Databehandleraftale vedrørende brug af WebReq

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

Version 4.1 – 22/10/2026

mellem

[KLINIK NAVN]
CVR-nr.: [CVR-NR]
[ADRESSE]
[POSTNUMMER OG BY]
[LAND]

herefter ”den dataansvarlige”

og

NEXUS / E-SUNDHED A/S
CVR-nr.: 32645534
Odeons Kvarter 19, 2. tv.
5000 Odense C
Danmark

herefter ”databehandleren”

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

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

1. Indhold

2. Præambel ... 3
3. Den dataansvarliges rettigheder og forpligtelser ... 4
4. Databehandleren handler efter instruks ... 4
5. Fortrolighed ... 4
6. Behandlingssikkerhed ... 5
7. Anvendelse af underdatabehandlere ... 6
8. Overførsel til tredjelande eller internationale organisationer ... 7
9. Bistand til den dataansvarlige ... 7
10. Underretning om brud på persondatasikkerheden ... 8
11. Sletning og returnering af oplysninger ... 9
12. Revision, herunder inspektion ... 9
13. Parternes aftale om andre forhold ... 9
14. Ikrafttræden og ophør ... 10
15. Kontaktoplysninger hos den dataansvarlige og databehandleren ... 10
Bilag A Oplysninger om behandlingen ... 11
Bilag B Underdatabehandlere ... 12
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 "WebReq", som er et webbaseret laboratorierekvireringssystem til læger, speciallæger, hospitaler og andre sundhedsfaglige institutioner, klinikker, laboratorier m.fl., og også omfatter indsamling af borgeres PRO-data via indtastning (spørgeskemaer) i Web-Patient.dk, hvor relevant 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[1] nationale ret og disse Bestemmelser.

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

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

4. Databehandleren handler efter instruks

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

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

5. Fortrolighed

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

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

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

6. Behandlingssikkerhed

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

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

   a. Pseudonymisering og kryptering af personoplysninger

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

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

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

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

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

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

7. Anvendelse af underdatabehandlere

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

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

3. Forud for skift af underdatabehandler informeres dette via WebReq så det er muligt for den dataansvarlige at gøre en indsigelse. Indsigelsesfristen er 14 dage inden accept. 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 hvis muligt i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

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

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

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

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

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

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

9. Bistand til den dataansvarlige

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

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

    a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    c. indsigtsretten
    d. retten til berigtigelse
    e. retten til sletning (”retten til at blive glemt”)
    f. retten til begrænsning af behandling
    g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering.

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

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

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

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

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

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

10. Underretning om brud på persondatasikkerheden

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

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

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

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

b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

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

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

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at 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.

12. Revision, herunder inspektion

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

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

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

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

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

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

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

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

5. Underskrift

   På vegne af den dataansvarlige

   [KLINIK NAVN]
   CVR-nr.: [CVR-NR]
   [ADRESSE]
   [POSTNUMMER OG BY]
   [LAND]

   På vegne af databehandleren

   NEXUS / E-SUNDHED A/S
   CVR-nr.: 32645534
   Odeons Kvarter 19, 2. tv.
   5000 Odense C
   Danmark

15. Kontaktoplysninger hos den dataansvarlige og databehandleren

1. Den dataansvarlige kan kontakte databehandleren via nedenstående oplysninger. Databehandleren benytter de eksisterende kanaler til at kontakte den dataansvarlige.
   Dataansvarlige: WebReq, mail eller telefonisk

   Databehandleren: DPO@nexus-esundhed.dk

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

Bilag A Oplysninger om behandlingen

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

WebReq anvendes til rekvirering af laboratorieundersøgelser og PRO-skemaer (indsamling af borgernes data via spørgeskemaer i Web-Patient.dk), hvor relevant, i sundhedsvæsenet og i sundhedsvæsenets dialog med borgeren, herunder bestilling kvalitetskontrol og Mobil-Lab.

