

# Databehandleraftale Netværkspraksis Danmark PS Version 1.3

## Standardkontraktbestemmelser

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

**mellem**

**Dataansvarlig ("Kunden")**

**Version 1.3**

"Kunden" er dataansvarlig i henhold til databeskyttelsesforordningen (GDPR) og relevant dansk lovgivning.

Kundens nærmere identitet (CVR, juridisk navn og adresse) fremgår af *den digitale oprettelse*, som ved accept henvises til denne aftale.

**herefter "den dataansvarlige"**

*og*

**Netværkspraksis Danmark PS**

CVR 45294102, Ndr. Ringvej 85,1, 6000 Kolding, Danmark.

**herefter "databehandleren"**

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

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

Netværkspraksis Danmark Databehandleraftale – Version 1.3 2

## Indhold

2. Præambel .....	3
3. Den dataansvarliges rettigheder og forpligtelser .....	3
4. Databehandleren handler efter instruks .....	4
5. Fortrolighed .....	4

6. Behandlingsikkerhed .....	4
7. Anvendelse af underdatabehandlere .....	5
8. Overførsel til tredjelande eller internationale organisationer .....	6
9. Bistand til den dataansvarlige .....	6
10. Underretning om brud på persondatasikkerheden .....	7
11. Sletning og returnering af oplysninger .....	8
12. Revision, herunder inspektion .....	8
13. Parternes aftale om andre forhold .....	8
14. Ikrafttræden og ophør .....	8
15. Kontaktpersoner og henvendelser .....	9
16. Bilag A Oplysninger om behandlingen .....	10
17. Bilag B Underdatabehandlere .....	12
18. Bilag C Instruks vedrørende behandling af personoplysninger .....	13

## 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 Netværkspraksis Danmarks platform, 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 tre 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. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
10. 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<sup>1</sup> 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.

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

### **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:

1. Pseudonymisering og kryptering af personoplysninger
  2. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
  3. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
  4. 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.
5. Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.
6. 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.
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:
  1. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
  2. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
  3. 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 standardkontraktbestemmelser 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:

1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
  2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
  3. indsigt retten
  4. retten til berigtigelse
  5. retten til sletning ("retten til at blive glemt")
  6. retten til begrænsning af behandling
  7. underrettingspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
  8. retten til dataportabilitet
  9. retten til indsigt
  10. 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:
1. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondata- sikkerheden til den kompetente tilsynsmyndighed, **Datatilsynet**, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
  2. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
  3. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
  4. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, **Data-tilsynet**, 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 unødigt 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:
  1. 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
  2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
  3. 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 slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, 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. Procedurene 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 lovgivning 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 parterers underskrift (eller elektroniske accept) 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 skriftligt varsel af begge parter.
5. I stedet for fysisk underskrift kan den dataansvarlige og databehandleren indgå og acceptere disse Bestemmelser elektronisk. Dette kan ske ved, at den dataansvarlige sætter flueben i en digital checkboks (eller anden entydig digital accept), der henviser til denne databehandleraftale og angiver "Jeg har læst og accepterer databehandleraftalen".

## **15. Kontakt og henvendelser**

1. Henvendelser vedrørende denne databehandleraftale, herunder udøvelse af rettigheder eller spørgsmål om behandlingen af personoplysninger, rettes til nedenstående kontaktoplysninger hos databehandleren.
2. Databehandleren kan ligeledes rette henvendelser til den dataansvarlige via de kontaktoplysninger, som den dataansvarlige har angivet i forbindelse med oprettelse og digital accept af aftalen.
3. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner og kontaktoplysninger.

