

Databehandleraftale

Administrations- og kontorservice, herunder Netværkspraksis Intra

Den dataansvarlige

Den klinik eller virksomhed, der køber administrations- og kontorservice eller abonnerer på Netværkspraksis Intra (herefter "Kunden").

Databehandleren

Netværkspraksis Danmark P/S
CVR-nr. 45294102
Ndr. Ringvej 85, 1., 6000 Kolding
kontakt@netvaerkspraksis.dk

Version 1.0 · gældende fra 20. oktober 2026. Aftalen indgås ved Kundens elektroniske accept ved oprettelse af abonnement på Netværkspraksis Intra, ved underskrift eller ved aftale om administrations- og kontorservice. Aftalen er udarbejdet efter databeskyttelsesforordningen (GDPR) artikel 28, stk. 3.

1. Baggrund og formål

Aftalen regulerer Databehandlerens behandling af personoplysninger på vegne af Kunden i forbindelse med:

- **Netværkspraksis Intra** ("Intra"): webbaseret system til klinikkens ledelse og drift, herunder instrukser og dokumenter, personale og HR, kontrakter med digital underskrift, vagtplan og timeregistrering, lønintegration, møder med dagsorden og referat, opgaver, nyheder og beskeder.
- **Administrations- og kontorservice**: administrativ bistand til klinikken, fx personaleadministration, lønforberedelse, bogføringsbistand, mødeadministration og support.

Aftalen har forrang for modstridende bestemmelser om behandling af personoplysninger i andre aftaler mellem parterne.

Patientdata: Intra er ikke et journalsystem og er ikke beregnet til patientoplysninger. Intra gemmer ikke patientdata. Kunden instruerer sine medarbejdere i ikke at skrive patientoplysninger i instrukser, referater, opgaver eller beskeder. Administrations- og kontorservicen omfatter ikke adgang til patientjournaler. Skulle en opgave undtagelsesvis kræve adgang til patientoplysninger, sker det kun efter skriftlig instruks fra Kunden og efter denne aftale.

Medicinsk Copilot er ikke omfattet af denne aftale. Copilot leveres af HenrikRasmussen Invest ApS under en særskilt databehandleraftale (medicinsk-copilot.dk/databehandleraftale).

2. Kundens forpligtelser og rettigheder

Kunden er dataansvarlig og har ansvaret for, at behandlingen sker lovligt, herunder at der er et behandlingsgrundlag, at de registrerede er oplyst om behandlingen, og at instrukserne til Databehandleren er lovlige. Kunden bestemmer, hvilke personoplysninger der lægges i Intra.

3. Databehandleren handler efter instruks

Databehandleren behandler kun personoplysninger efter dokumenteret instruks fra Kunden. Instruksen fremgår af denne aftale med bilag og af Kundens brug af Intra og servicen. Databehandleren underretter straks Kunden, hvis en instruks efter Databehandlerens vurdering er i strid med GDPR eller anden databeskyttelseslovgivning.

4. Fortrolighed

Kun medarbejdere, der har brug for det for at levere ydelsen, får adgang til Kundens personoplysninger. De har tavshedspligt eller har forpligtet sig til fortrolighed. Adgangen gennemgås løbende og lukkes, når den ikke længere er nødvendig.

5. Behandlingssikkerhed

Databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger efter GDPR artikel 32. Foranstaltningerne er beskrevet i Bilag C.

6. Underdatabehandlere

Kunden giver Databehandleren generel godkendelse til at bruge de underdatabehandlere, der står i Bilag B. Databehandleren indgår skriftlige aftaler, der pålægger underdatabehandlerne de samme databeskyttelsesforpligtelser som denne aftale. Databehandleren varsler planlagte ændringer mindst 30 dage før, så Kunden kan gøre indsigelse. Databehandleren er over for Kunden ansvarlig for underdatabehandlernes overholdelse.

7. Overførsel til tredjelande

Personoplysninger opbevares i EU/EØS. Overførsel til lande uden for EU/EØS sker kun efter Kundens instruks, som er givet ved godkendelsen af underdatabehandlerne i Bilag B, og kun på et gyldigt overførselsgrundlag efter GDPR kapitel V, fx EU-Kommissionens standardkontraktbestemmelser eller en afgørelse om tilstrækkeligt beskyttelsesniveau.

8. Bistand til Kunden

Databehandleren bistår Kunden, så vidt muligt og under hensyn til behandlingens karakter, med at besvare anmodninger fra registrerede (indsigt, berigtigelse, sletning, begrænsning, dataportabilitet og indsigelse), med konsekvensanalyser og forudgående høring af Datatilsynet og med Kundens øvrige forpligtelser efter GDPR artikel 32–36. Kunden kan selv udtrække og slette de fleste oplysninger i Intra.

9. Brud på persondatasikkerheden

Databehandleren underretter Kunden uden unødigt forsinkelse og så vidt muligt senest 24 timer efter at være blevet opmærksom på et brud på persondatasikkerheden, så Kunden kan anmelde bruddet til Datatilsynet inden for 72 timer. Underretningen indeholder de oplysninger, der er nødvendige efter GDPR artikel 33, stk. 3.

10. Sletning og tilbagelevering

Når aftalen ophører, kan Kunden inden for 30 dage eksportere sine data fra Intra. Herefter sletter Databehandleren Kundens personoplysninger, medmindre lovgivningen kræver opbevaring. Krypterede sikkerhedskopier af databasen udskiftes løbende og slettes senest efter 14 dage. Krypterede kopier af filer slettes, når aftalen ophører.

