# Databehandleraftale

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

mellem

Ryparken Lille Skole
CVR 28997418
Gartnerivej 3
2100 København Ø
Danmark

herefter "den dataansvarlige"

og

Lindhardt og Ringhof Forlag A/S
CVR-nr. 76351910
Vognmagergade 11
1120 København K
Danmark

herefter "databehandleren"

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

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

# 1. Indhold

## 2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af digitale læremidler behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

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

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

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

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

## 3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med

databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

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

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

## 4. Databehandleren handler efter instruks

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

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

## 5. Fortrolighed

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

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

## 6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau,

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

implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

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

a. Pseudonymisering og kryptering af personoplysninger

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

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

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

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

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

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

## 7. Anvendelse af underdatabehandlere

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

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

   Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 60 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

3. 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.

4. 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.

5. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

6. 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.

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

## 9. Bistand til den dataansvarlige

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

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

    a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

c. indsigtsretten
d. retten til berigtigelse
e. retten til sletning ("retten til at blive glemt")
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

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

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

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

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

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

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

## 10. Underretning om brud på persondatasikkerheden

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

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at

den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

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

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

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

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

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

## 11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

## 12. Revision, herunder inspektion

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

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmeret angivet i Bilag C.8. og C.9.

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

## 13. Parternes aftale om andre forhold

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

## 14. Ikrafttræden og ophør

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

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

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

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.6, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

| | |
|---|---|
| Navn | Casper Bartels |
| Stilling | IT-ansvarlig |
| Telefonnummer | +45 3929 6639 |
| E-mail | casper@ryp.dk |
| Underskrift | Casper Bartels<br>Casper Bartels (26. apr. 2023 12:03 GMT+2) |

   På vegne af databehandleren

| | |
|---|---|
| Navn | Pernille Christensen |
| Stilling | Kundechef - Kundeservice |
| Telefonnummer | +45 2134 4860 |
| E-mail | Databehandling@lrforlag.dk |

Underskrift

## 15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

| | |
|---|---|
| Navn | Casper Bartels |
| Stilling | IT-ansvarlig |
| Telefonnummer | +45 3929 6639 |
| E-mail | kontor@ryp.dk |

| | |
|---|---|
| Navn | Jonas Nielsen |
| Stilling | Digital udviklingschef |
| Telefonnummer | +45 6171 1712 |
| E-mail | Databehandling@lrforlag.dk |

# Bilag A: Oplysninger om behandlingen

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

Formålet med behandling af personoplysninger er at give adgang til databehandlerens digitale læremidler i henhold til Aftalen.
De digitale læremidler udbydes i en portal på internettet, hvortil elever og lærere gives adgang. Forskellige undervisningsforløb kan herefter understøttes/gennemføres vha. en internetbrowser, en app eller andet formidlingsmedie.

Personoplysningerne behandles af databehandleren for at kunne stille indholdet på de digitale læremidler til rådighed for den enkelte bruger samt løbende at sikre, at de digitale læremidler skaber optimalt læringsudbytte, er brugervenlige og lette at navigere i. Dette kræver, at der behandles oplysninger om brug af de digitale læremidler til brug for analyse.

Databehandleren behandler desuden personoplysningerne for, at brugerne kan anvende databehandlerens digitale læremidler, herunder besvare opgaver, bedømme opgaver og foretage egen-evaluering af opgaveløsning, samt at brugerne kan få support, såfremt behovet skulle opstå.

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

Databehandleren foretager følgende behandlinger af personoplysninger på vegne af den dataansvarlige:

- Etablering af den dataansvarliges brugeres adgang til de digitale læremidler ved at elevers/læreres Unilogin-oplysninger overføres fra Styrelsen for It og Læring (STIL) til databehandleren i forbindelse med login.
- Administration af brugernes adgange til tilknyttede læringsmoduler
- Opbevaring af de personoplysninger, som databehandleren modtager via STIL, og som brugerne potentielt indtaster ved brug af databehandlerens digitale læremidler
- Behandling af anonymiserede forbrugsdata til brug for rapportering til den dataansvarlige, herunder den dataansvarliges institution(er), om anvendelsen af de digitale læremidler
- Behandling af supporthenvendelser fra brugerne i forbindelse med anvendelsen af de digitale læremidler.

Ovennævnte aktiviteter indebærer at personoplysningerne bearbejdes som følger:

- indsamling,
- registrering,
- organisering,
- systematisering,
- opbevaring,
- tilpasning eller ændring,
- genfinding,
- søgning,
- brug,

- sletning/tilintetgørelse/anonymisering

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

Behandlingen omfatter almindelige oplysninger, jf. databeskyttelsesforordningen. Behandlingen tager udgangspunkt i eksport af personoplysninger fra Uni-login (ws17/wsiEKSPORT, lille pakke) og omfatter fornavn(e) og efternavn.

Supplerende oplysninger om elever:

- Studietype (elev/studerende)
- Studienummer
- Elevens niveau (for grundskoleelever)
- Elevens hovedgruppe (klasse)
- Yderligere grupper elever er tilknyttet
- Afdeling, bygning eller værelsesnummer på efterskoler
- ID i det lokale studieadministrative system

Supplerende oplysninger om ansatte:

- Ansættelsestype (lærer, tap, pæd eller gæst)
- Initialer
- Stilling
- Afdeling, bygning eller værelsesnummer på efterskoler
- Grupper medarbejderen er tilknyttet

Oplysninger om UNI-login for ansatte og elever/studerende:

- Uni login-brugernavn (bruger-id)

Oplysninger om grupper på institutionen:

- Gruppe-id
- Gruppenavn
- Gruppetype
- Niveau
- Spor
- Startdato
- Slutdato

Ved brugen af de digitale læremidler behandles desuden følgende personoplysninger af databehandleren:

- Loginoplysninger,
- Pseudonymiseret bruger-id,
- IP-adresse,
- forbrugsdata,
- brugernes anvendelse af databehandlerens digitale læremidler (kliks, tidsforbrug mv.), herunder besvarelse af opgaver, bedømmelse af opgaver og egen-evaluering af opgaveløsning.

