Databehandleraftale (gældende kommunal standard)

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

mellem din institution jf. accept ved aftale om licens til ”Pakketilbud” til SMART Kompetencehjulet - herefter ”den dataansvarlige”

og

LearnLab ApS
CVR 30 08 60 23
Hobrovej 91
9240 Nibe
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

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 SMART Kompetencehjulskonceptet: 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 fire 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. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. 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.

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

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.

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 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 60 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.

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 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 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:

   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 dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne. Sletningen sker gennem forntendbrugerfladen, hvor den dataansvarlige tildeles en eller flere brugere, som

definitivt kan slette data – både løbende og under kontraktperiodens og ved ophør af denne.

2. Databehandleren forpligter sig til efter ophør af tjenesterne vedrørende behandlingen af personoplysningerne alene at behandle til de(t) formål, i den periode og under de berettigelse, som særlige regler i EU-retten eller medlemsstaternes nationale ret forsvinder

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 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 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 skriftlig varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige

Navn
Stilling
Telefonnummer
E-mail

Underskrift og dato jf. accept i mail ved bestilling af licens til ”Pakketilbud” til SMART Kompetencehjulet

På vegne af databehandleren

Navn	Ethel Hansen
Stilling	Direktør
Telefonnummer	96352807
E-mail	info@learnlab.dk

Underskrift og dato jf. accept i mail ved bestilling af licens til ”Pakketilbud” til SMART

---

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Den dataansvarlige:
jf. accept i mail ved bestilling af licens til ”Pakketilbud” til SMART

Databehandleren:

Navn	Rikke Hansen
Stilling	IT og support
Telefonnummer	96352807
E-mail	rih@learnlab.dk

Bilag A Oplysninger om behandlingen

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

Databehandleren behandler personoplysninger på vegne af den dataansvarlige til levering af systemet Kompetencehjulskonceptet:

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

Databehandlerens behandling består i hosting af systemet og driftsovervågning.

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

Behandlingen indeholder personoplysninger i de nedenfor afkrydsede kategorier.

A.3.1 Almindelige personoplysninger (jf. databeskyttelsesforordningens artikel 6)

☒ Almindelige personoplysninger:

[*Angiv typen/typerne af personoplysninger – f.eks. navn, e-mail, adresse]:*
Børn: Navn, fødselsdato
Personale: Navn, e-mail, organisatorisk tilhørsforhold
Forældre: Navn og e-mail (ifm. adgang til deres barns data)

A.3.2 Følsomme personoplysninger (jf. databeskyttelsesforordningens artikel 9)

☐ Race eller etnisk oprindelse
☐ Politisk overbevisning
☐ Religiøs overbevisning
☐ Filosofisk overbevisning
☐ Fagforeningsmæssigt tilhørsforhold
☐ Genetiske data
☐ Biometriske data
☒ Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v.
☐ Seksuelle forhold eller seksuel orientering

[*Angiv hvilke oplysninger i kategorierne hvis relevant/særligt – f.eks. fingeraftryk i biometriske personoplysninger*]:
I forbindelse med udarbejdelse af handleplan og statusplan kan det være nødvendigt at angive helbredsforhold og lignende, der har betydning for forståelse af behov for f.eks. bevilling af støtte

A.3.3 Personoplysninger om straffedomme og lovovertrædelser (jf. databeskyttelsesforordningens artikel 10):

☐ Straffedomme
☐ Lovovertrædelser

A.3.4 Oplysninger om CPR-nummer (jf. databeskyttelsesforordningens artikel 87 og databeskyttelseslovens § 11):

☒ CPR-numre

A.3.5 Andre personoplysninger (f.eks. væsentlige sociale problemer eller andre rent private forhold):
Børn: Udviklingsmæssige oplysninger

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Børn på 0-6 år der er indmeldt i den dataansvarliges sundhedspleje, dagtilbud og dagpleje
- Pædagogisk personale og sundhedsplejersker ansat i sundhedspleje, dagtilbud og dagpleje
- Administrativt personale ansat i den dataansvarliges organisation
- Medarbejdere ved Pædagogisk Psykologisk Rådgivning (PPR) og tværfagligt ansat personale i øvrigt

