Databehandleraftale

Mellem

Den dataansvarlige

CVR

Adresse

Post nr og by

Danmark

og

Databehandleren

Software Fabric

CVR 30276981

Reberbanevej 8

8900 Randers C

Danmark

1 Indhold

2 Baggrund for databehandleraftalen 3

3 Den dataansvarliges forpligtelser og rettigheder 4

4 Databehandleren handler efter instruks 4

5 Fortrolighed 4

6 Behandlingssikkerhed 5

7 Anvendelse af underdatabehandlere 5

8 Overførsel af oplysninger til tredjelande eller internationale organisationer 7

9 Bistand til den dataansvarlige 7

10 Underretning om brud på persondatasikkerheden 9

11 Sletning og tilbagelevering af oplysninger 9

12 Tilsyn og revision 9

13 Parternes aftaler om andre forhold 10

14 Ikrafttræden og ophør 10

15 Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren 12

Bilag A Oplysninger om behandlingen 13

Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere 14

Bilag C Instruks vedrørende behandling af personoplysninger 15

Bilag D Parternes regulering af andre forhold 18

2 Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Aftalen 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 beskytte/se 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),* som stiller specifikke krav til indholdet af en databehandleraftale.

3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes Leje og brugsaftale af software ”Planner4You”

4. Databehandleraftalen og "Leje og brugsaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog - uden at opsige "hovedaftalen" - erstattes af en anden gyldig databehandleraftale.

5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

6. Til denne aftale hører fire bilag. Bilagene fungerer som en integreret del af databehandleraftalen.

7. Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

8. Databehandleraftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.

9. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

10. Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandleraftalen eller parternes "hovedaftale".

11. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

12. Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

3 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, 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; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn **til** vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.

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

5 Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.

3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

4. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

6 Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

2. Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

    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

3. Databehandleren skal i forbindelse med ovenstående - i alle tilfælde - som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.

4. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

7 Anvendelse af underdatabehandlere

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

2. Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige.

3. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

4. Den dataansvarliges nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.

5. Den dataansvarliges eventuelle godkendelse af specifikke underdatabehandlere er anført i denne aftales Bilag B.

6. Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat **i** denne databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene databeskyttelsesforordningen.

   Databehandleren er således ansvarlig for - igennem indgåelsen af en underdatabehandleraftale - at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.

7. Underdatabehandleraftalen 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 der er indgået en gyldig aftale mellem databehandleren og underdatabehandleren. Eventuelle kommercielle vilkår, f.eks. priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

8. Databehandleren skal **i** sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand **i** tilfælde af databehandlerens konkurs, så den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

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

8 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.

2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren - indenfor rammerne af databehandleraftalen - derfor bl.a. ikke;

    a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
    b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
    c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

3. Den dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

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 3.

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige 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. den registreredes indsigtsret
    d. retten til berigtigelse
    e. retten til sletning (»retten til at blive glemt«)

f. retten til begrænsning af behandling
g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

   Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
   b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
   c. forpligtelsen til - uden unødig forsinkelse - at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
   d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
   e. forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, hvis 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. Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

10 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

   Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter at denne er blevet bekendt med bruddet, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 10.2., litra b, skal databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne - bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden. Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:

   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. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
   c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

11 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

12 Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, 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. Den nærmere procedure for den dataansvarliges tilsyn med databehandleren fremgår af denne aftales Bilag C.

3. Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.

4. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13 Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgå af parternes Leje og brugsaftale1 eller af denne aftales Bilag D.

2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes [11]hovedaftale[11] eller af denne aftales Bilag D.

14 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift heraf.

2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.

3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes [11]hovedaftale[11] eller af denne aftales bilag D.

4. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af [11]hovedaftalen[11] .

5. Aftalen er gældende, så længe behandlingen består. Uanset [11]hovedaftalens[11] og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

6. Underskrift

På vegne af den dataansvarlige	På vegne af databehandleren
Navn:	Navn: Dennis Sørensen
Stilling:	Stilling: Direktør
Dato	
Underskrift:	

15 Kontaktpersoner / kontaktpunkter hos den dataansvarlige og databehandleren

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

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Navn:	Navn: Dennis Sørensen
Stilling:	Stilling: Direktør
Telefonnummer:	Telefonnummer: 88138120
E-mail:	E-mail: info@planner4you.dk

Bilag A Oplysninger om behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

- at den dataansvarlige kan anvende systemet "Planner4You", som ejes og administreres af databehandleren, til at indsamle og behandle oplysninger om den dataansvarliges medarbejdere og tilknyttede borgere.