### A.4. Behandlingen omfatter følgende kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede:
A) Elever, herunder studerende.
B) Lærere, herunder pædagoger og andre, der har en undervisningsfunktion.

C) Administrativt personale, herunder personer med tilknytning til en uddannelsesinstitution.

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

Databehandleren behandler personoplysningerne i den periode, som er relevant for, at databehandleren kan opfylde Aftalen.

Databehandleren sletter/anonymiserer oplysningerne senest 6 måneder efter eleven/læreren er slettet fra STILs systemer og ikke længere er aktive i disse, se supplerende oplysninger i hyperlink under afsnit C.2.4.

# Bilag B: Underdatabehandlere

## B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere for den beskrevne behandlingsaktivitet.

Microsoft Ireland Operations og Amazon Web Services er medtaget i nedenstående, da Lindhardt og Ringhof fører selvstændigt tilsyn med underdatabehandleren selvom aftalepartneren er Egmont IT.

| Navn | Datalokation | Firmaadresse | System | Beskrivelse af behandling |
|---|---|---|---|---|
| **Sentia A/S** | Sentia hostingcenter i EU | Lyskær 3A, DK-2730 Herlev, Danmark<br><br>CVR: 10008123 | Lindhardt og Ringhofs digitale læremidler | Hosting af digitale læremidler, herunder vedligehold af servere, backup, sikkerhed mv. Hosting sker i deres hostingcenter i Danmark. |
| **Microsoft Ireland Operations, Ltd.**<br><br>**(Azure West Europe Region)** | Azure datacenter i EU/EØS – specifikt West Europe region (Holland) | One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland | Lindhardt og Ringhofs digitale læremidler | Hosting af digitale læremidler, herunder vedligehold af servere, backup, sikkerhed mv. |
| **Egmont IT ved Egmont Fonden** | Azure datacenter i EU/EØS | Vognmagergade 11, 1148 København K<br><br>CVR: 11456111 | Alle digitale læremidler | Drift af løsninger på Microsoft Azure og Amazon AWS, herunder administration af miljøer, overvågning, brugeradministration mv. |
| **Dixa ApS** | AWS datacenter i EU/EØS | Vimmelskaftet 41A, 1 Sal., 1161 Copenhagen S<br><br>CVR: 36561009 | Kundesupport på alle digitale læremidler | Sagsstyringssystem til håndtering af kundehenvendelser. |
| **Sii Sp. z o.o** | Azure datacenter i EU/EØS | al. Niepodległości 69, 02-626 Warszawa, 3rd floor, Metron building<br><br>VAT: 140381516 | Lindhardt og Ringhofs digitale læremidler | Udvikling og support af licenssystem. |
| **Amazon Web Services EMEA SARL** | AWS datacenter i EU/EØS – specifikt region Irland | 38 Avenue John F. Kennedy L-1855 Luxembourg | Digitale læremidler på clio.me | Databehandleren hoster digitale læremidler ved brug af AWS' laaS (infrastructure-as-a-service). |

B.1.2. Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet.

**B.2. Varsel for godkendelse af underdatabehandlere**

B.2.1. Den dataansvarlige kan – ved skriftlig henvendelse til databehandleren hurtigst muligt og senest 30 dage efter dennes varsel for godkendelse af underdatabehandlere i henhold Bestemmelsernes 7.2. – modsætte sig brugen af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og/eller aftalte, og brugen af en anden underdatabehandler til denne behandlingsaktivitet, hvis der foreligger en saglig begrundelse herfor.

B.2.2 Modsætter den dataansvarlige sig brugen af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte og/eller brugen af en anden underdatabehandler til denne behandlingsaktivitet, må behandlingen af personoplysninger hos den pågældende underdatabehandler ikke påbegyndes.

# Bilag C: Instruks vedrørende behandling af personoplysninger

## C.1. Behandlingens genstand/instruks

C.1.1 Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Enhver behandling, som er nødvendig for, at databehandleren kan opfylde de forpligtelser, der er fastsat i Aftalen, herunder:

- Behandling af personoplysninger i forbindelse med brug af databehandlerens digitale læremidler, jf. Bilag A.
- Behandling af brugerhenvendelser via supportsystemer, jf. Bilag A og Bilag B.1.

Personoplysningerne behandles af databehandleren for at kunne stille indholdet på de digitale læremidler til rådighed for den enkelte bruger samt løbende at sikre, at de digitale læremidler er brugervenlige og lette at navigere i.

Databehandleren behandler desuden personoplysningerne for, at brugerne kan anvende databehandlerens digitale læremidler, herunder besvare opgaver, bedømme opgaver og foretage egen-evaluering af opgaveløsning, samt at brugerne kan få support, såfremt behovet skulle opstå.

Databehandleren behandler ligeledes personoplysninger for at kunne dokumentere overfor den dataansvarlige, hvor mange gange brugerne har logget sig på databehandlerens digitale læremidler (forbrugsdata).

Personoplysningerne kan endelig blive brugt i forbindelse med support af service og infrastruktur og databehandlerens logning.

## C.2. Behandlingssikkerhed

C.2.1. Sikkerhedsniveauet skal afspejle behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. Som følge heraf har den dataansvarlige og databehandleren begge udarbejdet en risikoanalyse vedrørende databehandlingen og er enige om de foranstaltninger som er beskrevet i det følgende.

C.2.2. databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

C.2.3. databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige herunder.