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Bestemmelserne træder i kraft ved parternes underskrift og løber frem til ophøret af Hovedaftalen eller ophøret af tjenesten vedrørende behandling af personoplysninger, alt efter hvad der ophører sidst.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Team.blue: Zitcom	29 41 20 06	Højvangen 4, 8660 Skanderborg Datacenter #1: 8660 Skanderborg	Hos Zitcom anvender databehandleren løsninger underbrandet Curanet A/S til hosting af databehandlerens løsning
		Datacenter #3: 8270 Højbjerg	Backup opbevares, der sker ikke behandling af data.
Syspro ApS	45 19 34 46	I. Verlingsvej 6, 7080 Børkop	Hosting og drift af løsningen.
Vega Solutions	36 26 59 22	Sivsangervej 7 9800 Hjørring	Teknisk support og udvikling af løsningen.

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.

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:

Behandling af personoplysninger vedrørende børn på 0-6 år, der er indmeldt i den dataansvarliges dagtilbud, i forbindelse med foretagelse af vurdering af børns: sociale, personlige, motoriske, sproglige, natur og science og kulturelle udvikling, der i medfør af dagtilbudslovens § 11 er lovpligtige. Der oprettes Kompetencehjul på børn med særlige udfordringer, så handleplan/statusplan kan udarbejdes, ligesom der kan oprettes henvisning/indstilling til Pædagogisk Psykologisk Rådgivning. Der er dog mulighed for at oprette Kompetencehjul på alle børn.

Derudover foretager databehandleren udtræk af diverse statistikmateriale.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter en større mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 6, artikel 9 om "særlige kategorier af personoplysninger" og artikel 87, jf. databeskyttelseslovens § 11 (CPR-nr.), hvorfor der skal etableres et "højt" sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

C.2.1. Tekniske og organisatoriske sikkerhedsforanstaltninger

C.2.1.1 Databehandleren skal i overensstemmelse med databeskyttelsesforordningens art. 32 implementere de nødvendige tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt at de ikke kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelsesforordningen, databeskyttelsesloven eller anden relevant lovgivning.

C.2.1.2 Databehandleren skal have en informationssikkerhedspolitik, der afspejler det aktuelle trusselsniveau og som minimum gennemgås mindst én gang om året. Tilhørende politikker, regler, procedurer og kontroller skal jævnligt gennemgås og om nødvendigt opdateres.

C.2.1.3 Databehandleren skal foretage de nødvendige tiltag til at identificere, vurdere og begrænse enhver – rimelig forudsigelig – intern og ekstern risiko for fortroligheden, integriteten og tilgængeligheden af de personoplysninger, der behandles på vegne af den dataansvarlige.

Hvis risici kan identificeres, skal databehandleren dokumentere, hvilke risici der er tale om, samt hvad der er gjort for at nedbringe dem til et acceptabelt niveau.

C.2.1.4 Databehandleren angiver, hvilke tekniske og organisatoriske foranstaltninger der er implementeret

- Databehandleren har foretaget risikovurdering samt konsekvensanalyse, hvor forskellige risici ved databehandlerens behandling af den dataansvarliges personoplysninger er blevet identificeret og vurderet
- Ledelsen hos databehandleren har det daglige ansvar for sikkerheden, hvorved det sikres, at de overordnede krav og rammer for sikkerheden er overholdt.
- Databehandleren har implementeret en central informationssikkerhedspolitik, hvori ledelsen har beskrevet databehandlerens struktur for informationssikkerhed.
- Der er udarbejdet en IT-sikkerhedshåndbog med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer.
- Informationssikkerhedspolitikken og IT-sikkerhedshåndbogen revideres som minimum én gang årligt.

C.2.2. Kryptering, pseudonymisering og anonymisering:
C.2.2.1 Ved transmission af personoplysninger, som foregår uden for databehandlerens domæne, og hvor personoplysningerne ikke er anonymiserede, skal der sikres en tilstrækkelig kryptering.

