

INDGÅELSE AF DATABEHANDLERAFTALE OG ACCEPT AF LIFE FONDENS BEVILLINGSVILKÅR

Herved indgås databehandleraftale (Version 7) ligesom LIFE Fondens bevillingsvilkår¹ accepteres.

Institutionens/Kommunens navn: _____

Inst.nr.: _____ CVR-nr.: _____

Herefter "Institutionen" eller "den dataansvarlige"

På vegne af Institutionen:

| Kontaktperson | |
|---------------|--|
| Navn | |
| Stilling | |
| E-mail | |
| Telefon | |

| Kontaktoplysninger vedr. pkt. 10 (underretning om brud på persondatasikkerheden) samt pkt. 7.3 (varsling om påtænkt ændring i kredsen af underdatabehandlere, herunder påtænkt tredjelands-overførsel) | |
|--|--|
| E-mail | |

| Underskriver: | |
|---------------|--|
| Navn | |
| Stilling | |

Dato:

Underskriver _____

På vegne af Databehandleren:

| Kontaktoplysninger LIFE A/S | |
|-----------------------------|--|
| Navn | LIFE A/S |
| CVR-nummer | 41439726 |
| E-mail | persondata@life.dk |
| Telefon | 2234 4896 |

Dato: 03/01/2023

Christine Antorini, Direktør for LIFE



¹ <https://life.dk/vilkaar-for-bevillinger>

DATAHANDLERAFTALE (STANDARDKONTRAKTBESTEMMELSER)²

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

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

| Versionshistorik | | |
|------------------|----------------------------|---|
| Version | Dato | Ændringer |
| 7 | Træder i kraft 1/1-2023 | Opdatering af bilag B med følgende nye underdatabehandlere: <ul style="list-style-type: none"> - Lindhardt og Ringhof Forlag A/S - Egmont IT v/ Egmont Administration A/S Samtidig udgår Clio ApS om underdatabehandler pga. fusion med LRF A/S. Konsekvensrettelse i Bilag C.2.1.3 hvor der er indsat beskrivelse af "Egmont Administration A/S ("Egmont IT") som leverandør af AWS-løsningen". Konsekvensrettelser af "Clio ApS" til "databehandleren". |
| 6 | August 2022 | Sammenlægning af version til hhv. kommuner og ungdomsuddannelser. Diverse smårettelser. Dixa fjernet som underdatabehandler, da supportværktøj er afviklet. Varslingsfrist ved brud i 10.2 samt Bilag C.3 konkretiseret til "så vidt muligt indenfor 24 timer". Farvemærkning af afvigelser fra Datatilsynets Standardkontraktbestemmelser 2020 Genindførelse af Bilag D Ændring af LIFE's underrettningsfrist fra "uden unødige forsinkelse" til "24 timer" (10.2) Tydeliggørelse af formålet i A.1 og forenkling af A.2 |

² Læsevejledning: LIFE's udfyldelse af Bestemmelserne fremgår med grå skrift.

| | | |
|--|--|--|
| | | Småjusteringer i C.2.1.3 om behandlingssikkerhed Sletning af Biologiens Vej 5, 2800 Kgs. Lyngby som lokalitet for behandlingen (C.5) Adressering af Datatilsynets udtalelse af 29. marts 2022 i KOMBIT-sagen (C.5) |
|--|--|--|

1. Indhold

| | |
|--|----|
| <i>INDGÅELSE AF DATABEHANDLERAFTALE OG ACCEPT AF LIFE FONDENS BEVILLINGSVILKÅR</i> | 1 |
| 2. Præambel | 5 |
| 3. Den dataansvarliges rettigheder og forpligtelser | 5 |
| 4. Databehandleren handler efter instruks | 6 |
| 5. Fortrolighed | 6 |
| 6. Behandlingssikkerhed | 6 |
| 7. Anvendelse af underdatabehandlere..... | 7 |
| 8. Overførsel til tredjelande eller internationale organisationer | 8 |
| 9. Bistand til den dataansvarlige..... | 9 |
| 10. Underretning om brud på persondatasikkerheden | 10 |
| 11. Sletning og returnering af oplysninger..... | 10 |
| 12. Revision, herunder inspektion | 10 |
| 13. Parternes aftale om andre forhold | 11 |
| 14. Ikrafttræden og ophør | 11 |
| 15. Kontaktpersoner hos den dataansvarlige og databehandleren | 11 |
| Bilag A Oplysninger om behandlingen | 12 |
| Bilag B Underdatabehandlere | 15 |
| Bilag C Instruks vedrørende behandling af personoplysninger..... | 18 |
| Bilag D Parternes regulering af andre forhold..... | 27 |

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 digitale læremidler via platformen www.mylife.dk ("MY:LIFE") jf. LIFEs [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 medlemsstaternes³ nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

³ Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

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.