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er, at databehandleren rekvirerer laboratorieanalyser, implementerer, supporterer, vedligeholder og eventuelt videreudvikler systemet med testdata.

PRO-skemaer videredeles til KIH-databasen, hvorfra den overførte data vil blive udstillet på sundhed.dk.
Formålet med databehandlingen er at dele og skabe overblik over relevante data i et behandlingsforløb på tværs af sundhedsvæsenets aktører gennem opsamling og deling af patienters hjemmemonitorerede og patientrapporterede helbredsoplysninger i den fælles digitale infrastruktur for dokumentdeling.

For praktiserende speciallæger gælder, at PRO-data videregives til kliniske kvalitetsdatabaser, der er godkendt af Sundhedsdatastyrelsen, hvor det er relevant. jf. Sundhedsloven §196 & BEK nr. 881 af 26/06/2018 Bekendtgørelse om godkendelse af landsdækkende og regionale kliniske kvalitetsdatabaser.

Derudover kan anonymiserede data fra PRO-skemaer anvendes og videregives til relevante forsknings- og kvalitetsenheder (f.eks. Forskningsenheden for Almen Praksis) med henblik på kvalitetssikring og validering af PRO-skemaer, herunder pilotafprøvning af nye eller reviderede skemaer

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

Databehandlerens behandling af personoplysninger sker primært ved, at denne implementerer, supporterer, vedligeholder og eventuelt videreudvikler WebReq.

Herigennem understøtter databehandleren den dataansvarlige med følgende behandlingsaktiviteter: indsamling, registrering, opbevaring, tilpasning, ændring, fremsøgning, videregivelse, sletning mv. af personoplysninger.

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

Borgerens navn, adresse, telefonnummer, mail, helbredsoplysninger og CPR-nr.
Lægens/sundhedspersoners navn, adresse, lokationsnummer og ydernummer.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Borgere, læger og sundhedspersoner.

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.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
DataGruppen MultiMed A/S	19403742	Storhaven 12, DK-7100 Vejle	Hosting, Videregivelse og Transmission
Region Nordjylland	29190941	Niels Bohrs Vej 30 DK-9220 Aalborg Øst	Videregivelse af PRO-data til KIH-databasen

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet.
Forud for skift af underdatabehandler informeres dette via WebReq, så det er muligt for den dataansvarlige at gøre en indsigelse. Indsigelsesfristen er 14 dage inden accept.

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:

- Indsamling - Borgers PRO-data indsamles via indtastning i Web-Patient.dk.
- Registrering - Sundhedspersoner kan oprette data (rekvisitioner).
- Organisering/systematisering - Data opbevares organiseret for at kunne tilbyde brugere adgang til relevante oplysninger.
- Opbevaring - Borgeres personoplysninger og helbredsoplysninger opbevares i de tidsrammer, der er angivet i sundhedsloven.
- Tilpasning eller ændring.
- Genfinding - Borgere og sundhedspersoner kan udsøge historisk data (80 dage).
- Søgning - Sundhedspersoner kan fremsøge relevante data på borgere.
- Videregivelse ved transmission - Rekvisitioner og PRO-skemaer transmitteres til lægesystemer og KIH-databasen.
- Sammenstilling eller samkøring - Oplysninger i systemet sammenstilles med oplysninger indhentet fra nationale registre, f.eks. Det Danske Vaccinationsregister.
- Sletning eller tilintetgørelse - Oplysninger vil blive slettet i overensstemmelse med bestemmelser om ophør i leveringskontrakten.
- Support – Data kan anvendes til fejlsøgning og anvenderhjælp.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen omfatter almindelige personoplysninger samt helbredsoplysninger omfattet af databeskyttelsesforordningens artikel 6 og 9, samt CPR-oplysninger omfattet af databeskyttelseslovens § 11.

