

Databehandlersaftale

i henhold til artikel 28, stk. 3, i databeskyttelsesforordningen

mellem

"Institutionen" eller "den dataansvarlige"

og

LIFE A/S
Biologiens Vej 5
2800 Kgs. Lyngby
CVR. nr.: 41439726

herefter "LIFE" eller "databehandleren"

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

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

Versionshistorik		
Version	Dato	Status
1.0	Marts 2020	Ikke gældende - erstattet af version 2.0
2.0	September 2020	Ikke gældende - erstattet af 3.0
3.0	November 2020	Gældende (denne aftale)
4.0	Januar 2021	Gældende (denne aftale) - LIFE A/S indsat som aftalepart

1. Indhold	
2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	3
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingsikkerhed	4
7. Anvendelse af underdatabehandlere.....	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige.....	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger.....	8
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør.....	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren	9
Bilag A Oplysninger om behandlingen	11
Bilag B Underdatabehandlere	12
Bilag C Instruks vedrørende behandling af personoplysninger.....	13

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 digitale læremidler via platformen MY:LIFE jf. LIFE's Vilkår og betingelser for bevillinger, 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. 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 medlemsstaternes¹ nationale ret og disse Bestemmelser.

¹ Henvvisninger til "medlemsstat" i disse bestemmelser 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 instruksene 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.

Databehandleren har ret til at udsætte behandlingen indtil instruksen er bekræftet eller ændret af den dataansvarlige eller dennes repræsentant.

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.
 4. 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. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere.
3. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.
5. Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.
6. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - 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 standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

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

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - c. indsigtretten
 - 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 unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, det danske Datatilsyn ("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 unødigt 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 unødige forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal ske uden unødige forsinkelse og altid således at den dataansvarlige kan opfylde sine forpligtelser i henhold til gældende lov 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 eller tilbagelevere alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet eller tilbageleveret, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

Side 9 af 16

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på tidspunktet for indgåelse af denne Databehandleraftale og accept af LIFE Vilkår og betingelser for bevillinger, ved besvarelse på e-mail.
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.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. LIFE's kontaktperson er

Navn	Marie Danø
Stilling	Leder af Redaktion og digital
Telefonnummer	31451185
E-mail	Mad@life.dk

2. Institutionens kontaktperson skal angives til LIFE i forbindelse med indgåelse af denne databehandleraftale.
3. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

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

Behandling af personoplysninger har til formål at give brugere adgang til LIFEs digitale læremidler, der stilles til rådighed for den danske grundskole og ungdomsuddannelserne, i henhold til platformens overordnede formål som angivet i LIFEs vilkår og betingelser for bevillinger.

LIFE må ikke anvende oplysningerne til andre formål end som beskrevet i Bestemmelserne, herunder i A.1. Personoplysningerne må ikke behandles efter instruks fra andre end Institutionen.

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

Som udbyder af en digital læringsplatform MY:LIFE til danske grundskoleelever og ungdomsuddannelser, behandler LIFE personoplysninger om lærere og elever med særligt henblik på at styrke elevernes læringsudbytte og feedback på LIFE Forløb fra både elever og lærere med henblik på at kvalificere forløbene yderligere og sikre den størst mulige effekt hos eleverne. LIFEs behandlinger sker med henblik på at stille LIFE Forløb til rådighed for Institutionen. LIFE vil desuden behandle personoplysninger om lærere til kommunikationsformål før, under og efter anvendelse af et LIFE Forløb.

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

Der vil som udgangspunkt blive registeret meget få personoplysninger om elever og lærer i forbindelse med LIFE forløbet. Behandlingen omfatter følgende oplysninger:

Navn, e-mail, klassetrin, lærer/elevstatus, skole, præstation, bedømmelser, evalueringer, læringsprogression, bruger ID samt UNI-C brugernavn.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Administrationsmedarbejdere tilknyttet Institutionen
- Lærer og andet uddannelsespersonale i grundskole og ungdomsuddannelserne
- Elever i grundskolen og ungdomsuddannelserne.

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

De angivne personoplysninger vil blive behandlet så længe institutionen er tilknyttet og anvender LIFEs digital læringsplatform MY:LIFE, og er underlagt de øvrige betingelser for brug af MY:LIFE platformen i LIFEs vilkår og betingelser for bevillinger.

Vores underdatabehandler, Clio, har konfigureret platformen til at slette data om elever eller lærere, hvis de pågældende lærere eller elever skifter til en anden skole som er uden for kommunen, med hvilken databehandleraftalen er indgået. Når en elev, hvis unilogin er tilknyttet et institutionsnummer, går ud af 9. klasse, vil eleven ikke længere være tilknyttet institutionsnummer, og data om den pågældende elev slettes derfor automatisk.

Derudover foretager Clio manuel sletning af data om elever eller lærere på My:LIFE platformen, hvis den pågældende elev eller lærer anmoder om det.