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.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst **30 dages varsel** og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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. [...] ⁴
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

- 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.
- 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.
- 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
- 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.
- 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.

⁴ Bestemmelsen i 7.6 i Datatilsynets standardkontraktbestemmelser er slettet, idet det ikke er et krav i henhold til artikel 28 i GDPR, at databehandleren forpligtes til at indføre den dataansvarlige som begunstiget tredjemand i databehandlerens aftale med underdatabehandlere, i tilfælde af databehandlerens konkurs. LIFE finder det uhensigtsmæssigt at Datatilsynets standardkontraktbestemmelser går videre end, hvad der følger af artikel 28 i GDPR.

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 unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal ske inden 24 timer 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 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. Databehandleren er ikke underlagt en sådan lovgivning.

12. Revision, herunder inspektion

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

på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder 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 sker på side 1.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via de kontaktoplysninger, der fremgår af 1. side.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Bilag A Oplysninger om behandlingen

LIFE tilbyder den dataansvarlige institution adgang til de digitale læremidler ("LIFE Forløb"), der fremgår af <https://life.dk/undervisningsforlob>.

LIFE Forløbene stilles til rådighed på de betingelser, der fremgår af LIFE's bevillingsvilkår, som findes her: <https://life.dk/vilkaar-for-bevillinger>.

Den dataansvarlige booker selv det/de ønskede LIFE Forløb via www.life.dk. Den dataansvarlige skal samtidig godkende LIFE's bevillingsvilkår og åbne for 3 datapakker til LIFE via STIL Tilslutning, jf. A.3.

Når LIFE har bekræftet bookingen, modtager den dataansvarlige institution en fysisk materialekasse med undervisningsmaterialer ("LIFE Kit"). Når arbejdet med LIFE Forløbet går i gang i skoleklassen, skal elever og lærere både bruge LIFE Kitten og undervisningsplatformen MY:LIFE (www.mylife.dk) (herefter "MY:LIFE"), som er den digitale ramme for LIFE Forløbet for både elever og lærere. I MY:LIFE findes lærervejledningen og digitale undervisningsmaterialer, fx faglige animationer, læringsmål, forsøgsbeskrivelser og interaktive opgaver.

Elevers og læreres brug af MY:LIFE indebærer den behandling af personoplysninger, der er beskrevet nedenfor.

I det omfang undervisningsmaterialet i MY:LIFE linker til – eller på anden vis indebærer brug af – eksterne platforme, hjemmesider eller værktøjer, ligger elever og læreres brug af indhold på disse eksterne platforme udenfor rammerne af nærværende databehandleraftale. LIFE har på det dataetiske plan påset, at udbyderen af den eksterne platform har en opdateret, dækkende privatlivspolitik, men henholder sig i øvrigt til, at formålet med brugen af den eksterne platform er formidling af fagligt indhold og ikke behandling af personoplysninger.

En oversigt over eksterne platforme findes på <https://life.dk/aftaler-med-life>

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

Behandling af personoplysninger har til formål at give brugere adgang til og anvende MY:LIFE i henhold til platformens overordnede formål, som dette er angivet i LIFE's vilkår og betingelser for bevillinger.

Herunder er formålet at styrke elevernes læringsudbytte samt modtage feedback på brugen af LIFE Forløb fra både elever og lærere med henblik på at kvalificere forløbene yderligere og sikre den størst mulige effekt hos eleverne.

LIFE må ikke anvende oplysningerne til andre formål end beskrevet i Bestemmelserne. 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 led i ovennævnte formål er behandlingen:

- Facilitering af login til MY:LIFE gennem UNI-login (Unilogin-oplysninger overføres fra Styrelsen for It og Læring (STIL) til LIFE (databehandleren) i forbindelse med login på MY:LIFE)
- Hosting af personoplysninger

- Behandling af personoplysninger (kontaktoplysninger) 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 registreret meget få personoplysninger om elever og lærere, når de anvender et LIFE Forløb.