### **Netværkspraksis Danmark PS**

Henrik Rasmussen E-mail: [Henrik@Netværkspraksis Danmark.dk](mailto:Henrik@Netværkspraksis Danmark.dk)  
Tlf.: +45 61655545

## **Bilag A Oplysninger om behandlingen**

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

Databehandlerens (Netværkspraksis Danmark PS) behandling af personoplysninger sker for at udføre de tjenester, som den dataansvarlige (sundhedspersonale/klinik) har bedt om, og som kræver adgang til oplysninger om patienter eller personale. Formålet er således ikke blot at levere en generel ydelse, men at behandle personoplysninger i det omfang, det er nødvendigt for at levere ydelsen, herunder ved at:

1. Databehandleren modtager oplysninger om medarbejdere, der skal have adgang til Netværkspraksis Intra, med det formål at oprette og vedligeholde brugere på platformen. Det drejer sig om navn, e-mail, adresse, telefonnummer, nærmeste pårørende, nærmeste pårørendes telefonnummer og nærmeste pårørendes emailadresse.
2. Hvis der ønskes integration til tidsregistrerings og lønsystem, er medarbejderes cpr nummer nødvendig, for at kunne generere løn og orientere relevante myndigheder i den forbindelse.

Personoplysningerne behandles udelukkende i henhold til den dataansvarliges instrukser og til det formål at reducere administrative byrder og sikre høj kvalitet i sundhedsfaglige dokumenter.

Oplysningerne behandles kun i det omfang, det er nødvendigt for at levere de beskrevne ydelser som instrueret af den dataansvarlige. Databehandleren er ikke berettiget til at bruge eller tilgå personoplysningerne til andre formål end dem, der er beskrevet her, eller som følger af den dataansvarliges dokumenterede instruks.

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

Behandlingen omfatter følgende aktiviteter, som den dataansvarlige har instrueret Databehandleren i at udføre:

- Udarbejdelse af sundheds- faglige dokumenter som instrukser, fraser, undervisning, MUS og APV værktøjer og GDPR dokumenter etc.
- I forbindelse med disse funktioner modtager Databehandleren besvarelse af fremsendte spørgeskemaer i forbindelse med afvikling af MUS, APV og materiale til instrukser, vejledninger og fraser samt undervisning, der kan understøtte det kliniske arbejde i den enkelte klinik.

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

Databehandleren kan - på baggrund af den dataansvarliges instrukser - komme i berøring med oplysninger, som i GDPR-termer kan være almindelige (art. 6) eller følsomme (art. 9). Listen er ikke udtømmende, da konsultationer, attester m.v. kan indeholde mange slags personoplysninger, herunder:

- Oplysninger som navn, kontaktoplysninger, CPR-nummer, adresse, familie-/økonomiske forhold eller anden identificerende information, der kan fremgå af registrering eller oplysninger der tilgår Netværkspraksis Danmark.
- Eventuelt andre følsomme oplysninger (f.eks. om religiøs overbevisning, seksualitet, strafbare forhold, politiske holdninger), hvis det fremgår af de oplysninger der tilgår Netværkspraksis Danmark.

#### A.4. Behandlingen omfatter følgende kategorier af registrerede

Databehandleren kan på den dataansvarliges instruks behandle personoplysninger om:

- Personale hos den dataansvarlige (f.eks. lægesekretærer, sygeplejersker, læger), hvis, navn eller andre oplysninger fremgår af registrering i stamoplysninger eller besvarelse af spørgeskemaer som MUS og APV mv.
- Pårørende eller andre tredjeparter, som registreres som medarbejderes nærmeste pårørende.

#### A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

**Varighed (Netværkspraksis Danmark):**

- Under kontraktperioden opbevarer Netværkspraksis Danmark data, hvorefter de slettes.
- Ved aftalens ophør slettes al personoplysninger i overensstemmelse med punkt 11 i hovedaftalen, medmindre lovgivning kræver andet.

### Bilag B Underdatabehandlere

NAVN	ADRESSE	BESKRIVELSE AF BE- HANDLING
KlinikHR	<b>CVR-nummer</b> 42233161 <b>Adresse</b> Frederiksberggade 1A, 1. <b>Postnummer og by</b> 1459 København K	Opbevarelse af data for medarbejdere, til tidsregistrering for den enkelte medarbejder. Disse data anvendes desuden til integration til lønsystem (Salary) samt økonomisk overblik for kliniker.
Peoples Doctor	<b>CVR-nummer</b> 40930809 <b>Adresse</b> C/O Kensmark Teglværksvej 2 <b>Postnummer og by</b> 5600 Faaborg	AI understøttelse af konsultationsprocessen ved at generere journalnotater ud fra transskription af samtale mellem patient og behandler. Derudover forslag til ydelser, diagnosekodning, attestværktøj og patientresume, der kan dannes ud fra samtale med patienten og oplysninger fra patientens journal.
DokuDok	<b>CVR-nummer</b> 45219380	AI understøttelse af konsultationsprocessen ved at generere journalnotater ud fra transskription af samtale mellem patient og behandler. Derudover forslag til ydelser, diagnosekodning,

