakommunikation.
* Etableres sikre forbindelser i form af kryptering af faste forbindelser og i form af VPN til etablering af midlertidige forbindelser.

**C.11 Underretning og bistand til den Dataansvarlige**

C.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-mail: xxxx@xxxx.dk

**C.12 Databehandlerens tilsyn med underdatabehandlere**

Hvis det er relevant, beskrives procedurerne for databehandlerens revisioner herunder inspektioner med behandlingen af personoplysninger, som er overladt til underdatabehandlere i bilag D.

C.12.1 Databehandleren skal årligt indhente en revisionserklæring eller inspektionsrapport fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag.

C.12.2 Såfremt der konstateres afvigelser ved revisionserklæringen eller inspektionsrapporten fremsendes dokumentation for de konstaterede afvigelser samt en plan for håndtering uden unødig forsinkelse til den Dataansvarlige til orientering. Den Dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen eller rapporten og kan i sådanne tilfælde anmode om en ny revisionserklæring eller inspektionsrapport under andre rammer og/eller under anvendelse af anden metode.

C.12.3 Baseret på planen for håndtering af de konstaterede afvigelser i erklæringen eller rapporten er den Dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag.

C.12.4 Databehandleren kan fravige kravet om revisionserklæring, såfremt Databehandleren vurderer, at Underdatabehandleren på anden vis vil kunne dokumentere overholdelse af Databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag.

**C.13 Den Dataansvarliges tilsyn med Databehandleren**

|  |  |
| --- | --- |
|  | Sæt kryds |
| Databehandleren skal på aftalte fremsendelsesdato fremsende revisionserklæring, ledelseserklæring eller tilsynsskema vedrørende Databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag. | X |
| ~~Databehandleren skal på anmodning fra den Dataansvarlige fremsende den aftalte revisionserklæring, ledelseserklæring eller tilsynsskema vedrørende Databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag.~~ |  |
| ~~Databehandleren skal på anmodning fra den Dataansvarlige besvare og fremsende det aftalte stikprøveskema vedrørende Databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag.~~ |  |

C.13.1 Erklæringen fremsendes uden unødig forsinkelse jf. den aftalte fremsendelsesdato. Den Dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen eller rapporten og kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og/eller under anvendelse af anden metode.

C.13.2 Baseret på resultaterne af erklæringen er den Dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag.

C.13.3 Den Dataansvarlige eller en repræsentant for den Dataansvarlige har herudover adgang til at foretage inspektioner herunder fysiske inspektioner med lokaliteterne, hvorfra Databehandleren foretager behandlingen af personoplysningerne omfattet af Hovedaftalen herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den Dataansvarlige finder det nødvendigt.

C.13.4 Såfremt den Dataansvarlige vurderer, at Databehandleren på anden vis vil kunne dokumentere overholdelse af Databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Databehandleraftalen med tilhørende bilag, kan anden tilsynsform aftales mellem parterne.

C.13.5

|  |  |  |  |
| --- | --- | --- | --- |
| **Erklæring** | **Anvendelse** | **Fremsendelsesdato** | **Sæt kryds** |
| ISAE3000Sæt kryds:Type I ( )Type II (X) | Ved behandling af fortrolige herunder følsomme personoplysninger skal der som udgangspunkt udarbejdes en ISAE3000 revisionserklæring om behandling af personoplysninger. | [dato] | X |
| ~~ISAE3402~~~~Sæt kryds:~~~~Type I ( )~~~~Type II ( )~~ | ~~Ved behandling af personoplysninger i overensstemmelse med databeskyttelses-~~~~forordningens artikel 6 eller hvis der mellem parterne aftales, at revisionserklæringen suppleres med andre auditaktiviteter.~~ |  |  |
| ~~Ledelseserklæring~~ | ~~Såfremt det mellem parterne aftales, at der ikke skal fremsendes en revisionserklæring, udarbejdes en ledelseserklæring om, at der er etableret passende sikringsforanstaltninger.~~ |  |  |
| ~~Tilsynsskema~~ | ~~Såfremt det mellem parterne aftales, at der ikke skal fremsendes en revisionserklæring, udfylder Databehandleren et tilsynsskema om, at der er etableret passende sikringsforanstaltninger.~~ |  |  |
| ~~Stikprøver~~ | ~~Såfremt det mellem parterne aftales, at der ikke skal fremsendes en revisionserklæring, udfyldes på anmodning af den Dataansvarlige et stikprøveskema om, at der er etableret passende sikringsforanstaltninger.~~ |  |  |

C.13.6 Databehandleren skal sende den aftalte erklæring til:

|  |  |
| --- | --- |
| **Navn** |  |
| **Stilling** |  |
| **Telefon** |  |
| **E-mail** |  |

**C.14 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande**

C.14.1 Godkendelse af overførsel og evt. specifik instruks vedr. overførsel af personoplysninger til tredjeland eller international organisation skal fremgå af bilag D.

C.14.2 Hvis den Dataansvarlige ikke i bilag D eller ved efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må Databehandleren ikke inden for rammerne af den udbudte aftale på hjemmeperitonealdialyse foretage en sådan overførsel.

Anfør overførselsgrundlag efter databeskyttelsesforordningens kapitel 5 i nedenstående tabel:

|  |  |
| --- | --- |
|  | Sæt kryds |
| Overførslen er baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet (artikel 45) |  |
| Overførslen er omfattet af fornødne garantier (artikel 46) |  |
| Overførslen er omfattet af bindende virksomhedsregler (artikel 47) |  |
| ~~Overførslen eller videregivelsen er uden hjemmel i EU-retten (artikel 48), angiv:~~ |  |
| ~~Overførslen er omfattet af undtagelser i særlige situationer (artikel 49), angiv hvilke:~~ |  |

**Bilag D - Parternes regulering af andre forhold**

**1. Beskriv baggrund for overførelse, jf. bilag C, punkt C.14.2**

|  |
| --- |
|  |

**2. Specifik instruks vedr. overførsel af personoplysninger, jf. punkt C.14.1**

|  |
| --- |
|  |

**3. Godkendelse vedr. overførsel af personoplysninger, jf. punkt C.14.1**

|  |
| --- |
|  |

**4. Overblik over dataflow enten indsat nedenfor eller vedlagt som separat dokument**

|  |
| --- |
|  |