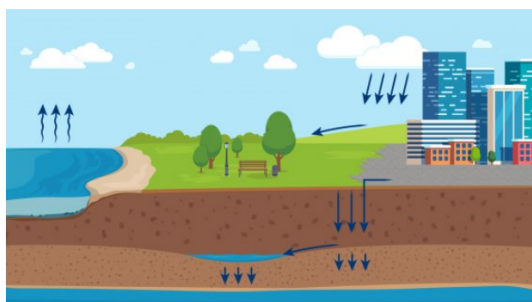
På baggrund af den dataansvarlige institutions godkendelse af dataaftaler i STIL Tilslutning, anvender LIFE følgende personoplysninger via datapakkerne Webservice 17 – lille, Webservice 22 og Webservice 71:

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

Endvidere registreres der følgende oplysninger:

- Elevers besvarelser i tekstfelter på MY:LIFE, fx "Tal sammen om, hvilke kategorier i KlimaAtlas der kan bruges til at udpege områder med risiko for stormflodshændelser. Skriv jeres svar i tekstfeltet herunder eller i jeres egne noter."
- Elevers resultater fra egne feltundersøgelser i tabeller på MY:LIFE, fx "Udfyld tabellen nedenfor ved at notere den undersøgte overfladetype og de beregnede K-værdier. Udregn herefter gennemsnittet af K-værdierne."
- Elevers svar og input i de interaktive quizzer, fx som screenshot herunder:

2. Brug din forhåndsviden til at placere fagordene korrekt på illustrationen af vandets kredsløb. Fagordene skal ikke placeres helt præcist, men blot inden for det korrekte område på illustrationen.



1. Nedbør 2. Ubefæstet overflade

3. Underjordisk afstrømning 4. Befæstet overflade

5. Grundvandsspejl 6. Nedsivning

7. Fordampning 8. Overfladisk afstrømning

Tjek dit svar

- Elevers selvevaluering under evalueringssider på MY:LIFE, fx "Skriv i fællesskab tre ting, som I har lært om: a) at planlægge og gennemføre undersøgelser af infiltration, b) at analysere resultater fra

en infiltrationsundersøgelse og vurdere risikoen for oversvømmelse. Skriv jeres svar i skrivefeltet eller i jeres egne noter.”

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Elever
- Lærere

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

Behandlingen er ikke tidsbegrænset og varer så længe, det er relevant for LIFE's udførelse af de aftalte opgaver og efterlevelse af forpligtelser over for den dataansvarlige Institution i Bevillingsvilkårene.

Om kassationsregler og sletterutiner, se C.4.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

| NAVN, CVR OG ADRESSE | BESKRIVELSE AF BEHANDLING | DATA DER BEHANDLES | LOKALITET + EVT. OVERFØRSELSGRUNDLAG |
|---|---|--|--------------------------------------|
| Lindhardt og Ringhof Forlag A/S, Vognmagergade 11, 1120 København K, CVR-nr. 76351910 | Levering og support af undervisningsplatformen MY:LIFE og dens funktioner | Almindelige personoplysninger. Ikke CPR. Følgende registreres: navn, e-mail, klassetrin, lærer/elevstatus, skole, egen-bedømmelse af præstation og læringsprogression, evaluering, bruger-ID. Endvidere fagligt relateret fritext i skrivefelter | Data opbevares hos AWS i Irland. |
| <i>Underleverandør til LRF A/S:</i> Egmont Administration A/S Egmont IT Vognmagergade 11, 1120 København K, CVR-nr. 84853518 | Drift af Lindhardt og Ringhofs løsninger på AWS, herunder administration af miljøer, overvågning, brugeradministration mv. Som udgangspunkt arbejdes der ikke ned i løsningerne, dvs. at der som udgangspunkt ikke sker behandling af personoplysninger om elever/lærere. | Som ovenfor | Som ovenfor |
| <i>Underleverandør til LRF A/S:</i> Amazon Web Services One Burlington Plaza, Burlington Road, Dublin 4, Ireland | Serverhosting af undervisningsplatformen MY:LIFE, der drives af databehandleren Supporthenvendelser via databehandleren. Via interne kontroller | Som ovenfor. | Data opbevares hos AWS i Irland. |

| NAVN, CVR OG ADRESSE | BESKRIVELSE AF BEHANDLING | DATA DER BEHANDLES | LOKALITET + EVT. OVERFØRSELSGRUNDLAG |
|--|--|--------------------|--------------------------------------|
| | sikres det, at support ikke indeholder personoplysninger | | |
| <i>Underleverandør til AWS:</i> Databehandlerens kontrakt-part er Luxembourg-selskabet, Amazon Web Services EMEA SARL, ("AWS Europe"). Der angives ingen under-databehandlere til dette selskab på AWS' info site, se her . | - | - | - |

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 under-databehandler til denne behandlingsaktivitet.

B.2 Varsel for underretning om planlagte ændringer i kredsen af underdatabehandlere, den dataansvarliges indsigelsesmulighed og LIFE's behandling af sådan indsigelse

B.2.1. LIFE har den dataansvarliges generelle godkendelse til brug af underdatabehandlere, jf. afsnit 7.3.