C.2.4. Databehandleren har vurderet, at de konkrete behandlingsaktiviteter medfører et lavt risikoniveau for de registrerede. Dog medfører det forhold, at behandlingen også vedrører almindelige persondata på børn, at databehandleren vælger at betragte risikoniveauet som "medium". Databehandleren implementerer derfor et sikkerhedsniveau der modsvarer en risikovurdering på niveauet

"medium" jf. European Network and Information Security Agency's (ENISA) "Handbook on Security of Personal Data Processing".
De aftalte sikkerhedsforanstaltninger fremgår af databehandlerens beskrivelse på:

- **L&R sikkerhedsforanstaltninger (https://www.alinea.dk/lr-sikkerhedsforanstaltninger)**

**C.3 Bistand til den dataansvarlige**
C.3.1. Databehandleren skal så vidt muligt – inden for nedenstående 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, jf. Bestemmelse 9.3**

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

Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren 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 data-beskyttelsesret.

**Databehandlerens information om brud på persondatasikkerhed til den dataansvarlige, jf. Bestemmelse 9.3 og 10.4**

Det påhviler databehandleren at underrette den dataansvarlige uden unødig forsinkelse efter at være blevet bekendt med et brud på persondatasikkerheden. Underretningen vil om muligt indeholde følgende oplysninger:

- Dato og tidspunkt for bruddet
- Dato og tidspunkt for bruddets konstatering
- Er bruddet ophørt igen – og hvornår?
- Sammenlagt varighed af bruddet
- Beskrivelse af hændelsen
- Årsagen til bruddet
- Hvilke typer personoplysninger, der er berørt – og hvor mange
- Hvilke registrerede, der er berørt – og hvor mange
- Hvilke sandsynlige konsekvenser, bruddet har for de berørte personer
- Hvilke afhjælpende foranstaltninger, der er truffet fra databehandlerens side og databehandlerens underdatabehandleres side
- Om underretningen er endelig eller om den dataansvarlige kan forvente supplerende oplysninger og i så fald tidshorisonten herfor
- Oplysninger om, hvor den dataansvarlige kan indhente yderligere oplysninger
- Evt. andre oplysninger, som er nødvendige for, at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens art. 33

**C.4 Opbevaringsperiode/sletterutine**

C.4.1 Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren senest 60 dage efter ophør af aftalen, slette alle de behandlede personoplysninger i overensstemmelse med Bestemmelse 11 & A.5., medmindre den dataansvarlige – efter underskriften af disse Bestemmelser – har ændret sit oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

**C.5 Lokalitet for behandlingen**

C.5.1. Lokaliteten for databehandlerens behandlingen af de af Bestemmelserne omfattede personoplysninger er databehandlerens adresse samt lokationerne nævnt for underdatabehandlere i Bilag B.

C.5.2. Lokaliteten for de på tidspunktet for Bestemmelsernes ikrafttræden godkendte underdatabehandleres behandling af de i Bestemmelserne omfattede personoplysninger følger af Bilag B.1.1.

C.5.3. Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter.

**C.6. Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren**

C.6.1. Databehandleren skal årligt foranledige, at der udarbejdes en revisionserklæring i overensstemmelse med anerkendt standard (pt. FSR ISAE3000 GDPR) herfor vedrørende databehandlerens overholdelse af Databeskyttelsesforordningen.

C.6.2.Revisionserklæringen fremsendes uden vederlag og unødig forsinkelse til den dataansvarlige til orientering. Såfremt den dataansvarlige måtte ønske andre eller supplerende revisionserklæringer aftales særskilt procedure og vederlag herfor.

C.6.3. Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner af lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner gennemføres efter nærmere aftale, såfremt den dataansvarlige finder det nødvendigt.

C.6.4. Omkostninger i forbindelse med en inspektion som nævnt i C.7.3 afholdes af den dataansvarlige. Databehandleren er forpligtet til at afsætte de nødvendige interne ressourcer, der er nødvendig for, at inspektionen kan gennemføres.

C.6.5. Foretager Datatilsynet tilsyn med databehandleren på eget initiativ afholdes alle udgifter i forbindelse hermed af databehandleren.

**C.7 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere**

C.7.1. Databehandleren skal årligt gennemføre et tilsyn vedrørende underdatabehandlerens overholdelse af Databeskyttelsesforordningen. Databehandleren tilrettelægger tilsynet på baggrund af databehandlerens

risikoanalyse af den enkelte underdatabehandlers konkrete databehandlingsaktiviteter.

C.7.2. Databehandlerens tilsynsaktiviteter dokumenteres og kan på anfordring fra den dataansvarlige stilles til dennes rådighed. Den dataansvarlige er berettiget til at anfægte rammerne for og/eller metoden i tilsynet, og kan i sådanne tilfælde - med angivelse af den konkrete årsag til, at det oprindelige tilsyn anses for utilstrækkeligt - anmode om et nyt tilsyn.

C.7.3. Baseret på resultatet af tilsynet er den dataansvarlige berettiget til at anmode om en gennemførelse af yderligere (kontrol)foranstaltninger med henblik på at sikre overholdelsen af Databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

C.7.4. Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af den dataansvarliges personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner gennemføres, når databehandleren eller den dataansvarlige finder det nødvendigt.

C.7.5. Den dataansvarlige kan anfægte rammerne og/eller metoden for den gennemførte inspektion, såfremt den dataansvarlige kan påvise, at inspektionen har været utilstrækkelig. I sådanne tilfælde skal en eventuel fornyet inspektion gennemføres efter overenskomst med databehandlerens om blandt andet rammer/metode samt fordeling af vederlag/omkostningsdækning for inspektionen.

