

## Databehandlersaftale

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

mellem

Kunden

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

**Indholdsfortegnelse**

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| 2. Præambel .....                                                       | 3  |
| 3. Den dataansvarliges rettigheder og forpligtelser .....               | 3  |
| 4. Databehandleren handler efter instruks .....                         | 4  |
| 5. Fortrolighed .....                                                   | 4  |
| 6. Behandlingssikkerhed .....                                           | 4  |
| 7. Anvendelse af underdatabehandlere .....                              | 5  |
| 8. Overførsel til tredjelande eller internationale organisationer ..... | 6  |
| 9. Bistand til den dataansvarlige .....                                 | 7  |
| 10. Underretning om brud på persondatasikkerheden .....                 | 8  |
| 11. Sletning og returnering af oplysninger .....                        | 9  |
| 12. Revision, herunder inspektion .....                                 | 9  |
| 13. Parternes aftale om andre forhold .....                             | 9  |
| 14. Ikrafttræden og ophør .....                                         | 9  |
| 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 .....       | 17 |
| Bilag D Parternes regulering af andre forhold .....                     | 26 |
| Bilag E Oversigt over kæde af databehandlere .....                      | 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 levering og drift af digitale læremidler via databehandlerens platform, jf. den til enhver tid gældende skriftlige aftale mellem den dataansvarlige og databehandleren, herunder de(n) ordrebekræftelse(r), vilkår og betingelser fremsendt af databehandleren samt tilkøb af digitale læremidler (herefter "Aftalen"), 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 præliminært har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bilag E indeholder en beskrivelse af databehandlerkæden
11. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
12. 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<sup>1</sup> 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, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder,

---

<sup>1</sup> Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS-medlemsstater".

gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et passende beskyttelsesniveau.

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

- a. pseudonymisering og kryptering af personoplysninger
  - b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
  - c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
  - d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
  3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

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

## 7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst

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. Underdatabehandlersaftale(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 underdatabehandlersaftalen, skal ikke sendes til den dataansvarlige.
6. Databehandleren skal i sin aftale med underdatabehandleren, hvis muligt, indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

## **8. Overførsel til tredjelande eller internationale organisationer**

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal

databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
  - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
  - b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
  - c. behandle personoplysningerne i et tredjeland
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

## 9. Bistand til den dataansvarlige

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

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
  - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
  - c. indsigtsretten
  - d. retten til berigtigelse
  - e. retten til sletning ("retten til at blive glemt")
  - f. retten til begrænsning af behandling
  - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
  - h. retten til dataportabilitet
  - i. retten til indsigelse
  - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

- a. den dataansvarliges forpligtelse til uden 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, 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, hvorved 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 om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
  - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
  - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
  - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.



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

## **11. Sletning og returnering af oplysninger**

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

## **12. Revision, herunder inspektion**

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende 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 ved indgåelse af Aftalen og accept af Databehandlerens handelsbetingelser.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre

bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

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

5. Underskrift

Databehandleraftalen er accepteret af Kunden ved indgåelse af Aftalen og accept af Databehandlerens handelsbetingelser.



På vegne af databehandleren

Dato

Navn

Kim Bjørn Tiedemann

Stilling

Direktør for teknologi og udvikling

Telefonnummer

+45 26 80 50 89

E-mail

Databehandling@lrforlag.dk

## 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.

Kontaktperson hos den dataansvarlige:

Navn:  
Stilling:  
Telefonnummer:  
E-mail:

Kontakt hos den dataansvarlige ved sikkerhedsbrud jf. afsnit 10:  
E-mail:

Kontaktperson hos databehandleren:

|                |                            |
|----------------|----------------------------|
| 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 behandlingen er at levere de tjenester, som den dataansvarlige har købt/licenseret af databehandleren.

Formålet med behandling af personoplysninger er at give adgang til databehandlerens digitale læremidler. 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.