B.2.2. LIFE skal pr. e-mail til kontaktpersonen/kontaktpunktet, der er anført i på side 1, underrette den dataansvarlige om eventuelle planlagte ændringer i kredsen af underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod ændringen.

Hvis den dataansvarlige har indsigelser mod den planlagte ændring, skal indsigelsen sendes til LIFE hurtigst muligt og senest 30 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre rimelig, konkret begrundet indsigelse.

B.2.3. LIFE er forpligtet til at tage den dataansvarliges indsigelse i betragtning. Hvis LIFE vælger ikke at imødekomme indsigelse, eller hvis LIFE ikke er i stand til at imødekomme indsigelse inden for en rimelig frist, går LIFE i dialog med den dataansvarlige om en fremadrettet plan.

B.2.4. Hvis den dataansvarlige tager den planlagte ændring til efterretning – enten ved at meddele dette aktivt eller undlade at gøre indsigelser – gennemfører LIFE den varslede ændring efter udløbet af 30-dages fristen.

B.2.5. Ved antagelse af nye underdatabehandlere i Bestemmelsernes løbetid, skal LIFE iagttage de aftalte vilkår i punkt C.5 om lokalitet for behandling samt punkt C.6 om instruks vedrørende overførsel af personoplysninger til tredjelande.

B.3 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

Databehandleren skal én gang årligt indhente en revisionserklæring eller en ledelseserklæring fra en uafhængig tredjepart om underdatabehandlerens overholdelse af denne databehandleraftale med tilhørende bilag.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

LIFE's behandling af personoplysninger på vegne af den dataansvarlige sker ved, at LIFE udfører følgende:

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

Endvidere hosting af personoplysninger.

Der henvises i øvrigt til Bilag A (Oplysninger om behandlingen).

C.2. Behandlingssikkerhed

C.2.1. Sikkerhedsniveauet

Sikkerhedsniveauet skal afspejle, at behandlingen angår data, der er omfattet af databeskyttelses-forordningens artikel 6 ("almindelige personoplysninger") og at hovedparten af de registrerede, er under 18 år.

LIFE er opmærksom på, at børn og unges rettigheder og frihedsrettigheder nyder en særlig beskyttelse i databeskyttelsesreglerne. LIFE har bestræbt sig på at tydeliggøre behandlingen, overvejelser og risici ved brugen af MY:LIFE nedenfor.

Det er databehandlerens opgave at træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger 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 lov om behandling af personoplysninger.

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 nedenstående foranstaltninger, som er aftalt med den dataansvarlige.

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

Endvidere skal Databehandleren på den dataansvarliges anmodning give den dataansvarlige tilstrækkelige oplysninger til, at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

C.2.1.2 Afgrænsning

LIFEs medarbejdere har udelukkende adgang til MY:LIFEs backend. Backend er dedikeret til udvikling og redigering af de undervisningsforløb, der senere hen udgives på og anvendes via MY:LIFEs driftsmiljø. Der behandles ingen personoplysninger i backend ifbm. LIFEs udviklingsarbejde.

LIFEs medarbejdere har ikke administrative adgange til driftsmiljøet og ikke adgang til at se eller behandle personoplysninger, der er indlæst via STIL eller som er inddateret som led i eleveres og læreres brug af et LIFE Forløb.

Dette afspejles i C.5., hvoraf det følger at lokationen for behandlingen *ikke* er LIFE Campus i Kgs. Lyngby.

LIFEs medarbejdere gennemgår 1 x årligt awareness ifht. korrekt håndtering af personoplysninger.

Nedenstående beskrivelse af behandlingen af personoplysninger og trufne sikkerhedsforanstaltninger retter sig mod LIFEs underdatabehandler, Lindhardt og Ringhof Forlag ApS, som leverer, drifter, vedligeholder og hoster MY:LIFE efter instruks fra LIFE.

C.2.1.3 Tekniske og organisatoriske sikkerhedsforanstaltninger

Pseudonymisering og kryptering af oplysninger

Overførsel af data mellem STIL og MY:LIFE

På baggrund af den dataansvarlige institutions godkendelse af dataaftaler i STIL Tilslutning, anvender LIFE de WS-datapakker med tilhørende personoplysninger, der er nævnt i A.3.

Når en bruger vil logge ind på MY:LIFE med sit UNI-Login, omdirigeres brugeren til STIL, som autentificerer brugeren ved at identificere denne og som over for MY:LIFE dokumenterer, hvem brugeren er. Herefter returneres brugeren til MY:LIFE, hvor brugeren sendes ind i LIFEs læringsforløb.