# Bilag D: Parternes regulering af andre forhold

## I Indledning

Nedenstående notat indeholder databehandlerens redegørelse for databehandlerens håndtering af problemstillingen vedrørende brug af Amazon Web Service og Microsoft Azure's cloud services. Grundlaget for databehandlerens redegørelse og vurderinger er de aftaler, der er indgået mellem databehandleren og henholdsvis AWS Web Services EMEA Sarl og Microsoft Ireland Operations Limited, dvs. de indgåede databehandleraftaler og instrukser (aftalegrundlaget),

## II Problemstilling i relation til brug af Amazon Web Services som cloud leverandør

### 1. Amazon Web Services' cloud service, herunder håndtering af support-sager

Databehandleren har ved brug af Amazon Web Services' (i det følgende benævnt AWS) cloud service aktivt valgt Irland som region for AWS' databehandling og dermed instrueret AWS i, at databehandlingen alene må ske indenfor EU/EØS. Derudover har databehandleren i tilfælde af behov for support sikret et teknisk set-up, der indebærer, at enhver adgang til personoplysninger (også inden for EU/EØS) kræver databehandlerens forudgående godkendelse og tildeling af adgang. Dette er sikret ved, at adgang er konfigureret via en proxy server som beskrevet i Bilag C.2. Adgang til denne proxy server er beskyttet med symmetrisk kryptering, hvor de private krypteringsnøgler, der er nødvendige for at opnå adgang, opbevares af databehandleren i en yderligere krypteret datafil, udenfor AWS. Databehandleren har således indført procedurer, der skal sikre, at databehandleren har kontrol med, hvem, der får adgang til personoplysningerne.

Ovenstående indebærer, at der ikke sker overførsler af personoplysninger til tredjelande i forbindelse med AWS' udførelse af cloud service, herunder i forbindelse med support-sager.

Det skal i den forbindelse oplyses, at der generelt set alene vil være behov for support fra AWS i sjældne tilfælde ved kritiske driftsfejl og nedbrud, og at databehandleren til dato ikke har haft behov for support af en sådan karakter fra AWS. Derudover har AWS heller ikke til dato af egen drift anmodet databehandleren om adgang til databaser, der indeholder personoplysninger.

### 2. Udleveringsanmodning fra de amerikanske myndigheder

Databehandleren er bevidst omkring det forhold, at en cloud leverandør, der er etableret i EU/EØS, qua sin koncernstruktur, kan blive mødt med anmodninger om udlevering af personoplysninger fra myndigheder i det tredjeland, hvor cloud leverandørens moderselskab er beliggende.

Som så mange andre virksomheder gør databehandleren brug af AWS som cloud leverandør. Både hovedkontrakten om levering af AWS' services samt databehandleraftalen er indgået med AWS Web Services EMEA Sarl (i det følgende benævnt AWS), og er i henhold til AWS' standardbetingelser.

Eftersom AWS' moderselskab er beliggende i USA, er det imidlertid nødvendigt at forholde sig til, om de amerikanske efterretningsmyndigheder vil kunne få adgang til de personoplysninger, som databehandleren behandler.

## 2.1 Amerikanske efterretningsmyndigheders adgang til personoplysninger

I det følgende har databehandleren forholdt sig til de tre hjemmelsgrundlag, som i videst omfang har været genstand for drøftelser i den seneste tid, og som den europæiske domstol i en vis udstrækning har forholdt sig til. Databehandlerens vurdering er alene baseret på baggrund af de informationer, som databehandleren har kendskab til.

FISA 702

FISA 702 (Foreign Intelligence Surveillance Act) (lov om overvågning af udenlandsk efterretningsvirksomhed)) vedrører adgang til personoplysninger om ikke-amerikanere, der befinder sig udenfor USA, og som forventes at besidde, modtage eller kommunikere udenlandske efterretningsoplysninger.

Formålet med FISA 702 er at opnå beskyttelse mod udenlandske angreb, terrorisme, spredning af masseødelæggelsesvåben og USA's håndtering af udenrigsanliggender.

Det fremgår ikke entydigt, om FISA 702 er eksterritorial, og derved kun finder anvendelse på virksomheder, der opererer i USA, eller om der tillige er adgang til data, der opbevares i EU af eksempelvis datterselskaber til amerikanske selskaber.

Datatilsynet angiver i fodnote 26, side 29 i Vejledning om cloud, at "Datatilsynet er bekendt med, at der er blevet fremført, at anden amerikansk lovgivning, herunder FISA 702, har eksterritorial virkning på samme vis som US CLOUD ACT. Der er imidlertid for nuværende Datatilsynets opfattelse, at det ikke er klarlagt i praksis, om – og i hvilket omfang – bl.a. FISA 702 har ekstraterritorial virkning."

På baggrund af ovenstående lægger databehandleren derfor til grund, at FISA 702 ikke finder anvendelse i relation til databehandlerens brug af AWS.

E.O. 12333

Executive Order 12333 (E.O. 12333) omhandler adgang til oplysninger, der er i "transit" til USA ved, at de amerikanske myndigheder kan opnå adgang til sådanne oplysninger ved at tilgå de undersøiske kabler, der ligger på havbunden i Atlanterhavet, og indsamle og opbevare disse oplysninger, før de når til USA. Oplysningerne bliver herefter undergivet FISA's bestemmelser.

Formålet med E.O. 12333 er indsamling af oplysninger vedrørende bl.a. udenlandsk efterretningstjeneste, kontraspionage, international narkotika eller international terrorundersøgelse.

Eftersom der ikke sker overførsel af personoplysninger til USA i forbindelse med databehandlerens levering og drift af digitale læremidler via databehandlerens platform, lægger databehandleren til grund, at E.O. 12333 ikke finder anvendelse i relation til databehandlerens brug af AWS.

US CLOUD ACT

US CLOUD ACT vedrører adgang til personoplysninger (uanset deres placering) på baggrund af en anmodning og en efterfølgende dommerkendelse. Formålet er efterforskning af kriminalitet, og gælder for alle elektroniske

kommunikationsvirksomheder eller remote computing-tjenester fra cloud leverandører til social media-sites og teleselskaber, som opererer under amerikansk lov, herunder europæiske virksomheder med datterselskaber i USA.

