DATABEHANDLERAFTALE

vedrørende brug af Peoples Clinic IT-løsningen

Mellem:

Den Dataansvarlige:
Den juridiske enhed, der oprettes som kunde i Peoples Clinic IT-løsningen, og hvis oplysninger (navn, CVR-nummer mv.) er registreret under oprettelsen.

og

Databehandleren:
Peoples Doctor A/S
CVR-nr.: 40930809

Version: 1.3
Dato for ikrafttræden: Dato for den Dataansvarliges digitale godkendelse af aftalen.

Indhold af dokument:

mk

1. Den dataansvarliges rettigheder og forpligtelser

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

1.2. 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.

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

2. Databehandleren handler efter instruks

2.1. 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.

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

3. Fortrolighed

3.1. 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.

3.2. Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt (f.eks. via ledelsesattestation eller underskrevne fortrolighedserklæringer)..

mk

3.3. Den Dataansvarlige anerkender, at Peoples Clinic-løsningen er designet til kollaborativ brug internt i klinikken. Den Dataansvarlige er eneansvarlig for at styre, autorisere og føre tilsyn med sine egne medarbejderes og personales (herunder administrativt personales) adgangsrettigheder til løsningen. Databehandleren stiller den tekniske ramme for brugerstyring til rådighed, men den Dataansvarlige bærer det fulde ansvar for at afgøre, hvilke af dennes medarbejdere der har et legitimt "tjenstligt behov", samt for at sikre, at alle autoriserede brugere håndterer loginoplysninger sikkert.

4. Behandlingssikkerhed

4.1. 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.

4.2. Databehandleren skal – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici.

4.3. 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.

4.4. De specifikke minimumskrav til tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren skal implementere, er specificeret i Bilag C.2.

5. Anvendelse af underdatabehandlere

5.1. 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).

5.2. Databehandleren har den dataansvarliges generelle skriftlige godkendelse til brug af underdatabehandlere.

5.3. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages

mk

varsel og dermed give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

5.4. 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.

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

5.6. En kopi af databehandleraftalen med underdatabehandleren og eventuelle senere ændringer hertil sendes – efter den Dataansvarliges anmodning herom – i kopi til den Dataansvarlige. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold, skal ikke sendes til den Dataansvarlige.

5.7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

6. Overførsel til tredjelande eller internationale organisationer

6.1. 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.

6.2. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland er angivet i bilag C.6.

6.3. 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.

mk

7. Bistand til den dataansvarlige

7.1. 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.

7.2. I tillæg bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med overholdelse af forpligtelser vedrørende:
a) anmeldelse af brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, uden unødig forsinkelse,
b) underretning af den registrerede om brud på persondatasikkerheden uden unødig forsinkelse,
c) at foretage en konsekvensanalyse vedrørende databeskyttelse (DPIA),
d) at høre den kompetente tilsynsmyndighed inden behandling, såfremt en DPIA viser, at behandlingen vil føre til høj risiko.

7.3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige, samt i hvilket omfang og udstrækning.

8. Underretning om brud på persondatasikkerheden

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

8.2. 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.

8.3. Databehandleren skal bistå den dataansvarlige med at tilvejebringe den information, som er angivet i Bilag C, i forbindelse med anmeldelsen af bruddet.

9. Sletning og returnering af oplysninger

9.1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger er Databehandleren forpligtet til uigenkaldeligt at slette alle personoplysninger efter udløbet af den periode, der er angivet

mh

i Bilag C.4. I denne periode kan den Dataansvarlige selvstændigt eksportere data via de tilgængelige selvbetjeningsværktøjer. Den Dataansvarlige anerkender og instruerer hermed om, at denne automatiske sletning udgør den valgte metode for håndtering af data i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 3, litra g.

9.2. Databehandleren skal overholde specifikke lovkrav om opbevaring af data som beskrevet i Bilag C.4.

10. Revision, herunder inspektion

10.1. 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.

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

10.3. Databehandleren er forpligtet til at give tilsynsmyndigheder, samt andre tredjeparter der har adgang hertil i henhold til gældende lovgivning eller forskrifter, adgang til Databehandlerens faciliteter mod behørig legitimation.

11. Parternes aftale om andre forhold

11.1. Parterne kan aftale andre Bestemmelser vedrørende tjenesten, f.eks. erstatningsansvar, så længe disse andre Bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder.

