XMedicus Systems ApS

Databehandleraftale

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

Mellem:

Den dataansvarlige:

CVR:

(Herefter kaldet "den Dataansvarlige ")

og

Databehandleren:

XMedicus Systems ApS
CVR: 38102877
Gladsaxevej 363
2860 Søborg

(Herefter kaldet "Databehandleren ")

Har aftalt følgende Databehandleraftale (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

24. november 2023
Version 2.0

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 et elektronisk patientjournalsystem til den Dataansvarlige 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.

[1] Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

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 den Dataansvarlige 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.

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 1 måneds 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 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.

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. 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. 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 24 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 vis-

er, 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 24 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 tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at slette alle personoplysninger, 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.

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

a. Sundhedsloven

b. Journalføringsbekendtgørelsen

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

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 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.

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:

På vegne af Databehandleren

Navn: Mikkel Kruse Johnsen
Stilling: CEO

15 Kontaktpersoner/kontaktpunkter hos den Dataansvarlige og Databehandleren

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

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

den Dataansvarlige

Navn:	
Stilling:	DPO
Telefonnummer:	
Email:	

Databehandleren

Navn:	Troels Kristensen
Stilling:	DPO
Telefonnummer:	8883 6000
Email:	security@xmedicus.com

A Oplysninger om behandlingen

A.1 Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige

a. Backup

b. Den Dataansvarliges adgang til data

c. Formidling af korrespondance mellem den Dataansvarlige og de registrerede

d. Formidling af korrespondance mellem den Dataansvarlige og andre interessenter

e. Brugersupport

f. Teknisk support

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

a. At foretage og gemme backup

b. At foretage udtræk af data efter instruks fra den Dataansvarlige

c. At formidle elektroniske beskeder fra den Dataansvarlige til de registrerede

d. At formidle elektroniske beskeder fra den Dataansvarlige til myndigheder og andre interessenter

e. At bistå den Dataansvarliges medarbejdere med at anvende systemet

f. At foretage fejlsøgninger for at identificere tekniske fejl med henblik på udbedring

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

a. Almindelige personoplysninger

(i) Navn

(ii) Adresse

(iii) Alder

(iv) Mail

(v) Telefonnummer

(vi) Kunde ID

(vii) Egen læge

(viii) Familieforhold

(ix) Betalingsoplysninger

(x) Forsikringsforhold

(xi) Autorisationsnummer

b. Følsomme personoplysninger

(i) Helbredsoplysninger

(ii) Seksuelle forhold og orientering

(iii) Genetiske data

c. Fortrolige oplysninger

(i) Personnummer

(ii) Særlige helbredsoplysninger

A.4 Behandlingen omfatter følgende kategorier af registrerede

a. Patienter

b. Pårørende

c. Medarbejdere

d. Tidligere medarbejdere

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

Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

B Underdatabehandlere

B.1 Godkendte underdatabehandlere

Forsendelse af elektronisk kommunikation med persondata

Navn	KMD A/S
CVR-nr	26911745
Adresse	Lautrupparken 40 2750 Ballerup

Forsendelse af tekstbeskeder (SMS)

Navn	OnlineCity ApS
CVR-nr	27364276
Adresse	Buchwaldsgade 50 5000 Odense C

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 at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den Dataansvarlige i hænde minimum 1 måned før anvendelsen eller ændringen skal træde i kraft. Såfremt den Dataansvarlige har indsigelser mod ændringerne, skal den Dataansvarlige give meddelelse herom til Databehandleren inden 1 uge efter modtagelsen af underretningen. Den Dataansvarlige kan alene gøre indsigelse, såfremt den Dataansvarlige har rimelige, konkrete årsager hertil.

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:

1. Opbevarer data på dedikerede servere og elektroniske lagerenheder,
2. Bearbejder personoplysninger efter konkret instruks fra den Dataansvarlige med henblik på at bistå den Dataansvarlige med dataudtræk, nødvendige ændringer, fejlrettelser, konvertering af data samt sletning af data,
3. Formidler udveksling af beskeder, henvisninger, epikriser, fakturaer og lignende mellem den Dataansvarlige og de registrerede samt myndigheder og øvrige interessenter,
4. Yder brugersupport for den Dataansvarliges personale,
5. Yder teknisk support,
6. Sikrer den Dataansvarlige adgang til data,
7. Foretager backup af data.

C.1.1 Ændringer i behandlingens genstand/instruks

Hvis den Dataansvarlige ønsker at ændre i behandlingens genstand/sin instruks til Databehandleren – herunder hvis der f.eks. sker ændringer i de kategorier af personoplysninger, som Databehandleren skal behandle på vegne af den Dataansvarlige – skal dette ske i henhold til den mellem parterne aftalte proces for håndtering af ændringer af Hovedaftalen.