Databehandleren behandler 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 anonymiseret brugsdata til brug for rapportering til den dataansvarlige samt til statistiske formål, med henblik på at analysere brugen af de digitale læremidler og for løbende at sikre, at de digitale læremidler skaber optimalt læringsudbytte, er brugervenlige og lette at navigere i.

### 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//anonymisering

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

| PERSON-OPLYSNINGER                             | Ansatte på institution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Elever på institution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Almindelige personoplysninger: (art. 6)</b> | <ul style="list-style-type: none"> <li>• Uni login-brugernavn (bruger-id)</li> <li>• Navn</li> <li>• Ansættelsestype (lærer, tap, pæd eller gæst)</li> <li>• Initialer</li> <li>• Stilling</li> <li>• Grupper medarbejderen er tilknyttet, herunder gruppe-id, gruppenavn, gruppetype, niveau, spor, startdato og slutdato</li> <li>•</li> </ul> <p>Ved brugen af de digitale læremidler behandles desuden:</p> <ul style="list-style-type: none"> <li>• Loginoplysninger,</li> <li>• Pseudonymiseret bruger-id,</li> <li>• IP-adresse,</li> <li>• forbrugsdata,</li> <li>• brugernes anvendelse af databehandlerens digitale læremidler (klik, tidsforbrug mv.), herunder besvarelse af opgaver, bedømmelse af opgaver og egen-evaluering af opgaveløsning.</li> </ul> <p>I forbindelse med levering af support behandles følgende:</p> <ul style="list-style-type: none"> <li>• Navn</li> <li>• E-mail (arbejdsmail)</li> <li>• Telefonnummer (arbejdstelefon)</li> <li>• Support tickets</li> </ul> | <ul style="list-style-type: none"> <li>• Uni login-brugernavn (bruger-id)</li> <li>• Navn</li> <li>• Studietype (elev/studerende)</li> <li>• Studienummer</li> <li>• Elevens niveau (for grundskoleelever)</li> <li>• Elevens hovedgruppe (klasse)</li> <li>• Yderligere grupper elever er tilknyttet, herunder</li> <li>• Oplysninger om grupper, herunder gruppe-id, gruppenavn, gruppetype, niveau, spor, startdato og slutdato</li> </ul> <p>Ved brugen af de digitale læremidler behandles desuden:</p> <ul style="list-style-type: none"> <li>• Loginoplysninger,</li> <li>• Pseudonymiseret bruger-id,</li> <li>• IP-adresse,</li> <li>• forbrugsdata,</li> <li>• brugernes anvendelse af databehandlerens digitale læremidler (klik, tidsforbrug mv.), herunder besvarelse af opgaver, bedømmelse af opgaver og egen-evaluering af opgaveløsning.</li> </ul> |

|                                               |                                                           |                                                           |
|-----------------------------------------------|-----------------------------------------------------------|-----------------------------------------------------------|
| <b>Følsomme personoplysninger: (art. 9)</b>   | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> |
| <b>Straffedomme og lovovertrædelser (§10)</b> | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> |
| <b>CPR-nummer (§11)</b>                       | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> |
| <b>Andre fortrolige personoplysninger</b>     | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> | <ul style="list-style-type: none"> <li>• Ingen</li> </ul> |

#### 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 Bestemmelser i krafttræden. Behandlingen har følgende varighed:

Så længe databehandleren er i besiddelse af den dataansvarliges data.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af parterne.