C.2.2.2 Hvis personoplysningerne pseudonymiseres, må de ikke længere kunne henføres til en bestemt registreret uden brug af supplerende oplysninger, der opbevares separat og er sikret mod, at personoplysningerne kan henføres til en identificeret eller identificerbar fysisk person.

C.2.2.3 Det er ikke tilladt at anvende personoplysninger i testmiljøer, medmindre oplysningerne er anonymiserede.

C.2.2.4 Databehandleren angiver, hvad der er implementeret til opfyldelse heraf

- Hvis personoplysninger videregives på f.eks. almindelig mail eller via link, anonymiseres filen, så alle personoplysninger fjernes, herunder navn, CPR-nr., institutionens navn og tekstfelter.
- Al transmission af personoplysninger sker krypteret med TLS, men databehandler sender ikke personoplysninger med mail.

C.2.3. Fortrolighed, integritet, tilgængelighed og robusthed:
C.2.3.1 Databehandleren skal have implementeret tilstrækkelige organisatoriske og tekniske foranstaltninger for at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af de anvendte systemer og tjenester – f.eks. via firewall, adgangsstyring og -kontrol, fysisk sikkerhed, logning og overvågning af netværk.

C.2.3.2 Databehandleren skal føre kontrol med afviste adgangsforsøg, og skal i tilfælde af gentagne afviste adgangsforsøg fra samme arbejdsstation/brugeridentifikation kunne blokere denne.

C.2.3.3 Databehandleren angiver, hvilke tekniske og organisatoriske foranstaltninger der er implementeret

- Printede dokumenter, som indeholder personoplysninger, makuleres straks efter, at de ikke længere skal anvendes. Dokumenterne indeholder dog ikke CPR-nr.
- Hvis der er behov for at opbevare fysiske dokumenter med personoplysninger, f.eks. i forbindelse med fejlretning, opbevares de sikkert i aflåst skab, eller der foretages anonymisering
- (Digitale) filer, der indeholder følsomme personoplysninger, slettes straks efter, at de ikke længere skal anvendes. Filen skal dermed altid slettes fra destinationsmappen samt ”papirkurven”.

- Der er etableret 2-faktor-login. Login er personligt, og en bruger afvises login, når pågældende forgæves har forsøgt at logge ind 3 gange. Sådanne afviste adgangsforsøg logges på mail og IP-adresse. Brugerens adgang åbnes af databehandleren ved henvendelse via brugerens mail.
- Alle arbejdsstationer er udstyret med firewall og antivirus, som opdateres løbende.

C.2.4. Genopretning af tilgængelighed:
C.2.4.1 Ved sikkerhedshændelser og svigtende drift af de systemer, der anvendes til opfyldelse af Hovedaftalen, er databehandleren forpligtet til at sikre, at driften genoprettes uden unødig forsinkelse.

C.2.4.2 Databehandleren skal til opfyldelse af pkt. C.2.4.1 have formelle processer til håndtering af sikkerhedshændelser samt svigtende drift, nulstilling af adgangskoder, et opdateret beredskab med tilhørende nødplaner, daglig backup og afprøvede restore rutiner.

C.2.4.3 Databehandleren angiver, hvilke foranstaltninger der er implementeret til genopretning af tilgængeligheden

- Der er systemmæssig overvågning af løsningen. Ved nedbrud eller anden fejl vil afhjælpning påbegyndes snarest muligt og senest inden for databehandlerens definerede reaktionstider.
- Indlæsning af backup iværksættes straks ved sikkerhedshændelser.
- Brugerne kan nulstille adgangskoden via loginsiden.
- Daglig backup og restore rutiner forestås af underdatabehandler.

C.2.5. Håndtering af personoplysninger under opbevaring:
C.2.5.1 Adgang til personoplysningerne, der behandles på vegne af den dataansvarlige, gives kun til de personer, der opfylder betingelserne i Bestemmelse 5.1, og hvor adgangen er arbejdsbetinget.

C.2.5.2 Databehandleren angiver, hvordan personoplysningerne håndteres under opbevaring

- Det er kun nøglepersoner, som får tildelt autorisation til at behandle personoplysninger som super-admin på kompetence.learnlab.dk, i forbindelse med support, der har adgang til den dataansvarliges personoplysninger. Autorisation annulleres ved ansættelsens ophør.
- Derudover er det den dataansvarlige, der har ansvaret for oprettelse af organisation og brugere og herved beslutter samt tildeler brugere rettigheder, der konkret er nødvendige.