Denne overførsel af data fra STILs systemer til MY:LIFE foregår via en krypteret forbindelse. De overførte data bliver placeret i LIFEs fysiske datamiljø, der er hostet hos Lindhardt og Ringhof Forlag A/S' underleverandør Amazon Web Services, jf. bilag B.

Data i transit

Alle personoplysninger, der sendes mellem MY:LIFE, brugeren og AWS er krypterede "in transit" for at sikre efterlevelse af de tekniske krav i databeskyttelsesforordningen. Ved transmissionen gøres brug af kryptering TLS, version 1.2 eller højere.

Hostede data

Personoplysningerne er ikke stærkt krypterede under hostingen hos Amazon Web Services i Irland (bemærk, at hosting og databehandlingen vurderes udelukkende at ske i EU, jf. C.5).

LIFE er opmærksom på, at en stærk kryptering af data i ro med nøgle opbevaret hos tredjepart er en supplerende teknisk foranstaltning, der kan nedbringe risikoen for, at de hostede personoplysninger måtte forlade EU som led i en US-udleveringsanmodning.

Med henvisning til de i C.2.1 nævnte kriterier for valg af passende sikkerhedsforanstaltninger, er begrundelsen for ikke at implementere kryptering, at risikoen for de registreredes rettigheder samlet set vurderes at være lav og at etablering af en stærk kryptering med nøgle hos tredjepart vurderes kun at give en begrænset, øget sikkerhed, som ikke står mål med implementeringsomkostningerne i bred forstand (økonomi, ressourcer, fleksibilitet, tilkomst af nye sårbarheder).

Begrundelsen for den lave risiko er, at:

- Det er LIFE's vurdering, at alene US CLOUD Act kan hjemle en udleveringsanmodning. Dette eftersom FISA 702 umiddelbart ikke har exterritorial virkning, jf. Datatilsynets cloudvejledning, note 26, og eftersom E.O. 12333 kun retter sig mod fysisk infrastruktur (undersøiske kabler) til USA.
- Risikoen for dataudlevering med hjemmel i CLOUD Act vurderes at være som i eksempel 14 i Datatilsynets Cloud-vejledning, dvs. lav.
- Den lave risiko skal ses i lyset af, at udgangspunkt for forståelsen af Cloud Acts anvendelsesområde er, at:
 - Udleveringen kræver en dommerkendelse, dvs. et forudgående retligt tilsyn
 - Myndighedsanmodningen skal være rimeligt begrundet og klar, præcis og proportionel ifht. de data, som ønskes udleveret. Anmodningen skal angive en navngiven person og angå et kriminelt forhold.
 - Dvs. at data ikke kan høstes i stor skala, men umiddelbart kun udleveres på individualiseret grundlag
 - At den retslige prøvelse ifbm. dommerkendelsen skal tage højde for konflikt med GDPR og EMRK

Som kilde kan der henvises til: https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf side 2 øverste afsnit. I det derpå følgende afsnit beskrives undtagelser her til.

Som foranstaltning imod risikoen for udlevering lægger vi vægt på, at AWS i AWS' "Supplementary Addendum to AWS GDPR Data Processing Addendum", som nøje beskriver de tiltag, som AWS vil gøre brug af, for at undgå at efterkomme en US-udleveringsanmodning. Såfremt dette ikke er muligt, meddeler AWS straks såvel sin aftalepart (Egmont IT v/ Egmont Administration A/S), at aftalen er misligholdt.

I den forbindelse bemærkes, det at eftersom en udlevering vil skulle ske fra EU-infrastruktur, vil udleveringen indebære en manuel proces, hvor AWS netop vil kunne aktivere de mitigerende tiltag, der er beskrevet i ovennævnte Addendum.

AWS' rapport over udleveringsanmodninger viser, at der i 2. halvår 2020 og 1. halvår af 2021 har været nul udleveringer af data på baggrund af myndighedsanmodninger. Rapporterne findes her: <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYS DRGWQ2C2CRYEF>

Begrundelsen for den samlet set lave risiko er endvidere, at der er få konsekvenser forbundet med en US-udleveringsanmodning for de registrerede. Dels fordi det er usikkert, om udleveringsanmodningen vil blive efterkommet, dels fordi der er tale om få kategorier af personoplysninger, som alle er omfattet af GDPR art. 6 og dels fordi sletning af personoplysningerne er undergivet den dataansvarliges rådighed, jf. C.4.