I det omfang sådanne ændringer medfører yderligere krav til Databehandlerens gennemførelse af tekniske og organisatoriske foranstaltninger, iagttagelse af særlige individuelle vilkår eller i øvrigt merarbejde/meromkostninger/øgede risici for Databehandleren, kan Databehandleren kræve særskilt vederlag herfor.

Databehandleren er forpligtet til at levere sine ydelser i overensstemmelse med de aftalte ændringer, når ændringerne er implementeret.

C.2 Behandlingssikkerhed

Behandlingen omfatter en større mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et højt sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren vil dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger:

C.2.1 Fysisk sikkerhed

Databehandleren gennemfører følgende fysiske sikkerhedsforanstaltninger:

a. Databehandlerens kontorlokaler er til enhver tid aflåst, selv i kontorets åbningstid.
b. Databehandleren har alarmsystem til at opdage og forhindre indbrud.

c. Databehandlerens udstyr (herunder PC'er, eventuelle servere m.v.) er sikret bag låste døre og vinduer.

d. Databehandleren anvender nøglestyring, dvs. udleverer nøgler til de relevante og nødvendige medarbejdere mv.

e. Databehandleren udsteder individuelle koder til alarm.

f. Databehandleren fjerner og destruerer medier, f.eks. harddiske, fra servere, netværkstilsluttet datalagere og pc'er før de bortskaffes.

g. Fysiske backups af personoplysninger krypteres og opbevares sikkert på minimum to fysiske lokationer.

h. I det omfang Databehandleren hoster servere hos leverandører, vælges alene leverandører, som tilbyder et højt sikkerhedsniveau, hvilket som minimum omfatter:
- Aflåste lokaler, sikret med f.eks. øjenscanning for at forhindre uautoriseret adgang.
- Alarmer og vagter døgnet rundt.
- Hosting rummet kan kun tilgås af på forhånd autoriseret personale

Kryptering

a. Personoplysninger krypteres i relevante systemer og/eller på opbevaringsmedier.

b. Databehandleren anvender kryptering når der overføres via internettet og i øvrigt, når det er muligt.

c. Personoplysninger, der overføres mellem løsningen og den enkelte klient krypteres.

d. Transmission af data på internt netværk kan krypteres men varetages af den Dataansvarlige.

e. Alle data krypteres efter FIPS 140-2 specifikationen.
- Harddiske med opbevaring af data eller backup krypteres.
- Transmission af data via VPN krypteres.
- Adgang til database sker igennem krypteret netværk jvf. punkt D.

Adgang til personoplysninger

a. Databehandlerens systemer har logisk adgangskontrol ved brugernavn og adgangskode eller anden autorisation f.eks. lokalt installereret sikkerhedscertifikat.

b. Databehandleren har sikker opbevaring (housing) af hardware på fysiske lokaliteter, hvor der opbevares persondata.

c. Alle adgange til løsningen fra hjemmearbejdspladser kræver to-faktor godkendelse

d. Databehandleren foretager regelmæssig gennemgang og kontrol af brugerautorisationer til specifikke systemer.

Beskyttelse af systemer

a. Hjemmearbejdspladser konfigureres og vedligeholdes.

b. Hjemmearbejde sker igennem sikret VPN-forbindelse og fordrer dels et lokalt installeret og gyldigt sikkerhedscertifikat, dels brugernavn og adgangskode.

c. Databehandleren har procedure(r) for at genskabe/reetablere data fra backup.

d. Backup udføres 1 gang i døgnet.

e. Det hardware hos Databehandleren, som indeholder persondata, benytter en firewall, når det er koblet til internettet,

f. Databehandleren skal periodisk teste, vurdere og sikre effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger.

Pseudonymisering

a. I henhold til behandlingen af personoplysninger jf. C.1 punkt 2, så bliver der pseudonymiseret eller anonymiseret, når det er relevant. F.eks. statistisk udtræk på instruks fra den Dataansvarlige.

Genoprettelse af tilgængeligheden og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

a. Mindst én gang årligt udfører Databehandleren en general test af proceduren for indlæsning af backup til reetablering

b. Den Dataansvarlige kan med 21 dages varsel anmode om, at Databehandleren udfører en test af reetablering af den Dataansvarliges database og adgang til samme. den Dataansvarlige afholder alle omkostninger til en sådan test, anslået 6 timers arbejde, og har ret til fuld indsigt i såvel proces som resultat af testen.