	<p><b>Adresse</b> Løkkesholmsvej 25</p> <p><b>Postnummer og by</b> 4750 Lundby</p>	<p>attestværktøj og patientresumé, der kan dannes ud fra samtale med patienten og oplysninger fra patientens journal.</p>
--	--------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------

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 en generel skriftlig godkendelse til at anvende underdatabehandlere. Databehandleren skal underrette den dataansvarlige om eventuelle nye eller ændrede underdatabehandlere med mindst 14 dages varsel, jf. hovedaftalens punkt 7.

## 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:

- Skaber instrukser, fraser, vejledninger, undervisning, spørgeskemaer, GDPR dokumenter mv. til brug i sundhedsmæssigt arbejde til at understøtte bæredygtig praksisdrift og høj faglig kvalitet i det kliniske arbejde.
- Stiller hjælpeværktøjer til rådighed, hvor brugeren kan få adgang til instrukser, fraser, vejledninger, GDPR dokumenter, MUS og APV til understøttelse af det kliniske arbejde.
- Opbevarer personoplysninger så længe der er samarbejdsaftale mellem parterne.
- Sletter data, når det ikke længere er nødvendigt for det formål, brugeren har instrueret databehandleren i.

### C.2. Behandlingssikkerhed

Behandlingen omfatter helbredsoplysninger (GDPR art. 9) og kræver et højt sikkerhedsniveau. Databehandleren er forpligtet til at træffe passende tekniske og organisatoriske foranstaltninger for at etablere det nødvendige sikkerhedsniveau. Følgende foranstaltninger er minimumskrav, der altid gennemføres i samarbejde med den dataansvarlige:

- Data krypteres i transit (TLS/HTTPS) og ved lagring hos eksterne hostingudbydere
- Adgangskontrol, logning og tofaktorgodkendelse sikrer vedvarende fortrolighed, integritet og tilgængelighed.
- Regelmæssige opdateringer og sikkerhedspatches udføres på systemer og infrastruktur.
- Logfilerne indeholder udelukkende tekniske metadata (tidspunkt, bruger-ID, IP-adresse m.v.) og ingen følsomme personoplysninger eller transskriberet indhold.

- En incident response-procedure gør det muligt hurtigt at reagere på og rapportere sikkerhedshændelser (jf. 24-timers underretningspligt).

Hvis den dataansvarlige kræver yderligere sikkerhedsforanstaltninger (f.eks. specifikke certificeringer, avanceret netværkssegmentering eller fysisk overvågning), kan dette aftales særskilt og implementeres i det omfang, det er praktisk gennemførligt. Databehandleren forpligter sig til løbende at vurdere og tilpasse sikkerhedsniveauet efter den aktuelle risiko, de teknologiske muligheder og den dataansvarliges instrukser.

### **C.3. Bistand til den dataansvarlige**

Databehandleren bistår den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2, så vidt det er muligt, og inden for det nedenstående omfang og udstrækning:

- Rettigheder og forespørgsler håndteres ved, at den dataansvarlige via Netværkspraksis Danmarks brugerflade. Såfremt en medarbejder anmoder om indsigt eller sletning af data, kan dataansvarlig således kontakte Netværkspraksis Danmarks support for yderligere hjælp.
- Underretning ved brud på persondatasikkerheden sker ved, at Databehandleren inden for 24 timer meddeler den dataansvarlige om hændelsen og fremlægger relevant dokumentation (f.eks. logfiler, tekniske forklaringer) for at lette den dataansvarliges eventuelle indberetning til Datatilsynet.
- Konsekvensanalyser (DPIA) understøttes ved, at Databehandleren stiller relevante oplysninger om tekniske og organisatoriske foranstaltninger til rådighed på forespørgsel. Hvis den dataansvarlige planlægger nye eller ændrede behandlingsaktiviteter, kan Databehandleren desuden hjælpe med tekniske beskrivelser og vurderinger af sikkerheden, så den dataansvarlige kan foretage en fyldestgørende vurdering af mulige risici