C.2.6. Fysisk sikring:
C.2. 6.1 Databehandleren skal implementere foranstaltninger, så it-udstyr, der anvendes til opfyldelse af Hovedaftalen, er sikret på en sådan måde, at uvedkommende ikke kan få adgang.

C.2.6.2 Databehandlerens lokaler skal være sikret mod adgang fra uvedkommende gennem bl.a. anvendelse af adgangssikring og aflåste døre. Serverrum, krydsfelter og lignende steder, hvor der foregår behandling af personoplysninger, skal være forsynet med yderligere adgangskontrol og beskyttelse mod brand- og vandskader.

C.2.6.3 Ved kassation af udstyr og lagringsmedier skal databehandleren sikre, at der forinden er sket sletning af samtlige personoplysninger, der er blevet behandlet på vegne af den dataansvarlige, og bekræfte sletningen over for den dataansvarlige ved anmodning herom.

C.2.6.4 Databehandleren angiver, hvilke foranstaltninger der er implementeret i relation til den fysiske sikring

- Databehandlerens bærbare PC'er, der anvendes af databehandlerens ansatte, må ikke efterlades uden opsyn i længerevarende perioder. Hvis der er behov for at efterlade den bærbare PC i kortere tidsrum, skal den opbevares sikkert.
- Databehandlerens lokaler er sikret mod adgang fra uvedkommende gennem aflåste lokaler og tyverisikring. Databehandlerens kontor er altid bemandet i åbningstiden. Medarbejdere har ikke nøgler og kan kun tilgå kontoret i åbningstiden 8-16.
- Databehandlerens udstyr destrueres, så personoplysninger og anden data ikke kan genskabes.

C.2.7. Hjemme- og fjernarbejdspladser

C.2.7.1 Databehandleren skal sikre, at hjemme- og fjernarbejdspladser lever op til de sikkerhedsmæssige krav, der fremgår af databehandleraftalen.

C.2.7.2 Der må kun anvendes IT-udstyr i behandlingen, der tilhører og administreres af databehandleren, og benyttes der fjernopkobling, skal denne foretages via en vpn-forbindelse. Al transmission af personoplysninger skal foregå krypteret.

C.2.7.3 Databehandleren angiver, hvilke foranstaltninger der er implementeret i forbindelse med anvendelsen af hjemme- og fjernarbejdspladser

- Medarbejdere, der har en hjemme- eller fjernarbejdsplads, benytter en bærbar PC, som er udleveret af databehandleren.
- Databehandling må kun ske via sikker netværksforbindelse, og der anvendes 2-faktor-login.
- Der er udarbejdet instruktion for hjemmearbejdspladser, som medarbejderen introduceres til.
- Medarbejderne forpligter sig til at have kode på sin PC, ikke at anvende "Gem kodeord" funktioner i de browsere, der anvendes til at logge ind på kompetence.learnlab.dk og til ikke at dele eller udlåne sin bærbare PC til andre.
- Medarbejderne foretager kun behandling af den dataansvarliges personoplysninger på sikre/kendte netværk. Dermed foretages der ikke behandling af de pågældende oplysninger, hvis medarbejdernes PC er tilkoblet offentligt netværk.

C.2.8. Logning

C.2.8.1 Databehandleren skal foretage logning.

C.2.8.2 Databehandleren skal føre hændelseslog for IT-systemer, der behandler følsomme personoplysninger, jf. databeskyttelsesforordningens art. 9, personoplysninger vedrørende straffedomme og lovovertrædelser, jf. art. 10, eller cpr-nr., jf. art. 87. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Af loggen skal fremgå entydig bruger-ID, brugerens handling samt dato og klokkeslæt for handlingen.

C.2.8.3 Databehandleren skal efter anmodning fra den dataansvarlige vederlagsfrit stille de nødvendige loginformationer til rådighed med henblik på gennemførelse af periodisk audit eller til undersøgelse af misbrug eller mistanke herom.

