Version 2.1 – marts 2023

Standardkontraktsbestemmelser

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

mellem

Navn på juridisk enhed

CVR nummer

Adresse

Postnummer og by

herefter ”den dataansvarlige”

og

CompuGroup Medical Denmark A/S
CVR-nr.: 24210529
Olof Palmes Allé 44
8200 Aarhus N

herefter ”databehandleren”

der hver især er en ”part” og sammen udgør ”parterne”

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. Indhold

2. Præambel

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

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

3. I forbindelse med leveringen af produkterne Equus, Etera eller Complimenta behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. 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.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

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

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

3. Den dataansvarliges rettigheder og forpligtelser

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

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

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

4. Databehandleren handler efter instruks

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

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

5. Fortrolighed

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

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

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

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

   c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

   d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

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

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

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

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

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

6. 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.

8. Overførsel til tredjelande eller internationale organisationer

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

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

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    c. behandle personoplysningerne i et tredjeland

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

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

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. indsigtsretten
d. retten til berigtigelse
e. retten til sletning ("retten til at blive glemt")
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

   c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

   d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden 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 om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

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

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

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

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige:

   Navn
   Stilling
   Telefonnummer
   E-mail
   Underskrift

   På vegne af databehandleren:

Navn	Kjeld Gandrup
Stilling	Corporate Data Protection Officer
Telefonnummer:	70 30 13 40
E-mail	databehandler.budk.dk@cgm.com
Underskrift:	

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

3. Kontaktperson hos den dataansvarlige

   Navn
   Stilling
   Telefonnummer
   E-mail

4. Kontaktperson hos CompuGroup Medical Denmark A/S

Navn:	Kjeld Gandrup
Stilling:	Corporate Data Protection Officer
Telefonnummer:	70 30 13 40
E-mail	databehandler.budk.dk@cgm.com

Bilag A Oplysninger om behandlingen

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

CompuGroup Medical Denmark A/S udvikler, leverer og hoster og leverer produkter, specialløsninger og services, som gør det muligt at registrere og dokumentere behandlinger samt klinisk data og muliggøre kommunikation og udveksling af sundhedsdata med patienter, andre behandlere og myndigheder i sundhedsvæsnet.

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

1. Levering af serviceydelser herunder:
    a. udvikling
    b. test,
    c. implementering
    d. drift
    e. support
    f. hosting og
    g. videreudvikling m.v.

2. Serviceydelserne kan tage form som it-systemer og andre it-løsninger, herunder:
    a. journalsystem,
    b. patientportal,
    c. mobilapplikationer,
    d. integrationer,
    e. tekniske anordninger og
    f. andre nødvendige it-relaterede løsninger til brug for behandling af personoplysninger vedrørende den dataansvarliges klinik som f.eks. kommunikation, datatransmission, videregivelse, sletning m.v.

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

Navn, e-mailadresse, telefonnummer, adresse, personnummer, familieforhold, sociale problemer, bolig, stilling, køn, betalingskortoplysninger, medlemsnummer, type af medlemskab, fremmøde i fitnesscenter, tilmelding til konkrete fitnesshold, oplysninger om forsikringsforhold, egen læge, sygesikringsgruppe samt helbredsoplysninger, helbredsforhold og registrering af ydelser den registrerede har modtaget.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Ansatte, brugere, patienter, borgere, klienter og lign. Herunder børn og unge under 18 år.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige påbegyndes efter parternes Hovedaftale træder i kraft og indtil denne ophører

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Medcom	26919991	Forskerparken 10, 5230 Odense	Sundhedsdatanet, CPR-opslag
Link Mobility A/S	30077520	Flæsketorvet 68, 1 1711 København K	SMS notifikationer
Netcompany A/S	39488914	Grønningen 17 1270 København K	Digital post og Beskeder til mit.dk
TrueCommerce Danmark ApS	33776349	Banevænget 13, 2. 3460 Birkerød	EDI og faktura transmission
QuickPay ApS	21822434	P. O. Pedersens Vej 2 8200 Aarhus N	Online betaling
CLEARHAUS A/S	33749996	P.O. Pedersens Vej 2 8200 Aarhus N	Indløsningsaftale til online betaling
Global Connect A/S	26759722	Havneholmen 6 2450 København SV	Housing af servere og infrastruktur