Der skal foreligge en klar, præcis og proportionel anmodning i forhold til de data, som ønskes udleveret. Anmodningen skal angive en navngiven person.

US CLOUD ACT indebærer i en vis udstrækning eksterritorialitet og i henhold til databehandlerens nuværende kendskab vil en myndighedsanmodning rettet mod AWS vedrørende udlevering af de personoplysninger, som databehandleren behandler, formentlig alene kunne komme på tale i medfør af US CLOUD ACT.

**2.2 Databehandlerens instruks til AWS**

Databehandleraftalen "AWS GDPR DATA PROCESSING ADDENDUM" (i det følgende benævnt "GDPR Addendum") er en del af AWS' standardbetingelser. GDPR Addendum indeholder vilkår omhandlende *"Transfers of Personal Data"* i pkt. 12.1 med følgende ordlyd:

*"Regions. Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "Region"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body."*

Databehandleren har i overensstemmelse med ovenstående valgt Irland som region for AWS' databehandling, som dermed er en del af instruksen fra databehandleren til AWS.

Det er databehandlerens opfattelse, at ordlyden *"..or as necessary to comply with the law or binding order of a governmental body"* i pkt. 12.1, har karakter af et generelt forbehold, idet det ikke nærmere er specificeret, hvilke love og/eller bindende myndighedsanmodninger der refereres til.

Endvidere vil det som ovenfor nævnt i forhold til databehandleren formentlig alene være myndighedsanmodninger i medfør af US CLOUD ACT, der kan komme på tale. Her vil det være nødvendigt med en dommerkendelse, hvorfor en myndighedsanmodning alene, jf. ordlyden *"..or binding order of a governmental body,"* ikke vil være tilstrækkeligt grundlag for en udlevering af databehandlerens personoplysninger. Dette forhold taler ligeledes for, at der med AWS' ordlyd i pkt. 12.1 er tale om et generelt forbehold.

Vedrørende myndighedsanmodninger om udlevering af personoplysninger har AWS i SUPPLEMENTARY ADDENDUM TO AWS GDPR DATA PROCESSING ADDENDUM" (i det følgende benævnt "Supplementary Addendum") beskrevet, hvilke foranstaltninger AWS vil træffe i tilfælde af en sådan anmodning. Den beskrevne proces må ligeledes skulle læses i lyset af AWS' forpligtelse om at skulle overholde instruksen fra databehandleren om, at Irlands-regionen er valgt som lokalitet for AWS' databehandling.

Det fremgår således af pkt. 1.1 i Supplementary Addendum under overskriften *"Requests for Customer Data,"* at

*"If AWS receives a valid and binding order ("Request") from any governmental body ("Requesting Party") for disclosure of Customer Data, AWS will use every reasonable effort to redirect the Requesting Party to request Customer Data directly from Customer."*

*"..If compelled to disclose Customer Data to a Requesting Party, AWS will:*

*(a) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so. If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible; and*

*(b) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union or applicable Member State Law)."*

Endvidere er det i pkt. 1.2 anført at: *"..If compelled to disclose Customer Data to a Requesting Party, AWS will:*

*(a) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so. If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible; and*

*(b) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union or applicable Member State Law)."*

Ovenstående bestemmelser i AWS' standard databehandleraftale taler således for, at AWS eksplicit påtager sig at overholde instruksen i forbindelse med en eventuel myndighedsanmodning fra de amerikanske efterretningsmyndigheder og dermed den europæiske lovgivning.

AWS' overholdelse af europæisk lovgivning

Det forhold, at AWS har pligt til at overholde den europæiske lovgivning og dermed GDPR-lovgivningen følger i øvrigt implicit af AWS' egenskab som databehandler. Derudover anfører AWS flere steder i GDPR Addendum, at AWS overholder den europæiske GDPR-lovgivning.

GDPR er i GDPR Addendum defineret på følgende vis:

*"Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)."*

Det fremgår bl.a. af pkt. 1.4 i GDPR Addendum, at *"..Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR."*

Utilsigtet overførsel af databehandlerens personoplysninger

På baggrund af ovenstående er det således databehandlerens vurdering, at såfremt AWS måtte vælge at efterkomme en myndighedsanmodning i henhold til US CLOUD ACT og overføre databehandlerens data til USA, vil AWS anses for at handle udenfor instruks. AWS vil dermed handle i strid med databehandleraftalen og der vil derfor være tale om en utilsigtet overførsel af databehandlerens personoplysninger.

Denne fortolkning understøttes af Datatilsynets vejledning om cloud side 29 hvoraf følgende fremgår: *"Hvis databehandleren vælger at overføre personoplysninger til tredjelandet i strid med databehandleraftalen, vil der være tale om en utilsigtet overførsel, og det betyder, at databeskyttelsesforordningens regler om overførsel til tredjelande ikke finder anvendelse i forhold til den dataansvarlige."*

Endvidere fremgår det af Datatilsynets vejledning om cloud side 30, at *"..hvis en databehandler handler i strid med databehandleraftalen ved at videregive personoplysninger til en myndighed i et tredjeland, og dermed selv fastlægger formålene med og hjælpemidlerne til en behandling, vil denne anses for selvstændig dataansvarlig for den pågældende behandling."*

Det skal i den forbindelse nævnes, at databehandleren til dato aldrig er blevet mødt med en myndighedsanmodning fra AWS.