## Bilag B Underdatabehandlere

### B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

| VIRKSOMHEDENS NAVN OG ADRESSE SAMT CVR ELLER ANDET VIRKSOMHEDS ID                                                                                | BESKRIVELSE AF BRUGEN AF UNDERDATABEHANDLERENS TJENESTER                                                                                                            | LOKALITET FOR BEHANDLING SAMT EVENTUELT OVERFØRSELSGRUNDLAG                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Microsoft Ireland Operations, Ltd. *</b><br>One Microsoft Place<br>South County Business Park<br>Leopardstown<br>Dublin 18, D18 P521, Ireland | System: Digitale læremidler.<br><br>Behandling: Hosting af digitale læremidler, herunder vedligehold af servere, backup, sikkerhed mv.                              | EU/EØS/USA.<br><br>Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF                                                      |
| <b>Egmont Administration A/S (Egmont IT)</b><br>Vognmagergade 11, 1148 København K<br>CVR: 84853518                                              | System: Digitale læremidler.<br><br>Behandling: Drift af løsninger på Microsoft Azure og, herunder administration af miljøer, overvågning, brugeradministration mv. | EU/EØS.                                                                                                                                       |
| <b>HubSpot</b><br>One Dockland Central, Guild Street, Dublin 1, Co. Dublin, Ireland                                                              | System: Kundesupport på alle digitale læremidler.<br><br>Behandling: Sagsstyringssystem til håndtering af kundenhenvelser.                                          | EU/EØS/USA<br>Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF                                                           |
| <b>Aircall</b><br>11 Rue Saint-Georges, 75009 Paris, France                                                                                      | System: Telefonisystem<br>Behandling: Håndtering af telefoni i forbindelse med kundenhenvelser. Der behandles telefonnummer på brugeren som ringer til support.     | EU/EØS/USA<br><br>Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF; EU-Kommissionens standardkontraktbestemmelser (SCC). |

\* Microsoft Ireland Operations er medtaget i ovenstående, da Lindhardt og Ringhof fører selvstændigt tilsyn med underdatabehandleren selvom aftalepartneren er Egmont IT.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden at følge den aftalte procedure for udskiftning af underdatabehandlere – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

## **B.2. Varsel for indsigelse ved skift af underdatabehandlere**

Den dataansvarlige kan gøre indsigelse mod tilføjelse af eller udskiftning af en underdatabehandler.

Den dataansvarliges eventuelle indsigelse skal meddeles ved skriftlig henvendelse til databehandleren. Modtager databehandleren ikke en skriftlig indsigelse inden 30 dage efter, at databehandleren har oplyst om en planlagt ændring af de angivne underdatabehandlere, anses ændringerne for godkendt af den dataansvarlige.

Modtager databehandleren en skriftlig indsigelse fra den dataansvarlige inden for 30 dage, og er indsigelsen konkret og sagligt begrundet, skal databehandleren tage indsigelsen til efterretning.

Hvis den dataansvarlige ikke kan acceptere en underdatabehandler, uden en konkret og saglig begrundelse bringes de(n) tjeneste(r), for hvilken underdatabehandleren deltager i behandlingsaktiviteter til ophør. Ophør af tjenesterne sker overensstemmelse med 14.4 i disse bestemmelser og de øvrige vilkår i Aftalen.



## Bilag C Instruks vedrørende behandling af personoplysninger

### C.1. Behandlingens genstand/instruks

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

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

#### Sikkerhedsniveau:

Sikkerhedsniveauet skal afspejle behandlingens karakter, omfang. På baggrund af de ovenfor angivne oplysninger om behandlingen, og under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål, samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder etableres følgende sikkerhedsniveau:

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". 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.

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.

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

### **C.2.1 Krav til pseudonymisering og kryptering af personoplysninger**

#### Krav til pseudonymisering af personoplysninger

Databehandler foretager pseudonymisering af personoplysninger, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det.

#### Krav til kryptering af personoplysninger

Databehandler foretager kryptering af personoplysninger, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det.

Databehandleren sikrer, at den kryptering der anvendes, er korrekt sat op og tilstrækkelig til sikring af de behandlede personoplysningers fortrolighed og integritet.

Der anvendes altid kryptering af personoplysninger ved enhver transmission af fortrolige og følsomme personoplysninger via eksterne kommunikationsforbindelser.

### **C.2.2 Krav vedrørende evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester**

1. Databehandler foretager mindst én gang årligt en risikovurdering for hver af de behandlingssystemer og tjenester, hvori den Dataansvarliges personoplysninger behandles. Databehandler foretager loyalt og professionelt mitigerende foranstaltninger baseret på risikovurderingens resultater.
2. Databehandler foretager løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet.