12. Ikrafttræden og ophør

12.1. Bestemmelserne træder i kraft på det tidspunkt, hvor den Dataansvarlige digitalt godkender aftalen som en del af onboarding-processen for Peoples Clinic IT-løsningen.

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

12.3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer.

mk

12.4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

Digital Godkendelse

Denne Databehandleraftale godkendes digitalt af den Dataansvarlige. Databehandlerens accept af aftalen er givet ved at stille tjenesten til rådighed på disse vilkår.
Ved at markere afkrydsningsfeltet "Jeg har læst og accepterer Databehandleraftalen" og efterfølgende klikke på knappen 'Godkend' eller en tilsvarende funktion i onboarding-processen, afgiver den Dataansvarlige en juridisk bindende accept af samtlige vilkår i denne aftale. Tidspunktet, brugeroplysninger og andre relevante data for denne handling logges af Databehandlerens system og udgør den officielle registrering af aftalens indgåelse. Denne digitale accept er i alle henseender ligestillet med en fysisk underskrift.

Bilag A: Oplysninger om behandlingen

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

- At levere Peoples Clinic IT-løsningen til den dataansvarlige (lægeklinikker).
- At transskribere og opsummere samtaler mellem læge og patient for at skabe objektive journalnotater.
- At forbedre lægens effektivitet gennem avanceret teknologi, der fungerer som en transient behandlingsmotor.
- At assistere lægen med AI-drevet analyse af historiske journaldata (Resume-funktion) for at minimere risikoen for overset klinisk information og øge patientsikkerheden.
- At understøtte klinisk forskning og kvalitetsudvikling gennem indsamling af pseudonymiserede datavolumina.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen):
Behandlingen omfatter levering af en AI-baseret Software-as-a-Service (SaaS) platform. Centrale aktiviteter inkluderer:

- Realtidstransskription af lyd fra samtaler ved hjælp af en hybrid, containeriseret taleteknologi.

mk

- Behandlingen omfatter etablering af en nødvendig datastruktur (patientregister) for at sikre klinisk kontinuitet og muliggøre avancerede hjælpefunktioner såsom historiske resuméer og beslutningsstøtte.
- AI-drevet analyse ved hjælp af selv-hostede open source-modeller for at generere udkast til journalnotater.
- Hosting af sessionsdata linket udelukkende til Læge-ID og Tidsstempel.

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

- Særlige kategorier af personoplysninger (GDPR art. 9):
    - Ustruktureret tekst i samtaletransskriptioner og journalnotater, der kan indeholde helbredsoplysninger.
- Almindelige personoplysninger (GDPR art. 6):
    - Data om den dataansvarliges brugere (læger): Navn, loginoplysninger, Læge-ID.
    - Sessions-metadata (Tidsstempel, Læge-ID).
- **Bemærk:** Databasen indeholder de for formålet nødvendige patient-identifikatorer (f.eks. navn eller CPR-nummer) for at muliggøre kobling til Dataansvarliges øvrige systemer og sikre korrekt identifikation ved brug af resumé- og beslutningsstøttefunktioner.

A.4. Behandlingen omfatter følgende kategorier af registrerede:

- Personer, hvis helbredsoplysninger fremgår af den ustrukturerede tekst i konsultationen (Patienter), identificerbare kun for den Dataansvarlige via tidsstempel.
- Brugere af Peoples Clinic-løsningen (Læger).

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed:
Behandlingen fortsætter i hele serviceaftalens løbetid mellem parterne. Specifikke datatyper opbevares som følger:

- **Samtaletransskriptioner (Sessionsdata):** Opbevares i maksimalt 3 måneder med henblik på kvalitetssikring, hvorefter sessionen slettes automatisk baseret på tidsstempel.
- **Lægegodkendte journalnotater:** Opbevares i maksimalt 90 dage som buffer, hvorefter de slettes. Den officielle journal ligger hos den Dataansvarlige.

Bilag B: Underdatabehandlere

mk

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandler:

NAVN	CVR (eller tilsvarende)	ADRESSE	BESKRIVELSE AF BEHANDLING
netcup GmbH	HRB 26500	Daimlerstraße 25, 76185 Karlsruhe, Tyskland	Hosting af hele Peoples Clinic løsningen (backend og frontend) på virtuel IT-infrastruktur (IaaS) i Nürnberg, Tyskland. Dette omfatter al datalagring, behandling og backup.