C.2.8.4 Databehandleren angiver, hvordan logning foretages

- Loggen sker:
    - Når redigering af bruger tilgås ("edit-user")

- Når en bruger er blevet oprettet (”new-user”) eller genoprettes, hvis brugeren allerede eksisterer (”add-user”)
- Når en profil for en bruger tilgås – også hvis det er direkte på URL (”user-profile”)
- Når en gruppe-profil tilgås (gælder alle brugere i gruppen) – også hvis det er direkte via URL (”group-profile”)
- Når en bruger tilgår en handleplan/actionplan for en bruger-profil – også hvis URL tilgås direkte (”action”)
- Når en bruger tilgår en statusplan for en bruger-profil – også hvis URL tilgås direkte (”status”)
- Når en bruger tilgår en handleplan/actionplan for en gruppe-profil – også hvis URL tilgås direkte (”action-group”)
- Når en bruger tilgår en statusplan for en bruger-profil – også hvis URL tilgås direkte (”status-group”)

- Derudover registreres brugeren ved oprettelse af besvarelse, ved svar herpå samt ved sletning af uploadede dokumenter. Ved svar registreres også det nøjagtige tidspunkt for besvarelsen af det konkrete spørgsmål.
- Opstår der begrundet mistanke om en medarbejders misbrug af login til at skaffe sig adgang til den dataansvarliges personoplysninger, som brugeren i kraft af sit arbejds- og ansvarsområde skal tilgå, kan den dataansvarlige ved henvendelse anmode om udskrift af loggen. Log for de seneste 12 mdr. er tilgængelig i 12 mdr. efter aftalens ikrafttræden.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt bistå den dataansvarlige, i overensstemmelse med Bestemmelse 9.1 og 9.2, med de oplysninger, der konkret er nødvendige og tilstrækkelige for, at den dataansvarlige kan opfylde sine forpligtelser over for de registrerede og Datatilsynet.

I tilfælde af sikkerhedsbrud har databehandleren som minimum pligt til at informere den dataansvarlige om, hvornår hændelsen begyndte, blev konstateret samt afsluttet, hvilke tiltag databehandleren har iværksat eller påtænker at iværksætte for at standse bruddet, de sandsynlige konsekvenser af bruddet, og hvor mange registrerede der er berørte.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares som udgangspunkt maksimalt i 5 år, hvorefter de slettes hos databehandleren.

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 dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

Derudover har den dataansvarlige i løbet af det tidsrum, hvor tjenesten vedrørende behandling af personoplysninger ydes, til enhver tid ret til at kræve personoplysningerne slettet eller tilbageleveret, hvis de er unødvendige eller af anden saglig årsag ikke længere skal være undergivet databehandlerens behandling.

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:

- Hobrovej 91, 9240 Nibe (LearnLab ApS)
- Højvangen 4, 8660 Skanderborg (Team.blue: Zitcom – under brandet Curanet A/S)
- Datacenter #3: 8270 Højbjerg
- Sivsangervej 7, 9800 Hjørring (Vega Solutions)
- I. Verlingsvej 6, 7080 Børkop (Syspro Aps)

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren
Databehandleren skal én gang årligt for egen regning indhente en revisorerklæring fra en uafhængig revisor vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisorerklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE 3000

Revisorerklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Revisionserklæringen foreligger medio juli og fremsendes til Dataansvarlige medio august.
Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisorerklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere
Databehandleren indhenter en gang årligt den revisionserklæring, som underdatabehandleren for egen regning får udarbejdet af en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen,

databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Hvis der ikke foreligger en færdig revisionserklæring, føres der tilsyn med underdatabehandleren på anden vis, f.eks. via tilsynsskema.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse bestemmelser:

- ISAE 3000 type 1 erklæring

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen/rapport og kan i sådanne tilfælde anmode om en ny erklæring/rapport under andre rammer og/eller under anvendelse af anden metode for den dataansvarliges egen regning.

Baseret på resultaterne af erklæringen/rapporten er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode. Den fornyede inspektion foretages for den dataansvarliges egen regning.

Bilag D **Parternes regulering af andre forhold**