Databehandler sikrer endvidere, at:

1. Adgang til de personoplysninger, som aftalen vedrører, er begrænset til personer, der har et sagligt formål.
2. Der er tekniske og/eller organisatoriske foranstaltninger, som sikrer, at alene disse autoriserede personer, har adgang. Autorisationen omfatter også personer, som udfører konsulentopgaver eller nødvendige revisions- drifts- og systemtekniske opgaver.
3. Der skal løbende foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have.
4. Ansatte og eventuelle samarbejdspartnere skal til stadighed være bekendt med og have tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejds-gange og om deres tavshedspligt.

### **C.2.3. Krav vedrørende evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse**

Databehandler sikrer, at

1. Databehandleren skal have opdaterede og effektive beredskabsplaner og -procedurer, der sikrer genetablering af personoplysninger og adgange inden for rimelig tid i tilfælde af driftsafbrydelser.
2. Databehandleren skal sikre, at der foretages regelmæssig backup af personoplysninger, der er omfattet af aftalen.
3. Databehandleren skal regelmæssigt afprøve og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser. Den Dataansvarlige kan anmode om at få dokumentation for gennemførelsen stillet til rådighed.

#### **C.2.4. Krav vedrørende procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden**

Der skal foreligge procedurer, som sikrer, at der sker regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Databehandler har til enhver tid tidssvarende procedurer for gennemførelse af:

1. Regelmæssig kontrol, vurdering, tilpasning og forbedring af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren er underlagt efter den til enhver tid gældende lovgivning, retspraksis, Datatilsynets afgørelser, anbefalinger og retningslinjer samt vilkårene i nærværende databehandlersaftale.
2. Kontrol af, at sikkerhedsforanstaltningerne faktisk efterleves i forhold til den til enhver tid værende risiko for de registreredes rettigheder og frihedsrettigheder.
3. Kontrol af brugeradgang for medarbejdere eller andre autoriserede.
4. Kontrol af at backuppen er læsbar, skrivebeskyttet, har det rette omfang og kan reetableres.
5. Kontrol af at der sker korrekt kryptering, herunder at krypteringsnøglen opbevares sikkert.
6. Kontrol med at sikkerhedsloggene er tilstrækkelige og relevante.
7. Kontrol med at det fysiske sikkerhedsniveau er afstemt med det til enhver tid værende truselsbillede.
8. Databehandleren har formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.
9. For kritiske sikkerhedsopdateringer skal Databehandleren have procedurer, der sikrer, at disse kan gennemføres uden unødigt forsinkelse.
10. At der føres ekstraordinære kontroller ved større ændringer af systemteknisk set-up og efter brud på persondatabeskyttelsen.

#### **C.2.5. Krav vedrørende adgang til oplysninger via internettet**

Når personer hos Databehandleren tilgår systemer indeholdende personoplysninger over internettet, så skal autentifikationen af personen ske ved flerkfaktorautentificering. Der må kun oprettes forbindelse til personoplysninger omfattet af disse bestemmelser igennem sikre krypterede forbindelser.

#### **C.2.6. Krav vedrørende beskyttelse af oplysninger under transmission**

Der skal anvendes tilstrækkelige sikkerhedsforanstaltninger i forbindelse med transmission af personoplysninger. Sikkerhedsforanstaltningerne skal leve op til de til enhver tid anerkendte og gældende branchestandarder for behandling af personoplysninger.

Databehandler sikrer i denne forbindelse, at personoplysninger er krypteret i forbindelse med transmissionen. Krypteringen skal løbende holdes opdateret, og følge den til enhver tid anerkendte og gældende branchestandard.

#### **C.2.7. Krav vedrørende beskyttelse af oplysninger under opbevaring**

Under opbevaring af personoplysninger skal der etableres tilstrækkelige sikkerhedsforanstaltninger under hensyntagen til karakteren af de behandlede personoplysninger, og risikoen for de registreredes rettigheder.