Følgende oplysninger skal som minimum logges

a. Den registreredes journal

   (i) Hvilke Brugere der har åbnet patientens journal og hvornår

   (ii) Hvilke Sundhedspersoner der har registeret behandlingsrelaterede oplysninger i patientens journal

b. Systemadgang

   (i) Hvilke Brugere der har logget på Systemet og hvornår.

C.2.2 Organisatorisk sikkerhed

Databehandleren gennemfører følgende organisatoriske sikkerhedsforanstaltninger:

a. Alle medarbejdere er underlagt fortrolighedsforpligtelse, der gælder for behandlede personoplysninger,

b. Medarbejdernes adgang til personoplysninger i systemer og på eventuelle fysiske medier eller faciliteter er begrænset, sådan at det kun er de relevante medarbejdere, der har rollebaseret adgang og login til de relevante personoplysninger, og det sikres, at adgang og login kun kan ske fra autoriseret udstyr.

c. Hvis medarbejdere skifter stilling, skal det sikres, at de ikke bevarer adgange, som ikke længere er nødvendige.

d. Der er tilknyttet en DPO.

C.3 Bistand til den Dataansvarlige

Databehandleren skal så vidt muligt bistå den Dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Omfang og udstrækning af bistanden

Rådgivning: Databehandleren skal yde rådgivning til den dataansvarlige om relevante databeskyttelsesforanstaltninger, bedste praksis og lovgivningsmæssige krav.

Risikovurdering: Databehandleren skal hjælpe den dataansvarlige med at udføre risikovurderinger for at identificere og evaluere potentielle trusler og sårbarheder i forbindelse med databehandlingsaktiviteterne.

Hændelseshåndtering: Databehandleren skal bistå den dataansvarlige i udarbejdelsen og implementeringen af en plan til håndtering af utilsigtede hændelser, herunder procedurer til håndtering af databrud, notifikationer og gendannelsesaktiviteter.

Tekniske og organisatoriske foranstaltninger i forbindelse med bistand

Adgangskontrol: Databehandleren skal etablere passende adgangskontroller, så kun autoriserede personer kan få adgang til de persondata, der behandles.

Kryptering: Databehandleren skal anvende krypteringsteknologier til beskyttelse af persondata under transmission og opbevaring.

Backup og gendannelse: Databehandleren skal implementere regelmæssige backup- og gendannelsesprocedurer for at sikre, at persondata kan genskabes i tilfælde af hændelser eller datatab.

Databehandleraftaler: Databehandleren skal etablere skriftlige databehandleraftaler med eventuelle underdatabehandlere for at sikre, at de også opretholder passende tekniske og organisatoriske foranstaltninger.

Medarbejderuddannelse: Databehandleren gennemfører relevant uddannelse og træning af deres medarbejdere om databeskyttelsesforanstaltninger, fortrolighed samt opfyldelse af databehandleraftalens instruks om bistand til den dataansvarlige.

C.4 Opbevaringsperiode/sletterutine

Som udgangspunkt slettes persondata efter ophør af aftaleforhold med den Dataansvarlige, eller ved anmodning fra den Dataansvarlige om at få oplysninger slettet eller tilbageleveret. Dog jf. Bestemmelse 11.1 samt 11.2.

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:

XMedicus Kontorer:
XMedicus Systems ApS
Gladsaxevej 363, parterre
2860 Søborg
Danmark

XMedicus Systems ApS
Hasselvænget 24
4760 Vordingborg
Danmark

Hosting Center:
Penta Infra
Smedeland 32
2600 Glostrup
Danmark

Særligt for support
Databehandling i form af support kan ske fra en af Databehandlerens arbejdscomputer eller andet tilsvarende udstyr udleveret fra Databehandleren til en medarbejder, herunder men ikke begrænset til telefon og bærbare enheder. Den form for databehandling er således ikke begrænset til en fysisk lokation.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Al data gemmes på servere inden for EU. Vi overfører derfor ikke dine personoplysninger til tredjelande.

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

Databehandleren skal indhente en revisorerklæring fra en uafhængig tredjepart vedrørende Databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæring / inspektionsrapport kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE3000

Revisionserklæringen skal gøres tilgængelig for den Dataansvarlige. Den Dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringsrapporten og kan i sådanne tilfælde, for den Dataansvarliges egen regning, anmode om en ny revisionserklæring / inspektionsrapport under andre rammer og/eller under anvendelse af anden metode.

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 disse Bestemmelser.

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

Den Dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den Dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den Dataansvarlige kan gennemføre sin inspektion.

D Parternes regulering af andre forhold

Der er ikke andre regulerede forhold mellem parterne.