Den øgede sikkerhed ved implementering af en stærk kryptering med nøgle hos tredjepart er endvidere begrænset, idet

- Løsningen ikke er en garanti mod udlevering af data til US-myndigheder i Cloud Act-situationer, hvor en dataudleveringsanmodning rettes mod en ikke-US-hosted løsning. En sådan udleveringsanmodning en administrativ proces og anmodningen må forventes ledsaget af et pålæg om afkryptering

- En stærk kryptering med nøgle hos tredjepart vil udløse andre sårbarheder ifht. beskyttelse af personoplysninger, da personoplysningerne bliver svært tilgængelige – også for teknikere og supportmedarbejdere med saglige grunde til at tilgå data. Det vil give hastighedstab fx ifbm. identifikation og håndtering af sikkerhedshændelser eller ved servicering af den registrerede persons anmodning om udøvelse af rettigheder.

Evnen til at sikre vedvarende fortrolighed, integritet, tilgængelig og robusthed af behandlingssystemer og -tjenester (Generelle sikkerhedsforanstaltninger)

Egmont Administration A/S ("Egmont IT") som leverandør af AWS-løsningen

Som led i Clio ApS' ophør gennem fusion med Lindhardt og Ringhof Forlag A/S, overtager Lindhardt og Ringhof Forlag A/S samtlige rettigheder og forpligtelser vedr. systemleverance og it-drift af MY:LIFE-undervisningsplatformen overfor LIFE A/S. Lindhardt og Ringhof Forlag A/S driver således MY:LIFE-platformen og det tekniske set up videre på uændrede vilkår ifht., hvad der hidtil har været gældende.

Lindhardt og Ringhof Forlag A/S ("underdatabehandleren") overlader opgaven med teknisk drift og AWS-kontraktadministration til Egmont IT, som hører under Egmont Administration A/S.

Fra 1/1-2023 yder Egmont IT således service, support og vedligehold af løsningen på systemniveau, hvorfor enkeltpersoner hos Egmont IT kan få adgang til databehandlerens driftsmiljø hos AWS. Denne brugeradgang omfatter ikke systematisk adgang til de personoplysninger, der er omfattet af Bestemmelserne, da det ikke er nødvendigt for udførelse af opgaverne.

Lindhardt og Ringhof Forlag A/S har instrueret Egmont IT om de databeskyttelsesforpligtelser, der fremgår af Bestemmelserne.

Funktionsadskillelse mellem test og drift

Udviklings-, test- og produktionsmiljø for MY:LIFE er adskilt, og der er etableret funktionsadskillelse mellem medarbejdere i udviklingsafdelingen og i drifts- og supportafdelingen.

Som led i LIFE's udvikling og test af undervisningsindholdet testes der aldrig på personoplysninger, der er omfattet af databehandleraftalen.

Adgangskontrol

Som beskrevet i C.2.1.2 har LIFE's medarbejdere ikke administrative adgang til driftsmiljøet på MY:LIFE og ikke adgang til at se eller behandle personoplysningerne der.

Hos underdatabehandleren Lindhardt og Ringhof Forlag A/S har få medarbejdere adgang til personoplysningerne med henblik på at problemsøge, og fejlfinde i interne systemer i forhold til at optimere LIFE's produkters performance og dermed understøtte formålet med databehandlingen.

Underdatabehandleren har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem med multi-factor authentication (MFA). Medarbejdere oprettes med unik brugeridentifikation og password og brugeridentifikationen anvendes ved tildeling af adgang til ressourcer og systemer.

Rettigheder til systemer og data tildeles underdatabehandlerens medarbejdere ud fra et arbejdsbetinget behov, og følger en fast procedure der sikrer, at adgange kun gives efter specifik godkendelse fra manager. Alle medarbejders rettigheder og adgange gennemgås hver anden måned for at sikre, at de fortsat er korrekt registreret, at nye medarbejdere er oprettet korrekt og gamle er rettidigt lukket.

Fortrolighed og aftalt tavshedspligt

Alle ansatte hos både LIFE og underdatabehandleren er underlagt tavshedspligt gennem ansættelseskontrakten. Gennem procedurer for on- og off boarding sikres det, at de ansatte er opmærksomme på de forpligtelser, der følger af fortroligheds- og tavshedspligten.

Awareness træning

Alle ansatte hos både LIFE og underdatabehandler gennemgår awareness træning mindst 1 gang årligt med fokus på persondataretlige forhold og IT-sikkerhed.

Sletning af datamedier

Når der opsættes brugte computere til nye medarbejdere, og når harddiske skal ud af huset til destruktion, bliver alt data og dataspor slettet efter nærmere procedurer.