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

- at databehandleren stiller systemet "Planner4You" til rådighed for den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges medarbejdere og tilknyttede borgere på databehandlerens servere.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- Almindelige personoplysninger
- Følsomme personoplysninger
- Nationalt regulerede personoplysninger - herunder:
    - Oplysninger om strafbare forhold
    - Oplysninger om CPR-nummer

Behandlingen omfatter følgende kategorier af registrerede:

- Medarbejdere hos den dataansvarlige.
- Borgere tilknyttet den dataansvarliges institutioner og bosteder.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

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

Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

B.1 Betingelser for databehandlerens brug af eventuelle underdatabehandlere

Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum 3 måneder før anvendelsen eller ændringen skal træde i kraft. Hvis den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 30 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

B.2 Godkendte underdatabehandlere

Databehandleren har en underdatabehandler aftale med:

MedCom

Forskerparken 10

5230 Odense M

Denne underdatabehandleraftale er etableret idet Planner4You benytter Sundheds datanettet.

MedCom Har etablevet underdatabehandleraftale med flere danske IT-leverandører, som, der er etableret gyldige underdatabehandleraftaler med.

Sinch Denmark ApS

Fruebjergvej 3

2100 Copenhagen

Denne underdatabehandleraftale er etableret, idet Databehandleren tilbyder en sms-service til den dataansvarlige, hvor informationer formidles vis underdatabehandleren.

B.3 Datacenter

Databehandlerens egne servere er at hensyn til datasikkerhed, placeret hos eksternt datacenter. Datacenteret har ingen adgang til data, og er dermed ikke underdatabehandler.

Serverne er placeret hos Fuzion A/S. Databehandleren har deres ISAE 3402 erklæring.

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:

- Databehandleren stiller systemet "Planner4You" til rådighed for den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges medarbejdere og tilknyttede borgere på databehandlerens servere.

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

At der er tale om behandling af en stor mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et "højt" sikkerhedsniveau.

Nærværende bilag har til formål at definere de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren er forpligtet til at implementere:

1. ORGANISERING AF INFORMATIONSSIKKERHEDEN
   1.1. Databehandleren skal træffe de nødvendige tekniske og organisatoriske foranstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen.
   1.2. Databehandleren skal nærmere præcist træffe de tekniske og organisatoriske foranstaltninger, som fremgår af nærværende bilag.

1. INTERNE SIKKERHEDSRETNINGSLINJER
   1.1. Databehandleren skal fastsætte og gennemføre interne risikobaserede retningslinjer for sikker behandling af personoplysninger i overensstemmelse med den til enhver tid gældende lovgivning om behandling af personoplysninger.
   1.2. Databehandleren skal desuden implementere en databeskyttelsespolitik i overensstemmelse med databeskyttelsesforordningens artikel 24(2).
   1.3. Databehandlerens relevante interne retningslinjer skal gennemgås mindst en gang om året med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold.

2. MEDARBEJDERSIKKERHED
   2.1. Alle personoplysninger skal behandles fortroligt. I overensstemmelse med Aftalens afsnit 5.3 har medarbejdere hos databehandleren tavshedspligt om alle de personoplysninger, som de får adgang til i forbindelse med databehandlingen.
   2.2. Alle databehandlerens medarbejdere med adgang til den dataansvarliges data skal sikkerhedsgodkendes efter databehandlerens faste procedure herfor.
   2.3. Databehandleren skal udarbejde en udtrykkelig liste over de af databehandlerens medarbejdere, som er sikkerhedsgodkendt og autoriseret til at tilgå eller modtage den dataansvarliges informationer.

3, FYSISK SIKKERHED OG IT-SIKKERHED

3.1. Der skal træffes sikkerhedsforanstaltninger til hindring af uvedkommendes adgang til personoplysninger, som databehandleren behandler i medfør af nærværende Aftale.

3.2. Hvis databehandlerens ansatte anvender hjemmearbejdsplads til behandling af personoplysninger, skal Leverandøren indestå for, at de interne sikkerhedsforanstaltninger overholdes inden for rammerne af Datatilsynets retningslinjer om anvendelse af hjemmearbejdspladser.