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte 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.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren har den Dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelser eller udskiftning af underdatabehandlere med mindst 30 dages varsel, jf. Databehandleraftalens afsnit 7.2.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

Behandling af personoplysninger og sundhedsdata jf. den aftalte it-ydelser jf. hovedaftale og andre særskilt indgående aftaler ml. parterne. Det omfatter, men er ikke begrænset til følgende behandlingsaktiviteter:

1. kommunikation og datatransmission til nødvendige tekniske sundhedstjenester via legale transportører og til legale modtagere, herunder Sundhedsdatanettet og VANS-nettet, som er en forudsætning for at foretage lovpligtige integrationer og gennemføre lovpligtig kommunikation, samt kommunikation og datatransmission.

2. udvikling, test, implementering, drift, support, hosting og videreudvikling m.v. af Equus og Etera (som beskrevet i særskilt hovedaftale eller øvrige aftaler mellem parterne)

3. at yde remote service og support til den dataansvarliges medarbejderes brug af Equus og Etera.

4. via tekniske anordninger bistå den dataansvarlige med udveksling af data med øvrige systemer via integrationer

5. at formidle personoplysninger til tredjeparter efter den dataansvarliges instruks, heriblandt at formidle personoplysninger til tredjeparter som påkrævet i lovgivning, f.eks. videregivelse af personoplysninger fra Sundhedsdatastyrelsens nationale it-infrastruktur til Sundhedspersoner via andre it-systemer

6. sletning i overensstemmelse med den dataansvarliges anvisninger

7. levere ydelser til at understøtte den dataansvarliges kvalitetsarbejde, herunder visning af patientoverblik for patienter, visning af kvalitetsrapporter samt bistand med indsamling og behandling af data til kvalitetsarbejdet.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Databehandleren iværksætter og gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med de behandlingsaktiviteter, Databehandleren foretager for den Dataansvarlige.
De tekniske og organisatoriske foranstaltninger fastsættes under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne, den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau. Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den Dataansvarlige:

C.2.1.Standarder

Databehandleren skal efterleve principperne i ISO 27001 på relevante områder, samt implementerede MedCom-standarder eller en i øvrigt anerkendt standard indenfor it-drift, i det omfang andet ikke fremgår af nærværende databehandleraftale.

C.2.2 Operationel sikkerhed

Databehandleren skal sikre:

1. at det nødvendige og tilstrækkelige sikkerhedsniveau vedligeholdes og opretholdes, samt at eventuelle ændringer i Databehandlerens sikkerhedsforanstaltninger relevante for personoplysningerne logges og dokumenteres,

2. at ændringer og vedligeholdelse af Databehandlerens sikkerhedsforanstaltninger så vidt muligt ikke påvirker den Dataansvarliges forretning, herunder men ikke begrænset til it-systemer, netværk, forbindelser og svartider,

3. at Databehandlerens eventuelle testmiljøer er tilstrækkelig afgrænset og i øvrigt sikret mod uautoriseret adgang,

4. at Databehandlerens it-systemer og netværk er tilstrækkeligt sikret mod hacking og anden uautoriseret adgang,

5. at Databehandleren gennemfører kontroller for at opdage og forhindre svindel, malware mv., og at dennes interne operationelle sikkerhedsprocedurer og -manualer følges

C.2.3 Fysisk sikkerhed

1. Databehandleren skal sikre sine fysiske lokaliteter, servere mv. mod uautoriseret adgang.

2. Databehandleren skal have interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den Dataansvarliges personoplysninger ikke kompromitteres

C.2.4 Backup

1. Databehandleren skal foretage backup af personoplysningerne samt teknisk test af backup, i det omfang backup er en del af Aftalen eller på anden vis er aftalt mellem Parterne.

2. Såfremt det er en del af Aftalen, eller hvis det på anden vis er aftalt mellem Parterne, vil Databehandleren herefter én gang i døgnet tage en backup af den Dataansvarliges oplysninger i journalsystemet. Backup-overførslen skal være krypteret. Backup skal opbevares i et aflåst område i en anden bygning end hvor produktionsserveren fysisk er placeret. Backup gemmes i henhold til den i Aftalen definerede periode eller en anden periode aftalt mellem Parterne.