Hvis den dataansvarlige har behov for yderligere bistand udover ovennævnte punkter, kan dette aftales særskilt. Databehandleren forpligter sig i givet fald til at bidrage i det omfang, de tekniske og praktiske rammer muliggør det.

### **C.4. Opbevaringsperiode/sletterutine**

#### **Opbevaringsperiode/sletterutine (Netværkspraksis Danmark): • Under kontraktperioden:**

Al data opbevares under kontraktperioden og slettes på dataansvarligs anmodning, senest efter 24 timer/24 timer.

#### **ophør af tjenesten:**

Databehandleren sletter alle oplysninger i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige har ændret sit oprindelige valg eller anden lovgivning kræver opbevaring.

### **C.5. Lokalitet for behandling**

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke ske på andre lokaliteter end følgende:

Netværkspraksis Danmark, Ndr. Ringvej 85,1, 6000 Kolding, Danmark.

Den dataansvarlige henvises til underdatabehandlernes til enhver tid gældende dokumentation for opdaterede oplysninger om præcise adresser og datacenter-lokationer.

Ingen yderligere lokaliteter tages i brug uden forudgående skriftlig godkendelse fra den dataansvarlige. 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.6. Instruks vedrørende overførsel af personoplysninger til tredjelande**

### **Overførsel til tredjelande (Netværkspraksis Danmark):**

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. Som udgangspunkt sendes data aldrig uden for EU/EØS.

## **C.7. Procedurer for den dataansvarliges revisioner, herunder inspektioner**

Den dataansvarlige har ret til at føre tilsyn med databehandlerens overholdelse af disse Bestemmelser, jf. afsnit C.8. I den forbindelse gælder følgende:

- Tilsyn kan som udgangspunkt gennemføres på skriftligt grundlag. Databehandleren skal stille nødvendig dokumentation og relevante rapporter til rådighed, så den dataansvarlige kan vurdere overholdelsen af databeskyttelsesforordningen.
- Hvis den dataansvarlige ønsker et fysisk tilsyn hos Netværkspraksis Danmark, skal dette aftales med et skriftligt varsel på mindst 30 dage, medmindre der er påvist væsentlige afvigelser eller brud på persondatasikkerheden, som kræver hurtigere handling. Fysiske inspektioner kan som udgangspunkt højst foretages én gang årligt, medmindre der er konkrete indikationer på overtrædelser eller brud.
- For så vidt angår underdatabehandlernes, anerkender parterne, at dataansvarlig selv er forpligtet til at kontakte disse, ved ønske om eller behov for tilsyn.

Denne bestemmelse sikrer, at den dataansvarlige kan føre kontrol med behandlingens lokation og sikkerhedsniveau *uden* at forstyrre driften unødigt, og at eventuelle fysiske tilsyn koordineres på en rimelig måde.

### **Revisioner (Netværkspraksis Danmark):**

- Databehandleren skal efter anmodning fra den dataansvarlige kunne fremlægge relevante revisions-/inspektionsrapporter.
- Den dataansvarlige eller en repræsentant kan gennemføre inspektioner på Netværkspraksis Danmarks fysiske lokaliteter når det er aftalt eller nødvendigt for at sikre overholdelse af GDPR.

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

### **Revisioner hos underdatabehandlere (Netværkspraksis Danmark):**

- Databehandleren skal (f.eks. årligt) kunne indhente en uafhængig tredjepartsrapport vedr. underbehandlere
- Dokumentation fremsendes uden unødigt forsinkelse til den dataansvarlige, hvis den dataansvarlige ønsker det.
- Hvis rapporten ikke giver tilstrækkelig sikkerhed, kan den dataansvarlige anmode om yderligere foranstaltninger eller en ny inspektion.