11. Revision og tilsyn

Databehandleren stiller de oplysninger til rådighed, der er nødvendige for at vise, at GDPR artikel 28 og denne aftale overholdes, og giver mulighed for revision, herunder inspektion, foretaget af Kunden eller en revisor, som Kunden har givet mandat. Databehandleren kan opfylde dette ved at fremlægge

dokumentation for sikkerhedsforanstaltningerne og underdatabehandleraftaler. Kunden afholder egne omkostninger ved revision.

12. Ikrafttræden og ophør

Aftalen træder i kraft ved Kundens accept eller underskrift og gælder, så længe Databehandleren behandler personoplysninger for Kunden. Bestemmelser, der efter deres natur skal gælde efter ophør, fx om fortrolighed og sletning, gælder fortsat.

13. Lovvalg og værneting

Aftalen er underlagt dansk ret. Tvister afgøres ved de danske domstole.

For Kunden (dato, navn og underskrift)

For Netværkspraksis Danmark P/S (dato, navn og underskrift)

Bilag A – Oplysninger om behandlingen

Formål

Levering af Netværkspraksis Intra og administrations- og kontorservice til Kundens klinik.

Behandlingens karakter

Opbevaring, strukturering, visning, søgning, overførsel til integrationer, som Kunden selv aktiverer (fx lønsystem), sletning, transskription af mødeoptagelser og AI-assisteret tekstbehandling af dagsordener og referater.

Kategorier af registrerede

- Kundens ejere, ansatte, vikarer og uddannelseslæger
- Brugere af Intra og mødedeltagere
- Kontaktpersoner hos samarbejdspartnere

Typer af personoplysninger

- Almindelige oplysninger: navn, stilling, kontaktoplysninger, login og adgangsrettigheder, ansættelseskontrakter, løn- og timeoplysninger, vagtplan, ferie og fravær, HR-samtaler, mødeindhold og aktivitetslog.
- CPR-nummer på ansatte (til kontrakter og løn), opbevaret krypteret.
- Oplysninger om sygefravær kan forekomme i fraværsregistrering.
- Patientoplysninger behandles ikke (se punkt 1).

Varighed

Så længe Kunden bruger Intra eller servicen, og derefter som beskrevet i punkt 10.

Behandlingssted

Data opbevares i EU (Frankfurt, Tyskland). Databehandleren arbejder fra Danmark.

Bilag B – Underdatabehandlere

Underdatabehandler	Formål	Behandlingssted og overførselsgrundlag
Render Services, Inc.	Drift og hosting af Intra, database og filer	EU (Frankfurt). Standardkontraktbestemmelser ved evt. supportadgang uden for EU/EØS.
Microsoft Ireland Operations Ltd.	E-mail (Microsoft 365) og krypteret natlig sikkerhedskopi (OneDrive). Microsoft har ikke krypteringsnøglen.	EU/EØS (EU Data Boundary).
Amazon Web Services EMEA SARL	AI-tekstbehandling af dagsordener og referater via Amazon Bedrock	EU (eu-central-1, Frankfurt). Ingen brug til træning af AI-modeller.

Anthropic Ireland, Limited	AI-tekstbehandling af dagsordener og referater (anvendes, hvis Amazon Bedrock ikke er tilgængelig)	Behandling kan ske i USA. EU-Kommissionens standardkontraktbestemmelser. Ingen brug til træning af AI-modeller.
Deepgram, Inc.	Tale-til-tekst ved optagelse af møder. Lyden gemmes ikke af Intra.	EU-endpoint. Standardkontraktbestemmelser.
Idura ApS (tidl. Criipto)	Login med MitID Erhverv	Danmark/EU.
Stripe Payments Europe, Ltd.	Betaling af abonnement (kun klinikens betalingsoplysninger og kontaktperson)	Irland (EU). Standardkontraktbestemmelser ved overførsel til Stripe, Inc.

Integrationer, som Kunden selv aktiverer (fx Danløn eller Salary), er Kundens egne databehandlere. Databehandleren overfører kun data til dem efter Kundens instruks i Intra.

Bilag C – Sikkerhedsforanstaltninger

- **Kryptering:** AI trafik sker over HTTPS/TLS. CPR-numre og adgangsnøgler til integrationer gemmes krypteret (AES-256-GCM). Sikkerhedskopier krypteres, før de forlader driftsmiljøet.
- **Adgangsstyring:** Individuelt login, evt. med MitID Erhverv. Roller og rettigheder pr. klinik. Data fra forskellige kunder holdes adskilt.
- **CPR-visning:** CPR-numre vises maskeret. Visning af det fulde nummer logges.
- **Logning:** Væsentlige handlinger logges med bruger og tidspunkt.
- **Sikkerhedskopier:** Daglig sikkerhedskopi. De 7 nyeste opbevares i driftsmiljøet, og krypterede kopier af databasen opbevares i 14 dage hos Microsoft (OneDrive).
- **Ingen patientdata:** Intra har ingen funktioner til at gemme patientjournaler.
- **AI:** Indhold sendt til AI-behandling bruges ikke til at træne modeller. Mødelyd transskriberes og gemmes ikke.
- **Organisatorisk:** Tavshedspligt, adgang efter behov, opdatering af systemer og afhængigheder, og plan for håndtering af sikkerhedsbrud.