3. Databehandleren stiller en erklæring om backup og teknisk test af backup til rådighed for den Dataansvarlige.

C.2.5 Adgang til personoplysninger

1. Databehandleren skal sikre, at kun relevante medarbejdere har adgang til de behandlede personoplysninger.

2. Databehandleren skal efter den Dataansvarliges anmodning på ethvert tidspunkt kunne afgive en erklæring om hvilke personer, som har haft adgang til personoplysningerne på vegne af Databehandleren.

3. Databehandleren skal sikre, at enhver person, der udfører arbejde for Databehandleren og får adgang til personoplysningerne, kun behandler sådanne oplysninger efter den Dataansvarliges instruks, medmindre behandlingen er påkrævet i henhold til EU-lovgivningen eller EØS-medlemsstaternes nationale lovgivning.

4. Databehandleren skal sikre, at enhver person, der udfører arbejde for Databehandleren og får adgang til personoplysningerne har oparbejdet tilstrækkeligt kendskab til korrekt håndtering af personoplysninger, og at de pågældende medarbejdere er bekendt med de for Aftalen gældende sikkerhedskrav

C.2.6 Logning

1. Databehandler foretager logning i overensstemmelse med lovgivningen og gældende branchestandarder.

2. Der skal foretages logning af alle afviste adgangsforsøg. alle adgangsforsøg logges – hvis der er 3 på hinanden følgende – lukkes adgang i et nærmere bestemt tidsrum. Der skal foretages maskinel logning af alle anvendelser af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører eller det anvendte søgekriterium.

3. Den Dataansvarlige kan på anmodning få de relevante logs udleveret fra Databehandleren.

4. Log opbevares i 6 måneder.

C.2.7 Samarbejde med myndigheder

1. Databehandleren samarbejder efter anmodning med Datatilsynet og eventuelle øvrige tilsynsmyndigheder i forbindelse med udførelsen af sådanne tilsynsmyndigheders opgaver. Databehandleren er herunder berettiget til at give Datatilsynet adgang til alle personoplysninger og oplysninger, der er nødvendige for at varetage Datatilsynets opgaver.

2. Efter Databehandlerens valg træffer enten den Dataansvarlige eller Databehandleren de nødvendige foranstaltninger til at sikre overholdelse af en afgørelse fra Datatilsynet. Eventuelle ændringer i forhold til sikkerhedsniveau gennemføres som en ændring i henhold til denne Aftale. Den Dataansvarlige underretter Datatilsynet om de foranstaltninger, der er truffet for at overholde afgørelsen.

3. Meddeler Datatilsynet Databehandleren påbud, skal Databehandleren efterkomme sådant påbud i overensstemmelse med den nærmere angivne måde og inden for den angivne frist.

C.2.8 Databehandlere, der har adgang til den Dataansvarliges it-systemer og/eller den Dataansvarlige fysiske bygninger mv.

1. Databehandlere, der har adgang til den Dataansvarliges it-systemer og/eller fysiske bygninger, skal ud over sikkerhedskravene i dette Bilag C, endvidere overholde de af dette pkt. 5 omfattede sikkerhedskrav.

2. Databehandleren har tilladelse til at tilgå den Dataansvarliges netværk og it-systemer i det omfang det er strengt nødvendigt. Dette sker via legale og sikkerhedsgodkendte værktøjer og kanaler, jf. Bilag C

C.3 Bistand til den Dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den Dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

På den Dataansvarliges specifikke anmodning bistår Databehandleren 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 udøvelse af de registreredes rettigheder som fastlagt i persondatalovgivningen.

Hvis en registreret fremsætter anmodning om udøvelse af sine rettigheder over for Databehandleren, giver Databehandleren uden ugrundet ophold meddelelse herom til den Dataansvarlige.