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

C.2.1 Pseudonymisering og kryptering
Der må kun etableres eksterne kommunikationsforbindelser, hvis forbindelsen er krypteret f.eks. til webside, front-ends og loginportaler. Dette gælder også forbindelser til underleverandøren f.eks. site-to-site forbindelse eller IP-filtrering.
Ved fortrolige og følsomme personoplysninger forventes der en stærk kryptering. HTTPS og nyeste eller næst nyeste version af TLS er et krav.
E-mails indeholdende fortrolige og følsomme personoplysninger skal også være beskyttet af kryptering.

C.2.2 Uddannelse og instruktion
Der stilles krav om, at alle ansatte hos databehandleren modtager den tilstrækkelig uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning samt databehandlerens og den dataansvarliges politikker og procedurer herfor.

C.2.3 Autorisation og adgangskontrol, herunder kontrol med afviste adgangsforsøg
Der skal gennemføres styring af den generelle adgang til personoplysninger.
Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har brug for.
Der gennemføres begrænsninger i adgangen til systemer og personoplysninger, der

behandles i henhold til databehandleraftalen, ved at definere brugerroller, for så vidt det er muligt, og ved at tildele privilegerede adgangsrettigheder samt at udføre attestering af brugere.

Databehandleren skal træffe foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, som den pågældende er autoriseret til.

Der skal gøres brug af sikre adgangskoder/passwords og autentifikation – samt multifaktorautentifikation ved adgang fra det åbne internet – eller tilsvarende sikkerhedsniveau, ved adgang til systemer eller personoplysninger, der behandles i henhold til databehandleraftalen.

Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

Databehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for brugere, der efter en konkret vurdering ikke længere bør have disse.

C.2.4 Genoprettelse af tilgængelighed i tilfælde af fysisk eller teknisk hændelse (backup og håndtering af driftsafbrydelser)
Der gælder de samme retningslinjer for backup som for al anden behandling af personoplysninger, der behandles i henhold til databehandleraftalen.

Databehandleren skal sikre, at der foretages regelmæssig backup af systemer og personoplysninger, der behandles i henhold til databehandleraftalen.

Backup skal opbevares adskilt fra serveren i et ikke tilstødende rum for at sikre, at denne ikke går tabt. Backup skal beskyttes, og opbevaring af backup skal altid ske på betryggende vis, så denne ikke fortabes.

Databehandleren skal regelmæssigt kontrollere, at backup er læsbart. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af et systems tekniske set-up.

Databehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.

Databehandleren skal regelmæssigt afprøve og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser. Den dataansvarlige kan anmode om at få dokumentation for dette stillet til rådighed.

C.2.5 Opdateringer og ændringer
Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.

C.2.6 Fysisk sikring
Databehandleren skal sikre, at it-udstyr, der anvendes i forbindelse med databehandlingen, er fysisk sikret i henhold til gældende lovkrav.

Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal desuden evaluere og forbedre effektiviteten af sådanne forholdsregler, hvor det er nødvendigt.

Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af mobile lagringsmedier.

I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier, skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov. Dette skal ske efter best-practice.

Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller afmagnetiseres, så der sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal opbevares i den periode, databehandlingen foregår og forevises, når den dataansvarlige anmoder herom.

C.2.7 Anvendelse af hjemme-/ad hoc-arbejdspladser

Ved anvendelse af hjemme-/ad hoc-arbejdspladser skal der anvendes fler-faktor-login (multifactor autentifikation) eller tilsvarende sikkerhedsniveau samt hensyntagen til time-out.

Databehandleren og dennes autoriserede medarbejdere må foretage databehandling fra mobile arbejdspladser, herunder med adgange til den dataansvarliges personoplysninger over internettet, såfremt databehandlingen sker fra arbejdspladser, som er underlagt databehandlerens egne sikkerhedsregler. Databehandlingen skal endvidere ske i overensstemmelse med databehandleraftalen og denne instruks.

Hjemme-/ad hoc-arbejdspladserne skal være sikret med tekniske kontroller, der sikrer, at behandlingen af personoplysninger sker i overensstemmelse med gældende lovgivning og den dataansvarliges og databehandlerens retningslinjer.