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Clio ApS	CVR-nr: 30583795	Esplanaden 8 A, 1. – 2. Sal 1263 København K Danmark	Drift og hosting af portalen samt support i forhold til portalen

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:

Ved opkobling til MY:LIFE platformen modtager LIFE personoplysninger fra dets brugere, for at verificere adgangen til platformen samt facilitere brug af platformens tjenester for data subjekter, der anvender platformen.

C.2. Behandlingssikkerhed

LIFE gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, og som dermed opfylder databeskyttelsesforordningens artikel 32.

Foranstaltningerne er fastlagt ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål
4. Konsekvenserne for borgerne ved et sikkerhedsbrud
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
 - a) tilintetgørelse af oplysningerne
 - b) tab af oplysningerne
 - c) ændring af oplysningerne
 - d) uautoriseret videregivelse af oplysningerne
 - e) uautoriseret adgang til oplysningerne

Foranstaltningerne som beskrevet nedfor foretages og sikres af LIFE's underdatabehandler, Clio, som leverer, drifter og hoster MY:LIFE platformen på vegne af LIFE.

Generelle sikkerhedsforanstaltninger

LIFE's underdatabehandler, Clio; som drifter og hoster platformen har adgang til personoplysninger med henblik på at problemsøge, og fejlfinde i interne systemer i forhold til at optimere vores produkters performance og dermed understøtte formålet med databehandlingen. Dette sker via en sikret adgang med brugernavn og adgangskode. Der bliver ført tilsyn med disse adgangstilladelser og disse ajourføres jævnligt.

Wiping af datamedier

Når der opsættes brugte computere til nye medarbejdere, bliver alt data og dataspor slettet. For Mac-computere anvendes det indbyggede diskværktøj til at slette hele partitionen på harddisken og geninstallerer styresystemet. For Windows computere anvendes den indbyggede 'Nulstil Windows' funktion, som ligeledes sletter alle partitioner på harddisken.

På harddiske, som skal ud af huset til destruktion, bliver alle sektorer på disken overskrevet med 0'er med Active Killdisk programmet.

Overførsel af data mellem Styrelsen for IT og Læring (STIL) og Clios systemer

LIFE anvender Webservice 17 – lille, Webservice 22 og Webservice 71. Når en bruger vil benytte LIFE portalen, omdirigeres brugeren til UNI•Login. UNI•Login autentificerer brugeren ved at identificere denne og dokumenterer over for LIFE's platform, hvem brugeren er. Efter denne autentifikation returneres brugeren til LIFE's platform, hvor der kontrolleres om brugeren har abonnement til LIFE's produkter og sendes derefter ind i LIFE's produkt-univers. Hvis den

pågældende institution har tilmeldt sig dataaftalen via STIL, giver det LIFEs systemer mulighed for at indhente og lagre følgende oplysninger:

Side 14 af 16

- UNI-C brugernavn
- E-mail
- Navn
- Klassetilhørsforhold (klassestrin) og institutionsnummer (skole)
- Funktion (Fx lærer, elev etc.)

Fysisk datamiljø er sikret efter Amazon Web Services høje standarder

Denne overførsel af data fra STILs systemer til LIFEs platform og database foregår via en krypteret forbindelse. Den overførte data bliver placeret i LIFEs fysiske datamiljø, der er sikret og adgangskontrolleret via Amazon Web Services.

Adgang til datamiljø sikret via Bastion jump-server

Det fysiske datamiljø er sikret og adgangskontrolleret via Amazon Web Services. Det er udelukkende medarbejdere, der har et formål med at arbejde med de pågældende personoplysninger, der har fået kontrolleret adgang til disse systemer via en kryptografisk keybaseret autentifikation samt brugernavn og kodeord. Selve adgangen til disse systemer foregår via en Bastion jump-server.

Inddatamateriale som indeholder personoplysninger

Ud over den data, der bliver overført via sikrede forbindelse fra STIL til LIFEs systemer, så bliver der også genereret andre typer af data. Det drejer sig overordnet om følgende data, som bliver registeret og lagret:

- Elevens resultater og besvarelser fra Opgavesystemet
- Elevens noter til læringsportalernes fagtekster
- Elevens svar og input i de interaktive elementer på læringsportaler
- Selvevaluering fra de interaktive forløb på læringsportal
- Sidevisninger og interaktion med produkterne

Ovenstående datatyper indhentes med henblik på at styrke mulighederne for at monitorere elevernes læringsprogression samt forbedre brugeroplevelsen. Data er lagret i et fysisk datamiljø, der er sikret og adgangskontrolleret via Amazon Web Services.

Uddatamateriale som indeholder personoplysninger

LIFEs platform har et API (Application Programming Interface), der tillader at integrere andre typer af software med LIFEs, og dermed muliggør, at der kan overføres data mellem systemerne. Denne integration vil som hovedregel være med forskellige leverandører af LMS (Learning Management Systems). I dette setup vil der foregå en autorisering af den uddata, der vil flyde fra LIFEs system og over i et LMS. Denne autorisation foregår ved, at læreren skal logge sig ind i LMS'et, som den pågældende skole anvender, og godkender, at elevdataen fra LIFEs systemer bliver overført til det pågældende LMS. Denne data bliver overført via en krypteret SSL-forbindelse.