Fortegnelse over kategorier af behandlingsaktiviteter

Både LIFE og underdatabehandleren har indført politikker og procedurer, der sikrer, at der føres fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen ajourføres regelmæssigt. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

Fysisk sikkerhed

Det fysiske datamiljø, som personoplysningerne behandles i, er hosted, sikret og adgangskontrolleret via Lindhardt og Ringhof Forlag A/S' underdatabehandler, Amazon Web Services.

Amazon Web Services er ISO 27001-certificeret for informationssikkerhed og aflægger årligt SOC2-erklæringer, som i lighed med ISAE 3000-erklæringer dokumenterer it-sikkerhed, tilgængelighed, fortrolighed, ægthed og beskyttelse af de registreredes rettigheder.

Eksterne kommunikationsforbindelser

Når der anvendes eksterne kommunikationsforbindelser ved tilslutning til internettet, andre åbne net, samt ved brug af interne webapplikationer sikrer databehandleren 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).

Logning

For at sikre platformens stabilitet og drift logger fejl og performance i kritiske services i produktionsmiljøet. For at sikre overblik og overvågning af disse services anvendes et internt system, Sentry.io (algoritmer til brug for fejlsøgning og overvågning). Dette betyder, at data opsamlet til analyse ikke forlader databehandlerens interne systemer.

Der logges ikke forbrugshistorik på brugerniveau.

Underdatabehandleren har desuden en adgangslug i AWS, der overvåger, hvilke medarbejdere, som har adgang til de specifikke systemer, da denne information skal kunne findes i forbindelse med et databrud eller et kritisk systemnedbrud.

Alle logs slettes automatisk efter 60 dage.

Genopretning af tilgængelighed til personoplysninger

Den digitale undervisningsplatform MY:LIFE hostes i skyen hos AWS. Kildekoden ligger hos Github og er ligeledes sikret ved fysisk adskilt duplikering. Underdatabehandleren vil derfor ikke blive påvirket af en fysisk eller elektronisk hændelse. Såfremt der skulle ske en teknisk hændelse, og afhængig af graden af hændelsen, er det underdatabehandlerens vurdering, at tjenesten vil være oppe at køre igen inden for et døgn og maksimalt senest inden for 7 arbejdsdage. Underdatabehandleren har en proces for "disaster and recovery", der træder i kraft ved en sådan hændelse.

Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden

Som en del af underdatabehandlerens ISAE 3000 opdateres og forbedres procedurer løbende for at sikre effektiviteten af de tekniske og organisatoriske foranstaltninger, der skal sikre den rette behandling af personoplysninger. Ved tekniske ændringer til systemer, der håndterer personoplysningerne, opdateres og efterprøves procedurer efter behov. Procedurene efterses årligt af et eksternt revisionselskab, der som uvildig part sikrer, at procedurerne efterleves og lever op til gældende standarder.

Hjemmearbejdspladser

Underdatabehandlerens 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 server-miljøer sker gennem en avanceret kryptografisk keybaseret forbindelse til det fysiske datamiljø, der er sikret med *Amazon Web Services*.

C.3 Bistand til den dataansvarlige vedr. den registreredes rettigheder samt evt. brud på persondatasikkerheden

LIFE 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 følgende tekniske og organisatoriske foranstaltninger:

Begæring vedrørende registreredes rettigheder

LIFE skal uden unødigt forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til LIFE eller dennes underdatabehandler fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret.

LIFE er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. LIFE skal i stedet på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

Databehandlerens information om brud på persondatasikkerhed til den dataansvarlige, jf. punkt 10.4 i Databehandleraftalen

Det påhviler LIFE at underrette den dataansvarlige uden unødigt forsinkelse – og så vidt muligt inden 24 timer, jf. 10.2 – efter at være blevet bekendt med et brud på persondatasikkerheden. Underretningen vil om muligt indeholde følgende oplysninger:

1. Dato og tidspunkt for bruddet
2. Er bruddet ophørt igen – og hvornår?
3. Beskrivelse af, hvad der er sket i praksis
4. Årsagen til bruddet
5. Hvilke typer personoplysninger, der er berørt – og hvor mange
6. Hvilke registrerede, der er berørt – og hvor mange

7. Hvilke sandsynlige konsekvenser, bruddet har for de berørte personer
8. Hvilke afhjælpende foranstaltninger, der er truffet fra LIFEs og LIFEs underdatabehandlers side
9. Om underretningen er endelig eller om den dataansvarlige kan forvente supplerende oplysninger og i så fald tidshorisonten herfor
10. Oplysninger om, hvor den dataansvarlige kan få yderligere oplysninger

C.4 Opbevaringsperiode/sletterutine

Ved ophør eller opsigelse af Bevillingsvilkårene vedrørende brugen af MY:LIFE, er LIFE 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.