Det skal sikres, at uvedkommende ikke får adgang til personoplysninger, der behandles ved hjemmearbejdspladser, ligesom de enkelte medarbejdere skal instrueres i, hvordan uvedkommende ikke får adgang.

C.2.8 Logning

Der skal foretages maskinel registrering (logning) ved al behandling af personoplysninger.

Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium.

Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode, af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

C.3 Bistand til den dataansvarlige

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

Foranstaltningerne fremgår af afsnit C.2. Databehandleren bistår herudover den dataansvarlige med at besvare anmodninger om udøvelse af de registreredes rettigheder (Bestemmelse 9.1) og med at overholde forpligtelserne ved brud på persondatasikkerheden (Bestemmelse 9.2 og 10).

C.4 Opbevaringsperiode/sletterutine

Oplysningerne i Webreq lagres i 200 dage efter prøvetagningsdato. Hvis der ikke er sket en prøvetagning, slettes oplysningerne.

Hvis der er sket en prøvetagning, lagres oplysningerne i 80 dage herefter inden oplysningerne slettes.

PRO-skemaer opbevares i op til 2 år, herefter slettes skemaerne.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse Bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

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:

Virksomhedens navn og adresse	CVR (eller tilsvarende)	Lokalitet for behandling
NEXUS / E-SUNDHED A/S	32645534	Odeons Kvarter 19, 2. tv., 5000 Odense, Danmark
Data Gruppen MultiMed A/S	19403742	Storhaven 12, 7100 Vejle, Danmark
Region Nord, KIH-database	29190941	Niels Bohrs Vej 30, 9220 Aalborg Øst

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Der må i forbindelse med behandlingen ikke overføres personoplysninger til tredjelande, med mindre den dataansvarlige udtrykkeligt har godkendt dette skriftligt på forhånd.

Hvis den dataansvarlige ikke i disse bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren
Databehandleren skal årligt for egen regning indhente en revisionsrapport 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 én af følgende typer af erklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

ISO 27001 i kombination med ISO27701 eller ISAE 3000 revisionserklæring

ISO27001 & ISO27701
Databehandleren er forpligtet til at opretholde både ISO 27001 (informationssikkerhed) og ISO 27701 (privatlivsbeskyttelse). Dokumentation på databehandlerens efterlevelse af ISO-standarderne skal, efter anmodning, fremsendes til den dataansvarlige.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at føre tilsyn, herunder fysisk tilsyn, hos underdatabehandleren, når der efter databehandlerens vurdering opstår et behov herfor. Et sådan tilsyn skal varsles med mindst 2 måneder.

Databehandleren modtager betaling for sin bistand til sådanne yderligere revisioner, herunder kontrolbesøg, baseret på medgået tid. Betalingen vil blive beregnet ud fra en timepris, der fastsættes i overensstemmelse mellem parterne.

Som led i ovenstående certificeringer er databehandleren forpligtet til årligt at følge op på eventuelle underdatabehandlere. Dette sker for databehandlerens egen regning.

Databehandleren er forpligtet til uden unødigt ophold at underrette den dataansvarlige såfremt ISO 27001 eller ISO 27701-certificeringen ikke opretholdes.

ISAE 3000 revisionserklæring
En revisionserklæring kan laves på den dataansvarliges regning efter aftale mellem partnerne. Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering.

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

Databehandler er ansvarlig for, at dennes underdatabehandlere overholder de forpligtelser, der måtte følge af denne aftale, samt de til enhver tid gældende databeskyttelsesretlige regler.
Det påhviler databehandleren at sikre passende kontrol med dennes underdatabehandlere, herunder revision og tilsyn, i et sådant omfang, at databehandler kan dokumentere underdatabehandlers overholdelse af de forpligtelser, der måtte følge af denne aftale samt de til enhver tid gældende databeskyttelsesretlige regler. Denne dokumentation skal, efter anmodning, fremsendes til den dataansvarlige.