Behandlingen af personoplysningerne ved det pågældende LMS er den pågældende leverandørs ansvar, hvorfor det er Institutionens ansvar at indhente en separat databehandlertale med denne leverandør.

Eksterne kommunikationsforbindelser

Når der anvendes eksterne kommunikationsforbindelser ved tilslutning til Internettet, andre åbne net, samt ved brug af interne webapplikationer sikrer LIFE imod uvedkommende trafik og forhindrer adgang fra det åbne net via en firewall, som løbende kontrolleres og ajourføres. Det trådløse netværk er ligeledes sikret imod aflytning af kommunikationen og opsnappe



brugeridentifikationer og dertil hørende fortrolige adgangskoder, som anvendes i forbindelse med autoriserede brugeres adgang til personoplysninger. Alt sammen ligger inde bag Network Layer Firewalls og Web Application Layer Firewalls (WAF).

Hjemmearbejdspladser

LIFE's behandling af personoplysninger sker delvist ved anvendelse af hjemmearbejdspladser. Hvis interne systemer tilgås fra en hjemmearbejdsplads, foregår det via krypterede VPN-forbindelser og tilgang til vores server-miljøer sker igennem en avanceret kryptografisk key-baseret forbindelse til vores fysiske datamiljø, der er sikret med *Amazon Web Services*.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for rimeligt omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre de tekniske og organisatoriske foranstaltninger som anført under C.2.

C.4 Opbevaringsperiode/sletterutine

Ved ophør eller opsigelse af tjenesterne vedrørende behandling forpligtes LIFE til at slette alle personoplysninger, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne. Oplysningerne slettes automatisk senest tre (3) måneder efter ophør af brugen af LIFE portalen. Såfremt Institutionen ønsker at oplysningerne skal slettes før, skal Institutionen rette henvendelse til LIFE herom i umiddelbar forlængelse af ophøret/opsigelsen.

C.5 Lokalt for behandling

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

På databehandlerens adresse og enhver godkendt underdatabehandlerens adresse som specificeret i bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

LIFE må anvende underdatabehandlere, der befinder sig i EU eller sikre tredjelande eller underleverandører, der har underskrevet EU Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande.

Den dataansvarlige bemyndiger LIFE til at indgå EU-Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger til underdatabehandlere i tredjelande på vegne af den dataansvarlige.

LIFE indestår således for, at de anvendte underdatabehandlere enten er etableret i et sikkert tredjeland eller har underskrevet EU Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande.

Ud over hvad der følger af dette punkt C.6 eller inden for rammerne af disse Bestemmelser, er databehandleren ikke berettiget til at foretage sådanne overførsler, medmindre den dataansvarlige efterfølgende giver en dokumenteret instruks vedrørende overførelse af personoplysninger til et tredjeland.

I tilfælde af, at retsgrundlaget for overførslen af personoplysninger angivet i dette punkt C.6 ikke stemmer overens med den gældende databeskyttelseslovgivning og er erstattet eller på anden måde ikke længere betragtes som værende et gyldigt retsgrundlag for overførslen af personoplysninger uden for EU/EØS, vil Parterne sammen og uden unødige forsinkelser finde og aftale et andet retsgrundlag for overførslen af personoplysninger uden for EU/EØS.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

LIFE er forpligtet til at give Institutionen nødvendige oplysninger til, at Institutionen til enhver tid kan sikre sig, at LIFE overholder de krav, der følger af denne Aftale.

Institutionen, en repræsentant for Institutionen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision, stille spørgsmål til og få udleveret dokumentation med henblik på at kontrollere, at LIFE overholder de krav, der følger af denne aftale.

LIFE fremsender én gang årligt en erklæring til Institutionen om overholdelse af denne aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende anerkendte branchestandarder på området, og skal omfatte både Leverandørens og eventuelle underdatabehandleres databehandling. En sådan erklæring forelægges ved, at LIFE indhenter en ISAE 3000 erklæring, der dækker den behandling, der foretages i henhold til databehandleraftalen. Den første erklæring skal foreligge senest den 1. januar 2021.

I tilfælde af, at Institutionen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter LIFE og LIFE's underleverandører sig til at stille tid og ressourcer til rådighed herfor. Såfremt Institutionen vurderer, at der er behov for at anvende eksterne ressourcer i denne inspektion, så afholder Institutionen alle udgifter hertil.

Den dataansvarlige kan årligt med 30 dages varsel indhente en revisionserklæring fra en autoriseret uafhængig tredjepart vedrørende databehandlerens overholdelse 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

Der er enighed mellem parterne om, at LIFE som databehandler har ansvaret for at føre tilsyn med de underdatabehandlere, der er angivet i bilag B. Et sådant tilsyn kan være i form af modtagelsen af en revisionserklæring, eksempelvis en ISAE 3000 revisionserklæring, fra de(n) pågældende underdatabehandler(e).

Den dataansvarlige kan med rimeligt forudgående varsel forlange at LIFE udleverer dokumentation for det udførte tilsyn med underdatabehandler(e)(n).