Databehandler sikrer, at personoplysningerne er krypteret under opbevaring. Krypteringen skal løbende holdes opdateret, og følge den til enhver tid værende anerkendte og gældende branchestandard.

#### **C.2.8. Krav vedrørende fysisk sikring af lokaliteter, hvor der behandles oplysninger**

Databehandler sikrer, at der er passende sikkerhedsforanstaltninger mod enhver uautoriseret adgang til lokationer, hvor den Dataansvarliges data behandles.

Sikkerhedsforanstaltninger skal være afstemt med det aktuelle trusselsbillede samt den følsomhed og mængde af personoplysninger, som Databehandler behandler for den Dataansvarlige.

Behandlingen foregår fra lokationer, som er beskyttet mod skader forårsaget af fysiske forhold som f.eks., - men ikke begrænset til - brand, overophedning, vandskade, magnetisme, forsyningssvigt, tyveri eller hærværk.

Databehandleren skal sikre, at alt anvendt udstyr, der anvendes i forbindelse med behandlingen af personoplysninger, er underlagt passende tekniske foranstaltninger.

#### **C.2.9. Krav vedrørende anvendelse af hjemme-/fjernarbejdspladser**

Hjemme-/fjernarbejdspladser skal være sikret med tekniske kontroller, der sikrer, at behandlingen af personoplysninger sker i overensstemmelse med gældende lovgivning og den Dataansvarliges og Databehandlerens retningslinjer.

Det skal sikres, at uvedkommende ikke får adgang til personoplysninger, der behandles ved hjemme-arbejdspladser, ligesom de enkelte medarbejdere skal instrueres i, hvordan uvedkommende ikke får adgang.

Databehandler sikrer, at der anvendes kryptering af kommunikationsforbindelser. Fjernadgange skal være sikret af en VPN-løsning eller anden sikkerhedsteknologi, så det kun er autoriserede personer, som kan få adgang til personoplysninger.

Autentifikation af personer hos Databehandleren der får adgang til personoplysninger, benytter multifaktorautentifikation.

#### **C.2.10. Krav vedrørende logning**

Der skal foretages maskinel registrering (logning) ved al behandling af personoplysninger.

Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium.

Loggen skal opbevares i tolv måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

Databehandleren fører løbende kontrol med, at loggen indeholder de nødvendige oplysninger, som fremgår af disse bestemmelser.

Databehandleren skal ved mistanke om misbrug eller brud på persondatasikkerheden vederlagsfrit udlevere en log over brugeraktivitet. Databehandleren skal sikre, at loggen er forståelig og indeholder de relevante aktiviteter.

### **C.2.11. Øvrige foranstaltninger**

#### Opdateringer og ændringer

Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.

#### Awareness / kendskab til informationssikkerhed

Ansatte og eventuelle samarbejdspartnere, som har adgang til personoplysninger omfattet af disse Bestemmelser, skal gennemgå regelmæssig uddannelse vedrørende behandling af personoplysninger, som sikrer et vedvarende kendskab til databeskyttelsesreglerne, samt procedurer for behandlingen af personoplysninger

#### Mobile lagringsmedier:

Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares med tilstrækkelig stærk kryptering under opsyn eller under lås, når de ikke benyttes.

Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.

Der skal føres en fortegnelse over, hvilke mobile lagringsmedier der benyttes i forbindelse med databehandlingen.

Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af mobile lagringsmedier.

#### Reparation, service og kassation af udstyr:

I forbindelse med reparation og service af udstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at

personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov.

Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller renses, så der sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal opbevares i den periode, databehandlingen foregår og forevises, på den Dataansvarliges anmodning.

Databehandlerens sikkerhedsforanstaltninger er ikke begrænset til det, der er fastsat i ovenstående beskrivelse og skal om nødvendigt, tilpasses løbende med henblik på at sikre et passende sikkerhedsniveau i forhold til risikoen.

Databehandleren orienterer den dataansvarlige hvis sikkerhedsforanstaltninger ændres væsentligt.