Oplysningerne slettes automatisk senest tre (3) måneder efter den dataansvarlige Institution har meddelt LIFE, at man ønsker at ophøre med brug af MY:LIFE.

Hvis Institutionen ønsker, at oplysningerne skal slettes før, skal Institutionen rette henvendelse til LIFE herom. Kontaktoplysninger fremgår af side 1.

Personoplysningerne i MY:LIFE slettes endvidere i følgende tilfælde:

- Vores underdatabehandler har konfigureret platformen til at slette data om elever eller lærere, hvis de pågældende lærere eller elever skifter til en anden institution, som der ikke er indgået databehandleraftale med. **Bemærk, at denne sletteproces udløses ved at brugeradministrator for den pågældende institution via <https://brugeradministration.emu.dk/> fjerner elevens/lærerens UNI-log fra skolens institutionsnummer.**
- Når en elev udskrives af skolen og dermed ikke længere er tilknyttet et institutionsnummer
- Hvis den pågældende Institution anmoder om sletning på vegne af den registrerede person til persondata @life.dk. Hvis LIFE kan efterkomme sletteanmodningen helt eller delvist, sker sletning inden 45 dage.

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:

- På de i Bilag B nævnte lokaliteter

LIFE er berettiget til at overføre eller tillade overførsel af personoplysninger til behandling uden for Danmark. Mht. behandling i tredjelande se punkt C.6 nedenfor.

Som led i driften af MY:LIFE opbevares personoplysninger hos Amazon Web Services, Irland, som underdatabehandler, jf. B.1. Disse data bliver udelukkende opbevaret, behandlet og supporteret i EU.

For at sikre dette har LIFEs underdatabehandler etableret et teknisk set-up hos AWS, der betyder, at enhver adgang til persondata fra lokationer udenfor EU/EØS kræver underdatabehandlerens positive godkendelse. Underdatabehandleren har indført procedurer der skal sikre, at en sådan positiv bekræftelse ikke gives, herunder at support tickets ikke må forlade EU.

Datatilsynets udtalelse af 29. marts 2022 i KOMBIT-sagen om tolkning af AWS GDPR Data Processing Addendum, afsnit 12.1., har sået tvivl om, hvorvidt valget af geografisk region til "EU" er uden undtagelse – eller om den dataansvarlige skal indrette sig som om data reelt behandles udenfor EU.

Det er underdatabehandlerens og LIFEs vurdering, at valget af "EU" som region er effektivt.

Dette skyldes,

- at underdatabehandleren ikke har tilkøbt nogen ekstraydelser fra AWS, som kunne begrunde flytning af data ud af EU for at levere specifikke AWS-services (1. undtagelse), og
- at underdatabehandleren i juni 2022 formelt har indskærpet sin instruks overfor AWS om, at AWS i overensstemmelse med den indgåede databehandleraftale alene må behandle personoplysningerne indenfor EU (2. undtagelse)
- at Datatilsynet i KOMBIT-udtalelsen ikke forholder sig til AWS' "Supplementary Addendum to AWS GDPR Data Processing Addendum", som nøje beskriver AWS' tiltag for at undgå at efterkomme en US-udleveringsanmodning og som taler for, at AWS eksplicit påtager sig at overholde databehandlerinstruksen om valgt EU-region, hvis denne kommer i konflikt med en myndighedsanmodning fra de amerikanske efterretningsmyndigheder og dermed den europæiske lovgivning.

Af disse årsager er det LIFEs og underdatabehandlerens vurdering, at data behandles i – og kun i – EU iht. instruksen. Af denne grund har underdatabehandleren ikke indgået SCC'er med AWS eller gennemført supplerende foranstaltninger til sikring af at den europæiske databeskyttelse ikke undermineres (som beskrevet i C.2.1.3., er der således ikke implementeret stærk kryptering af data i ro med nøgle hos tredjepart).

Håndteringen af dataudleveringer pbga. en US-myndighedsanmodning er herefter – efter underdatabehandlerens og LIFEs opfattelse – et spørgsmål om behandlingssikkerhed og risiko for tab af fortrolighed, jf. art. 32. Dette spørgsmål er behandlet ovenfor i C.2.1.3.

Underdatabehandleren har dokumenteret ovenstående overfor LIFE. Dokumentationen ajourføres årligt på baggrund af underdatabehandlerens tilsyn med AWS som underdatabehandler.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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

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

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. 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 underdatabehandlere(n).