B.2. Varsel for godkendelse af underdatabehandlere

Varslingsperioden for databehandlerens underretning af den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere er 30 dage i henhold til Bestemmelse 5.3.

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 de tjenester, der er beskrevet i Bilag A.1 og A.2.

- **AI-Modeller:** Databehandleren instrueres i at anvende en dynamisk selektion af open-source modeller (f.eks. DeepSeek, Qwen), som er implementeret lokalt hos Databehandleren.
- **Modeltræning:** Databehandleren er eksplicit instrueret i **ikke** at anvende personoplysninger til træning, gen-træning eller finjustering af nogen AI-modeller.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle den høje risiko, der er forbundet med behandlingen af særlige kategorier af helbredsoplysninger. Der skal etableres et "Højt" sikkerhedsniveau.

Databehandleren skal som minimum gennemføre følgende foranstaltninger:

mk

- **Kryptering:** Alle data "at rest" krypteres på database-niveau. Alle data "in transit" krypteres med stærke, moderne protokoller (TLS 1.2+).
- **Adgangskontrol:** Streng rollebaseret adgangskontrol (RBAC) håndhæves. Direkte menneskelig adgang til produktionsdata er begrænset til den EU-baserede systemadministrator under kontrollerede og dokumenterede omstændigheder.
- **Dataadskillelse:** Et dedikeret Data Access Layer sikrer streng logisk adskillelse af data mellem forskellige lægeklinikker (dataansvarlige) med en nultolerancepolitik over for adgang på tværs af brugere.
- **System- og miljøsikkerhed:** Produktions- og udviklingsmiljøer er strengt adskilte, og ingen reelle patientdata anvendes i udvikling. Regelmæssige sårbarhedsscanninger udføres, og en risikobaseret patch-proces er på plads.
- **Fysisk sikring:** Leveres af underdatabehandleren (netcup GmbH), som er certificeret efter ISO 27001 og ISO 27701 for sine EU-datacentre.
- **Logning og overvågning:** Omfattende systemlogning er på plads. Logs, der indeholder følsomme data, er underlagt en maksimal opbevaringsperiode på 3 måneder.
- **Sikker sletning:** Der er processer på plads for at sikre den automatiske sletning af transskriptioner og journalnotater efter udløb af deres opbevaringsperiode.
- **Dataadskillelse og Pseudonymisering:** Løsningen anvender strukturel pseudonymisering, hvor kliniske data opbevares adskilt fra administrative data. Identifikation sker via autoriserede adgangsveje, der sikrer, at kun relevant sundhedspersonale kan sammenkoble sessions-artefakter med den konkrete patient.
- **Netværkssikkerhed:** Specifik egress-filtrering blokerer AI-containere fra at tilgå internettet for at sikre mod datalækage.
- **Forbud mod transmission af personfølsomme oplysninger via e-mail:** Den Dataansvarlige instrueres i, at transmission af helbredsoplysninger eller uredigerede transskriptioner via e-mail til Databehandleren (herunder til `support@peoplesdoctor.com`) er strengt forbudt. Supporthenvendelser må kun indeholde administrative metadata eller tekniske fejlbeskrivelser.

C.3. Bistand til den dataansvarlige

Databehandleren bistår den dataansvarlige ved at levere følgende tekniske og organisatoriske foranstaltninger:

- Databehandleren stiller selvbetjeningsværktøjer til rådighed i brugergrænsefladen, som gør det muligt for den Dataansvarlige selvstændigt at identificere patienter i patientregisteret og eksekvere sletning eller udtræk (dataportabilitet) af transskriptioner, journalnotater og resuméer.