### **C.3 Bistand til den dataansvarlige**

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren vederlægges for bistand til den dataansvarlige i overensstemmelse med Hovedaftalen.

#### Underretning af den dataansvarlige om anmodninger fra de registrerede

Databehandleren skal uden unødigt forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes databehandlere 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 på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

#### Bistand ved sikkerhedsbrud, herunder underretning af den dataansvarlige om sikkerhedsbrud

Databehandlerens bistand i forbindelse med den dataansvarliges forpligtelser efter databeskyttelsesforordningens artikel 33 og 34 sker ved, at databehandleren indgiver de oplysninger, der følger af Bestemmelse 10.3, til den dataansvarlige inden for den frist, der følger af Bestemmelse 10.2. Databehandleren skal efterfølgende bistå den dataansvarlige ved på den dataansvarliges anmodning at stille de oplysninger til rådighed, som er nødvendige for, at den dataansvarlige kan foretage anmeldelse af brud på persondatasikkerheden til den kompetente tilsynsmyndighed eller som er nødvendige for, at den dataansvarlige kan underrette den registrerede herom.

#### Bistand i forbindelse med risikovurderinger og konsekvensanalyser

Databehandleren skal bistå den dataansvarlige ved at stille de nødvendige oplysninger til rådighed, så den dataansvarlige kan gennemføre de nødvendige risikovurderinger. Såfremt den dataansvarlige vurderer, at behandlingen sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder, skal databehandleren på anmodning fra den dataansvarlige bistå den dataansvarlige i forbindelse med dennes forpligtelser efter databeskyttelsesforordningens artikel 35 og 36 ved at indgive de oplysninger til den dataansvarlige, der er nødvendige for, at den dataansvarlige kan foretage en konsekvensanalyse i overensstemmelse med artikel 35 og foretage en forudgående høring af den kompetente tilsynsmyndighed i overensstemmelse med artikel 36.

#### Sikring af tekniske og organisatoriske foranstaltninger

Databehandleren skal endelig sikre, at dennes tekniske og organisatoriske foranstaltninger gør det muligt for den dataansvarlige at overholde sine forpligtelser efter databeskyttelsesforordningens artikel 33-36, herunder f.eks. gennem de foranstaltninger vedrørende styring af sikkerhedsbrud, styring af aktiver, logning mv., der følger af bilag C.

#### **C.4 Opbevaringsperiode/sletterutine**

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

Ved ophør af tjenesten eller disse Bestemmelser vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

Personoplysninger opbevares i 6 måneder efter eleven har forladt grundskolen (0-10 klasse, generelt) hvorefter de slettes hos databehandleren. Personale slettes 6 måneder efter de har forladt en institution. En bekræftelse af sletning fremsendes til den dataansvarlige efter anmodning.

Der kan læses mere om databehandlerens løbende sletning og retention perioder på Alineas side om sikkerhedsforanstaltninger: <https://www.alinea.dk/lr-sikkerhedsforanstaltninger>

#### **C.5 Lokaltet for behandling**

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

| Virksomhedens navn og adresse                                                                                                                     | CVR eller andet virksomheds ID | Lokalitet for behandling | Eventuelt overførselsgrundlag                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------|-----------------------------------------------------------------------|
| <b>Microsoft Ireland Operations, Ltd.</b><br>One Microsoft Place<br>South County Business Park<br>Leopardstown<br>Dublin 18, D18 P521,<br>Ireland |                                | EU/EØS/USA.              | Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF |
| <b>Egmont Administration A/S (Egmont IT)</b><br>Vognmagergade 11,<br>1148 København K<br>CVR: 84853518                                            | CVR: 84853518                  | EU/EØS.                  | N/A                                                                   |

|                                                                                     |  |               |                                                                                                                             |
|-------------------------------------------------------------------------------------|--|---------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>HubSpot</b><br>One Dockland Central, Guild Street, Dublin 1, Co. Dublin, Ireland |  | EU/EØS/USA    | Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF                                                       |
| <b>Aircall</b><br>11 Rue Saint-Georges, 75009 Paris, France                         |  | EU/EØS<br>USA | Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF; EU-Kommissionens standardkontraktbestemmelser (SCC). |