Registreredes krav på erstatning

I tillæg til ovenstående gentager AWS i Supplementary Addendum den registreredes rettigheder under databeskyttelsesforordningens artikel 82, hvorefter den registrerede kan kræve erstatning hos AWS, såfremt den registrerede har lidt skade som følger af AWS' manglende overholdelse af databeskyttelseslovgivningen. Dette er i Supplementary Addendum beskrevet, som følger:

*"Nothing in this Addendum restricts Customer's data subjects from exercising their rights under the GDPR, including their rights to compensation from AWS for material or non-material damage under, or in accordance with, Article 82 of the GDPR."*

Endelig fremgår det af GDPR Addendum, at AWS garanterer overfor sine kunder, at AWS ikke har grund til at tro, at den gældende lovgivning forhindrer AWS i at overholde instruksen fra kunderne, og at AWS garanterer at orientere sine kunder i tilfælde af, at lovgivningen ændrer sig, så AWS ikke længere kan opfylde sine kontraktuelle forpligtelser. I disse tilfælde er kunderne berettiget til at suspendere overførsel af data til AWS samt ophæve kontrakten med AWS. Dette er formuleret i GDPR Addendum pkt. 3 med følgende ordlyd:

*"AWS agrees and warrants that it has no reason to believe that the legislation applicable to it, or its sub-processors, including in any country to which Customer Data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from Customer and its obligations under this Addendum and the AWS GDPR DPA and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum and the AWS GDPR DPA, AWS will promptly*

*notify the change to Customer as soon as AWS is aware, in which case Customer is entitled to suspend the transfer of Customer Data and/or terminate the Agreement."*

Med ovenstående beskriver AWS således selv, at såfremt AWS handler udenfor databehandlerens instruks, vil dette være at betragte som væsentlig misligholdelse af kontraktforholdet, hvorefter databehandleren og/eller de registrerede kan gøre misligholdelsesbeføjelser gældende, hvilket i øvrigt er i overensstemmelse med gældende retsprincipper.

### 2.3 Indskærpelse af databehandlerens instruks overfor AWS

Set i lyset af den seneste tids drøftelser om brug af AWS som cloud leverandør og foranlediget af den usikkerhed, der er opstået på baggrund af Datatilsynets udtalelse af 29. marts 2022 i KOMBIT-sagen vedrørende tilsigtede eller utilsigtede overførsler i forbindelse med udlevering af personoplysninger til myndigheder i tredjelande, har databehandleren valgt at følge op overfor AWS den 2. juni 2022 med en skriftlig indskærpelse af databehandlerens instruks overfor AWS om, at AWS i overensstemmelse med den indgåede databehandleraftale alene må behandle personoplysningerne indenfor EU.

## III Problemstilling i relation til brug af Microsoft Azure som cloud leverandør

### 1. Microsoft Azure's core cloud services, herunder håndtering af support-sager

Udover at gøre brug af AWS' cloud service anvender databehandleren ligeledes Microsoft Azure's cloud service (i det følgende benævnt Microsoft). Såvel den kommercielle aftale (volumenlicensaftalen) og databehandleraftalen er indgået med Microsoft Ireland Operations Limited. I den forbindelse har databehandleren valgt Vesteuropa som region for Microsoft's databehandling. Ved valg af Vesteuropa ligger datacentret i Holland.

Ligesom tilfældet er med AWS har databehandleren i tilfælde af support sikret et teknisk set-up, der indebærer, at en medarbejder hos databehandleren aktivt skal give adgang til databehandlerens data, såfremt en tekniker fra Microsoft skal have adgang. Dette tekniske system er sikret ved et såkaldt "Customer Lock Box" system. Systemet består i, at såfremt Microsofts teknikere ikke kan løse en support-sag uden adgang til databehandlerens indhold, herunder databaser med personoplysninger, kan den pågældende tekniker via Customer Lock Box anmode databehandleren om adgang. Dette giver den eller de personer hos databehandleren, der er tildelt administratorrollen til "kundelåskasseadgangen", mulighed for at godkende eller afvise anmodningen og give direkte adgangskontrol til databehandlerens indhold. Såfremt den pågældende medarbejder med administratorrettigheder til Customer Lock Box systemet godkender anmodningen, modtager teknikeren fra Microsoft godkendelsesmeddelelsen, logger på databehandlerens database, og løser support-sagen. Microsofts teknikere har den af databehandleren ønskede/valgte varighed til at løse problemet, hvorefter adgangen tilbagekaldes automatisk.

Alle handlinger, der udføres af en Microsoft tekniker i forbindelse med en support-sag via Customer Lock Box systemet, logføres i en overvågningslog. Databehandleren kan således til enhver tid søge efter og gennemse disse

overvågningsposter, og vil således altid kunne monitorere hvilke adgange der er givet og til hvem i forbindelse med support-sager.

Databehandleren har med implementering af ovennævnte system sikret et system, hvorefter det er databehandleren som egenhændigt styrer, om Microsofts teknikere skal gives adgang til databehandlerens personoplysninger i forbindelse med en supportsag. På denne måde kan databehandleren ligeledes styre, at en given support altid ydes fra en tekniker, der befinder sig indenfor EU.

Det skal nævnes, at det hos databehandleren alene er få medarbejdere, der er tildelt administratorrollen i forbindelse med håndtering af Customer Lock Box systemet, og at der er indført procedurer, der sikrer, at de pågældende medarbejdere er instrueret i korrekt håndtering af systemet. Endvidere fremgår det af procedurerne, at der aldrig må gives adgang til Microsoft teknikere, der befinder sig udenfor for EU.  Derudover kan det oplyses, at Microsoft heller ikke til dato af egen drift via Customer Lock Box systemet har anmodet databehandleren om adgang til databaser, der indeholder personoplysninger.

Derudover har databehandleren etableret tekniske foranstaltninger som krypterer databasernes data-at-rest med egen krypteringsnøgle (customer-managed-key) således at Microsoft under ingen omstændigheder vil kunne tilgå data-at-rest.

På baggrund af ovenstående sker der således ikke overførsler af personoplysninger til tredjelande i forbindelse med Microsofts udførelse af cloud service, herunder i forbindelse med supportsager.