mk

    - Henvendelser vedrørende bistand til registreredes rettigheder, som ikke kan løses via selvbetjeningsværktøjerne, skal rettes til `privacy@peoplesdoctor.com`.
- Selvstændig DSR-håndtering: Da systemet indeholder et patientregister, er den Dataansvarlige ansvarlig for at identificere de relevante poster via Patient-ID, Navn eller CPR-nummer direkte i løsningen. Databehandlerens personale yder udelukkende proceduremæssig vejledning via privacy@peoplesdoctor.com og foretager ikke sletning eller udtræk på den Dataansvarliges vegne for at sikre adskillelse af ansvar.
    - Databehandlerens personale yder udelukkende proceduremæssig vejledning og foretager ikke sletning eller udtræk på den Dataansvarliges vegne.
- At levere nødvendig information og logs (som tilgængeligt og tilladt ved lov) for at bistå den dataansvarlige med håndtering af databrud og besvarelse af anmodninger fra registrerede.
- Underretning om potentielle sikkerhedshændelser eller brud på persondatasikkerheden kan ske direkte til `security-incident@peoplesdoctor.com`.

C.4. Opbevaringsperiode/sletterutine

- Personoplysninger opbevares kun i de perioder, der er specificeret i Bilag A.5.
- Ved tjenestens ophør opbevarer Databehandleren data i en periode på 90 dage. I denne periode skal den Dataansvarlige selvstændigt udtrække eventuelle nødvendige data via platformens selvbetjeningsværktøjer. Efter udløbet af denne periode vil alle personoplysninger tilhørende den Dataansvarlige blive slettet automatisk og uigenkaldeligt. Databehandleren er ikke forpligtet til at udføre manuel tilbagelevering af data eller levere specialudtræk.

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:

- **Primær lokalitet:** Nürnberg, Tyskland (netcup GmbH datacenter).
- **Backup-lokaliteter:** Andre datacentre inden for EU, drevet af netcup GmbH, udelukkende til backup- og disaster recovery-formål.

C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande

Der er ingen instruks om at overføre personoplysninger til tredjelande. Databehandleren er instrueret i, at al behandling af personoplysninger, herunder adgang, lagring og support, udelukkende skal finde sted inden for Den Europæiske Union/Det Europæiske Økonomiske Samarbejdsområde (EU/EØS). Databehandleren er ikke berettiget til at overføre personoplysninger til noget tredjeland eller nogen international organisation.

mk

C.7. Procedurer for den dataansvarliges revisioner, herunder inspektioner
Databehandleren skal årligt for egen regning indhente en relevant tredjeparts revisionserklæring, der påviser overholdelse af forpligtelserne i henhold til databeskyttelsesforordningen og disse Bestemmelser.

Dette vil som udgangspunkt være en **ISAE 3000 Type 1** erklæring, men kan efter aftale erstattes af en anden anerkendt erklæring, som f.eks. en ISO 27001 certificering, såfremt denne vurderes at give den dataansvarlige tilstrækkelig sikkerhed for overholdelse. Denne erklæring, der dækker overholdelse af GDPR og de sikkerhedsforanstaltninger, der er beskrevet i disse Bestemmelser, vil blive stillet til rådighed for den dataansvarlige efter anmodning. Denne erklæring skal være den primære revisionsmetode.

Den dataansvarlige er berettiget til at anmode om yderligere dokumentation for at verificere overholdelse. Hvis revisionserklæringen giver anledning til bekymring, eller i tilfælde af en specifik sikkerhedshændelse, kan den dataansvarlige anmode om at foretage en inspektion, herunder en fysisk inspektion, som vil være for den dataansvarliges egen regning.

C.8. Procedurer for revisioner, herunder inspektioner, med underdatabehandlere
Databehandleren er ansvarlig for at sikre, at dens underdatabehandlere er underlagt tilsvarende revisionsforpligtelser. Databehandleren skal årligt indhente og gennemgå underdatabehandlerens seneste tredjeparts revisionserklæringer (f.eks. ISO 27001 og ISO 27701). Resuméer af disse gennemgange eller selve erklæringerne (hvor det er tilladt) vil blive leveret til den dataansvarlige efter anmodning for at påvise underdatabehandlerens overholdelse.

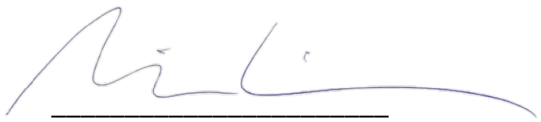
mk

Bilag D: Parternes regulering af andre forhold

Ingen yderligere aftaler er indgået under dette bilag.

Dato: 15-04-2026

Databehandleren:



_____

Michael Hein
CEO

Dato:

Den Dataansvarlige:

_____