Under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, bistår Databehandleren efter specifik anmodning også den Dataansvarlige med at sikre overholdelse af den Dataansvarliges forpligtelser i forhold til:

1. Gennemførelse af passende tekniske og organisatoriske foranstaltninger
2. Sikkerhedsbrud
3. Underretning om brud på persondatasikkerheden til den registrerede
4. Gennemførelse af konsekvensanalyser
5. Forudgående høringer fra tilsynsmyndighederne

Der betales almindelig timebetaling for denne service.

C.4 Opbevaringsperiode/sletterutine

Der foretages fysisk sletning efter 6 måneder inkl. retentionsperiode på 3 måneder.

Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at slette alle personoplysninger i overensstemmelse med Bestemmelse 11.1, der er blevet behandlet på vegne af den Dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den Dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Behandlingen af persondata sker på Databehandlerens adresser samt de anførte Databehandlere og deres underdatabehandleres adresser

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den Dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er Databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler

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

Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i Bestemmelserne, til rådighed for den dataansvarlige. Databehandleren giver herunder mulighed for og bidrager til revisioner, herunder tilsyn og inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Den dataansvarlige har efter databeskyttelsesforordningens art. 24 og 28 ret og pligt til at gennemføre tilsyn med databehandlerens behandling af personoplysninger på den dataansvarliges vegne. Den dataansvarliges gennemførelse af tilsyn med databehandleren kan ske ved, at den dataansvarlige udfører en eller flere af følgende handlinger:

1. Egenkontrol på baggrund af dokumenter, som databehandleren gør tilgængelig for den dataansvarlige,
2. Skriftligt tilsyn eller
3. Fysiske inspektioner.

C.7.1 Egenkontrol

Den dataansvarlige skal på opfordring have adgang til en række dokumenter til brug for gennemførelse af egenkontrol, herunder:

1. Dokumentation for efterlevelse af ISO27001:2022 i form af løbende opretholdelse af dokumentation.
2. Beskrivelse af fysisk og organisatorisk sikkerhed hos databehandleren.
3. Risikovurdering – af delt infrastruktur (firewall, backup etc.).
4. IT Sikkerhedspolitik.
5. Beredskabsplaner hos databehandleren

C.7.2 Skriftligt tilsyn og fysisk inspektion

Den dataansvarlige kan vælge at gennemføre et tilsyn enten som skriftligt tilsyn eller ved fysisk inspektion. Tilsynet kan udføres af den dataansvarlige selv og/eller i samarbejde med tredjepart.

Den udførende person skal være generelt egnet til at udføre inspektioner og tilsyn, og den dataansvarliges valg af person/repræsentant/revisor skal forelægges databehandleren til godkendelse.

Tilsyn og inspektion kan finde sted efter forudgående varsel på minimum 2 uger og skal udføres så det sker til mindst mulig gene for databehandlerens øvrige virksomhed.

Udføres revision, herunder tilsyn og/eller inspektion af en anden end den dataansvarlige selv, skal denne anden revisor være uafhængig og ikke-konkurrerende i forhold til databehandleren og i øvrigt være underlagt fortroligheds- og tavshedspligt enten som følge af lov eller som følge af en fortrolighedsaftale, hvorpå databehandleren kan støtte ret direkte over for den pågældende anden revisor.

Databehandleren underretter omgående den dataansvarlige, hvis en instruks om at stille oplysninger til rådighed eller give mulighed for revisioner, herunder tilsyn og/eller inspektioner efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller national ret.

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

Databehandleren skal en gang årligt føre tilsyn med underdatabehandlere, som behandler personoplysninger, vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen og hvis det skønnes nødvendigt indhente revisionserklæring eller ISO-certifikat.

Bilag D Parternes regulering af andre forhold

D.1 Fravigelser til Aftale

Parterne har fraveget pkt. 7.6, som ikke er gældende for aftalen. Pkt. 7.6 har følgende ordlyd:

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.

D.2 Betalbar ydelse

Databehandleren har krav på særskilt betaling for ydelser efter punkt 9, 10 og ved deltagelse i revisioner i henhold til pkt. 12.

Såfremt Databehandlerens arbejde med håndtering af sikkerhedsbrud skyldes misligholdelse hos Databehandleren, vil Databehandleren ikke være berettiget til betaling for dette arbejde.