### 2.1 Amerikanske efterretningsmyndigheders adgang til personoplysninger

I relation til de amerikanske efterretningsmyndigheders adgang til personoplysninger som følge af, at Microsoft Ireland Operations Limited's moderselskab er beliggende i USA henvises til det under Afsnit I, pkt. 2.1 anførte. Det lægges således også her til grund, at en myndighedsanmodning rettet mod Microsoft vedrørende udlevering af de personoplysninger, som databehandleren behandler, formentlig alene vil kunne komme på tale i medfør af US CLOUD ACT, jf. Afsnit I, pkt. 2.1.

### 2.2 Databehandlerens instruks til Microsoft

Som nævnt ovenfor under Afsnit I, punkt 1 har databehandleren aktivt valgt Vesteuropa (Holland) som region for Microsofts databehandling. Valg af region og land for databehandlingen er en del af databehandlerens instruks til Microsoft.

Databehandleraftalen "Tillæg om databeskyttelse for Microsofts Produkter og Tjenester" (senest opdateret 15. september 2022) (i det følgende benævnt "Tillæg om databeskyttelse") er en del af Microsofts standardbetingelser, som finder anvendelse ved kunders køb af Microsofts produkter, herunder køb af Microsofts cloud-løsninger.

En række af de principper, der er formuleret i databehandlerens databehandleraftale med AWS er også at finde i Tillæg om databeskyttelse.

Således indeholder Tillæg om databeskyttelse vilkår omhandlende *"Videregivelse af behandlede data"* hvoraf følgende fremgår:

*"Microsoft hverken videregiver eller giver adgang til Behandlede data, undtagen: (1) efter Kundens anvisninger; (2) som beskrevet i denne Tillæg om databeskyttelse eller (3) som krævet ved lov. For så vidt angår formålene med dette afsnit, betyder "Behandlede data": (a) Kundedata, (b) Data fra Professionelle ydelser; (c) Personoplysninger og (d) eventuelle andre data, der behandles af Microsoft i forbindelse med Produkterne og Tjenesterne, og som er Kundens fortrolige oplysninger i henhold til volumenlicensaftalen. Al behandling af Behandlede data er underlagt Microsofts fortrolighedsforpligtelse i henhold til volumenlicensaftalen."*

Videre følger det, at *"…Microsoft hverken videregiver eller giver adgang til Behandlede data til ordensmagten, medmindre det er påkrævet af lovgivningen. Hvis en politimyndighed kontakter Microsoft med et krav om udlevering af Behandlede data, vil Microsoft forsøge at få politimyndigheden til at udbede sig sådanne data direkte fra Kunden. Hvis vi er nødsaget til at videregive eller give adgang til Behandlede data til ordensmagten, underretter Microsoft straks Kunden og sender en kopi af kravet, medmindre vi er juridisk forhindret i at gøre det.*

*Microsoft vil udelukkende videregive eller give adgang til Behandlede data som krævet ved lov, under forudsætning af at disse love og praksisser respekterer de grundlæggende rettigheder og friheder og ikke overskrider, hvad der er nødvendigt og passende i et demokratisk samfund, for at beskytte et af de formål, der fremgår af artikel 23, stk. 1 i GDPR. Ved modtagelse af en anmodning fra tredjemand om Behandlede data vil Microsoft straks meddele Kunden dette, medmindre vi er juridisk forhindret i at gøre det. Microsoft afviser anmodningen, medmindre imødekommelse heraf er påkrævet af lovgivningen. Hvis anmodningen er gyldig, forsøger Microsoft at omdirigere tredjemanden til at anmode om dataene direkte fra Kunden. Microsoft vil ikke levere følgende til tredjemand: (a) direkte, indirekte eller fri adgang til Behandlede data, (b) platformskrypteringsnøgler til beskyttelse af Behandlede data eller mulighed for at bryde en sådan kryptering eller (c) adgang til Behandlede data, hvis Microsoft ved, at dataene skal bruges til andre formål end angivet i anmodningen fra tredjemand."*

Som tilfældet er i databehandleraftalen med AWS er der ikke med ovenstående formuleringer henvist til en konkret lovgivning og/eller specifikke myndighedsanmodninger, hvorfor det er databehandleren opfattelse, at der også her er tale om et generelt forbehold, der ikke finder anvendelse i aftaleforholdet mellem databehandleren og Microsoft, idet databehandleren som nævnt ovenfor har valgt, at al databehandling foregår i Holland. Parterne har således eksplicit valgt, at Microsoft alene må behandle databehandlerens personoplysninger inden for EU, hvormed EU-lovgivningen, herunder databeskyttelsesforordningen, finder anvendelse.

<u>Microsofts yderligere tiltag for at overholde europæisk lovgivning</u>
Det skal nævnes, at Microsoft har iværksat tiltag i forhold til at sikre deres europæiske kunders overholdelse af den europæiske GDPR-lovgivning. Således har Microsoft i Appendiks C til Tillæg til databeskyttelse tilføjet en række yderligere sikkerhedsforanstaltninger vedrørende Microsofts beskyttelse af behandling af deres kunders personoplysninger.

Det fremgår bl.a. af Appendiks C, at

*"Microsoft accepterer og indestår for, at der ikke er nogen grund til at tro, at den lovgivning, der gælder for Microsoft eller Microsofts underbehandlere, herunder i ethvert land, hvor data overføres af sig selv eller via en underbehandler, forhindrer Microsoft i at opfylde de anvisninger, der er modtaget fra Kunden og dennes forpligtelser i henhold til dette Tillæg eller Standardkontraktbestemmelserne fra 2021, og at Microsoft i tilfælde af en ændring i denne lovgivning, der formentlig vil have en væsentlig negativ indvirkning på de garantier og forpligtelser, der er givet i henhold til dette Tillæg eller Standardkontraktbestemmelserne, straks vil give Kunden besked om dette, så snart Microsoft bliver bekendt med dette, i hvilket tilfælde Kunden er berettiget til at suspendere overførslen af data og/eller bringe kontrakten til ophør."*

Det er således vigtigt at bemærke, at Microsoft med ovenstående garanterer, at gældende lovgivning – ifølge Microsoft- ikke forhindrer Microsoft i at opfylde anvisninger modtaget fra Kunden, hvilket må læses som den af kunden dikterede instruks. Såfremt billedet måtte ændre sig som følge af lovændringer mv. med den konsekvens, at Microsoft ikke kan leve op til sine garantier overfor sine kunder, anerkender Microsoft, at kunden kan suspendere og/eller ophæve kontraktforholdet med Microsoft.