4. SIKRING AF UDSTYR

4.1. I forbindelse med reparation, service eller destruktion af udstyr og medier, som indeholder personoplysninger omfattet af nærværende Aftale, skal det sikres, at uvedkommende ikke får adgang til personoplysningerne.

5. TRANSMISSION AF OPLYSNINGER OVER INTERNETTET

5.1. Ved tilslutning til internet eller andre åbne net skal der træffes foranstaltninger, som sikrer imod, at uvedkommende får adgang til databehandlerens interne net.

5.2. Ved transmission af personoplysninger over det åbne internet (f.eks. e-mail) skal databehandleren efterleve følgende minimumskrav:

5.2.1. Transmission af fortrolige personoplysninger skal ske ved forsvarlig kryptering baseret på en anerkendt algoritme (AES eller tilsvarende).

5.2.2. Sikkerhed for afsenders og modtagers identitet (autencitet) skal sikres i nødvendigt omfang ved anvendelse af f.eks. digital signatur eller individuelle, fortrolige adgangskoder.

6, SLETNING AF PERSONOPLYSNINGER

2.1. Papirdokumentation skal makuleres, når der ikke længere er behov for at opbevare personoplysningerne. Personoplysninger, der opbevares digitalt, skal slettes på en anerkendt måde, når der ligeledes ikke er behov for opbevaring af oplysningerne.

3. LOGNING

3.1. Alle transaktioner med fortrolige personoplysninger skal logges, og loggen skal indeholde oplysninger om,

3.1.1. Tidspunkt,

7.1.2.Bruger,

7.1.3. Type af anvendelse,

7.1.4. Angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

7.2. Loggen skal opbevares i seks måneder, hvorefter den skal slettes.

7.3. Databehandleren er ligeledes forpligtet til at udlevere udskrifter/give den dataansvarlige adgang til logs, efter anmodning fra den øverste sikkerhedsansvarlige hos den dataansvarlige.

8, ADGANGSSTYRING

8.1. Kun de personer hos databehandleren, som er autoriseret hertil, må have adgang til personoplysningerne. Der må ikke gives adgangsrettigheder til personoplysningerne i videre omfang, end de pågældende har behov for i forhold til deres jobfunktion.

8.2. Brugeradgange til fortrolige personoplysninger skal revurderes årligt.

8.3. Medarbejderens adgangskoder skal være tilstrækkeligt komplekse.

8.4. Der skal føres kontrol med afviste adgangsforsøg, og der skal blokeres for yderligere forsøg efter flere på hinanden følgende adgangsforsøg inden for den fastsatte, almindelige arbejdsdag.

8.5. Databehandleren må ikke anvende software, programmel og hardwarekonfigurationer med kendte svagheder og sårbarheder, som kan udnyttes til at få adgang til personoplysningerne.

C.3 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

C.4 Lokalitet for behandling

Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de følgende:

- Software Fabric ApS, Reberbanevej 8, 8900 Randers C
- Databehandlerens servere fysisk placeret i aflåst rack i Nianets co-location faciliteter, Silkeborgvej 53, 8000 Aarhus C. Det er udelukkende autoriserede medarbejdere hos databehandleren, der har adgang til serverne.

C.5 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande

Databehandleren overfører ikke personoplysninger til tredjelande.

C.6 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Databehandleren skal i december hvert år indhente en erklæring fra en uafhængig revisor eller anden ekspert angående databehandlerens overholdelse af kravene til sikkerhed i Aftalens punkt 6 og 10 samt relevante bilag.

Revisionserklæringen gøres snarest muligt efter indhentelsen tilgængelig for den dataansvarlige til orientering.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at føre tilsyn, herunder fysisk tilsyn, hos databehandleren, når der efter den dataansvarliges vurdering opstår et behov herfor.

Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sit fysiske tilsyn. Ønsker den dataansvarlige yderligere oplysninger, udover den beskrevne årlige erklæring, skal den Dataansvarlige betale for den medgåede tid hos Databehandleren.

C.7 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

Databehandleren eller en repræsentant for databehandleren foretager et fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos underdatabehandleren.

Udover det planlagte tilsyn, kan der føres tilsyn med underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.

Dokumentation for de afholdte tilsyn sendes snarest muligt til orientering hos den dataansvarlige.

Bilag D Parternes regulering af andre forhold