### C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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

Den dataansvarlige giver ved indgåelsen af denne aftale skriftlig instruks til databehandleren i at overføre personoplysninger til tredjelande i forbindelsen med tilføjelser af underdatabehandlere i det omfang, dette er nødvendigt for leveringen af tjenesterne. Ved overførsel af personoplysninger til tredjelande er databehandleren ansvarlig for, at der foreligger et gyldigt overførselsgrundlag.

Gyldigt overførselsgrundlag for overførslerne er navnlig:

1. En afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henholdt databeskyttelsesforordningens artikel 45 eller
2. EU-Kommissionens standardkontraktbestemmelser i henhold til databeskyttelsesforordningens artikel 46, når databehandleren samtidig vurderer – og i nødvendigt omfang implementerer supplerende foranstaltninger med henblik på at sikre – den pågældende overførsels lovlighed

Databehandleren skal underrette den Dataansvarlige om enhver henvendelse, som Databehandleren eller dennes underdatabehandlere modtager fra en myndighed i et tredjeland om videregivelse af personoplysninger omfattet af disse Bestemmelser.

Såfremt Databehandleren, direkte eller indirekte, modtager en anmodning om at udlevere oplysninger omfattet af disse Bestemmelser, herunder personoplysninger, til en modtager, der geografisk er placeret uden for EU/EØS, er Databehandleren til enhver tid forpligtet til at modsætte sig en sådan anmodning om udlevering, så vidt det er muligt for Databehandleren i henhold til EU-ret eller medlemsstaternes nationale ret.

Databehandleren skal, eventuelt i fællesskab med den pågældende underdatabehandler, udtømme enhver mulighed for at påklage anmodninger om videregivelse af personoplysninger omfattet af disse Bestemmelser, hvis der er tale om generelle anmodninger eller anmodninger, der ikke er i overensstemmelse med EU-retten, herunder databeskyttelsesforordningen, samt øvrig national lovgivning, som supplerer databeskyttelsesforordningen. Databehandleren skal, i det omfang det er muligt, give den Dataansvarlige mulighed for at indtræde i klage- og retssager, med henblik på at give den Dataansvarlige mulighed for at varetage sine egne interesser.



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

Databehandleren vil én gang årligt enten fremsende eller på sin hjemmeside fremlægge en erklæring om overholdelse af denne aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder. Databehandleren tilstræber i april måned at offentliggøre erklæring for den senest afsluttede erklæringsperiode.

Den dataansvarlige kan gennemføre revision, inspektion eller tilsyn hos databehandleren, når den dataansvarlige finder det nødvendigt og i det omfang, at det ønskede emne for inspektionen eller tilsynet ikke allerede er adresseret i erklæringen nævnt ovenfor.

**C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere**

Databehandleren fører tilsyn med underdatabehandlere. Databehandleren fører tilsyn med underdatabehandlere i form af vurderinger af revisionserklæringer, fysiske besigtigelser eller skrivebordstilsyn. Valget af tilsynsform er baseret på karakteren af underdatabehandleren og den overladte behandling af personoplysninger.

## **Bilag D      Parternes regulering af andre forhold**

### **D.1 Databehandlerkæden**

Databehandleren skal identificere – og kortlægge – underdatabehandlere, som behandler personoplysninger på vegne af databehandleren samt disses underdatabehandlere. Denne kortlægning skal ikke omfatte underdatabehandlere, som databehandleren – ud fra tekniske, organisatoriske og kontraktuelle foranstaltninger – kan sandsynliggøre ikke behandler den dataansvarliges personoplysninger.

## Bilag E Oversigt over kæde af databehandlere

E.1 Databehandlerens kortlægning af underdatabehandlere er illustreret i diagrammet nedenfor.