Utilsigtet overførsel af databehandlerens personoplysninger

På baggrund af ovenstående indebærer Microsofts egne formuleringer i Tillæg til databeskyttelse samt yderligere foranstaltninger i Appendiks C, at Microsoft anerkender, at det vil være at handle udenfor databehandlerens instruks (og dermed en misligholdelse af aftaleforholdet), såfremt Microsoft i forbindelse med en myndighedsanmodning eller lign. overfører databehandlerens personoplysninger til jurisdiktioner udenfor EU. I givet fald vil der være tale om en utilsigtet overførsel af databehandlerens personoplysninger, hvormed Microsoft bliver selvstændig ansvarlig for den konkrete overførsel. Der henvises i den forbindelse til afsnittet *"Utilsigtet overførsel af databehandlerens personoplysninger"* under II, punkt 2.2 ovenfor.

Også her skal det nævnes, at databehandleren til dato aldrig er blevet mødt med en myndighedsanmodning fra Microsoft.

Registreredes krav på erstatning

På samme vis som i databehandleraftalen med AWS indeholder Appendiks C en bestemmelse om skadesløsholdelse af de registrerede hvorefter

*"I henhold til afsnit 3 og 4 skal Microsoft skadesløsholde en registreret i forhold til alle væsentlige og ikke-væsentlige skader, som den registrerede har pådraget sig, og som skyldes Microsofts videregivelse af den registreredes personoplysninger, der er blevet overført som svar på en anmodning fra en offentlig myndighed, der ikke er fra EU/EØS, eller en politimyndighed i modstrid med Microsofts forpligtelser i henhold til Kapital V i GDPR (en "Relevant videregivelse").*

Ovenstående formuleringer vidner således om, at Microsoft anerkender at være erstatningsansvarlig overfor de registrerede, såfremt Microsoft handler i strid med databeskyttelsesforordningens kapital V, der omhandler overførsler af

personoplysninger til tredjelande eller internationale organisationer. Vigtigt i denne sammenhæng er det at understrege, at Microsoft udtaler, at i de tilfælde Microsoft ikke kan overholde sine forpligtelser i henhold til EU-lovgivningen, er de registrerede berettigede til at rejse et erstatningskrav overfor Microsoft, såfremt disse måtte have lidt et tab.

### 2.3 Indskærpelse af databehandlerens instruks overfor Microsoft

Set i lyset af den seneste tids drøftelser om brug af cloud leverandører og foranlediget af den usikkerhed, der er opstået på baggrund af Datatilsynets udtalelse af 29. marts 2022 i KOMBIT-sagen vedrørende tilsigtede eller utilsigtede overførsler i forbindelse med udlevering af personoplysninger til myndigheder i tredjelande, har databehandleren valgt at følge op overfor Microsoft den 10. november 2022 med en skriftlig indskærpelse af databehandlerens instruks overfor Microsoft om, at Microsoft i overensstemmelse med den indgåede databehandleraftale alene må behandle personoplysningerne indenfor EU.

## IV Databehandlerens tilsyn med AWS og Microsoft

Til orientering skal det oplyses, at databehandleren løbende fører tilsyn med sine underdatabehandlere, herunder AWS og Microsoft, og der gennemføres hvert år revision i form af en ISAE 3000 revisionserklæring.

I relation til den ovenfor skitserede problemstilling og generelt i forhold til brug af ovennævnte cloud leverandører følger databehandleren tæt gældende lovgivning og praksis på området, herunder udtalelser fra såvel de danske og europæiske myndigheder.

Databehandleren orienterer sig løbende på Datatilsynets hjemmeside omkring processen i forhold til indgåelse af en juridisk aftale mellem EU-Kommissionen og USA på baggrund af principaftalen om transatlantiske overførsler af personoplysninger, som blev indgået i marts 2022 samt det af Joe Biden udstedte præsidentielle dekret af den 7. oktober 2022 om udveksling af personoplysninger mellem USA og EU. Som det fremgår af Datatilsynets hjemmeside, skal EU-Kommissionen efter en særlig procedure, der også indbefatter høring af Det Europæiske Databeskyttelsesråd, afgøre, om der kan laves en tilstrækkelighedsvurdering, hvorefter indsamlingen af personoplysninger skal være proportional og begrænset til det strengt nødvendige. Endvidere skal det sikres, at de EU-borgere, der får behandlet deres personoplysninger af de amerikanske myndigheder, skal have adgang til at få prøvet deres sag ved en uafhængig klageinstans. Den endelige juridiske aftale mellem EU og USA forventes at foreligge i løbet af første halvår 2023. Det bemærkes at EU-Kommissionen har anført, at dekretet efter Kommissionens opfattelse tager hensyn til de betænkeligheder EU-Domstolen rejste i Schrems II-dommen. Derudover forventes klageinstansen allerede at træde i kraft i december 2022, og EU forventes at blive udpeget til at kunne gennemgå klager vedr. USA's overvågningsaktiviteter. Herefter vil det være muligt at overføre personoplysninger fra EU til virksomheder i USA, som har tilsluttet sig ordningen, uden at skulle iværksætte supplerende foranstaltninger.

***