



## Changelog

VERSION	ÆNDRINGER
1.1	Implementeret den 31. juli 2023 som erstatning for den hidtil brugte databehandleraftale. Der er valgt standardaftalen fra Det Europæiske Databeskyttelsesråd, da FrontRead opererer i flere lande i EU



## Standardkontraktbestemmelser

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

mellem

[NAVN]

CVR [CVR-NR]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

herefter "den dataansvarlige"

og

FrontRead ApS

CVR 25663497

Aabogade 15

8200 Aarhus N

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



<b>1. Indhold</b>	
2. Præambel .....	4
3. Den dataansvarliges rettigheder og forpligtelser .....	4
4. Databehandleren handler efter instruks .....	5
5. Fortrolighed .....	5
6. Behandlingsikkerhed .....	5
7. Anvendelse af underdatabehandlere.....	6
8. Overførsel til tredjelande eller internationale organisationer .....	7
9. Bistand til den dataansvarlige.....	7
10. Underretning om brud på persondatasikkerheden .....	9
11. Sletning og returnering af oplysninger .....	9
12. Revision, herunder inspektion .....	9
13. Parternes aftale om andre forhold .....	10
14. Ikrafttræden og ophør.....	10
15. Kontaktpersoner hos den dataansvarlige og databehandleren .....	11
Bilag A Oplysninger om behandlingen .....	12
Bilag B Underdatabehandlere .....	13
Bilag C Instruks vedrørende behandling af personoplysninger.....	14
Bilag D Parternes regulering af andre forhold.....	17



## 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 FrontRead læsetræningsplatform behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

## 3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes<sup>1</sup> nationale ret og disse Bestemmelser.

---

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



2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

#### 4. Databehandleren handler efter instruks

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

#### 5. Fortrolighed

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

#### 6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

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

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



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

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

## 7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående specifik skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 30 dage inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.



Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

## 8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
  - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
  - b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
  - c. behandle personoplysningerne i et tredjeland
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

## 9. Bistand til den dataansvarlige



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

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
  - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
  - c. indsigtretten
  - d. retten til berigtigelse
  - e. retten til sletning ("retten til at blive glemt")
  - f. retten til begrænsning af behandling
  - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
  - h. retten til dataportabilitet
  - i. retten til indsigelse
  - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren desuden, 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 analysere 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 nødvendige tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.





## 10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal 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.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

## 12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.



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

### 13. Parternes aftale om andre forhold

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

### 14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

Navn [NAVN]  
Stilling [STILLING]  
Telefonnummer [TELEFONNUMMER]  
E-mail [E-MAIL]  
Underskrift

På vegne af databehandleren

Navn Kim Høgskilde  
Stilling Administrerende direktør  
Telefonnummer 2999 4502  
E-mail kah@frontread.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	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Navn	Kim Høgskilde
Stilling	Administrerende direktør
Telefonnummer	2999 4502
E-mail	kah@frontread.dk



## **Bilag A Oplysninger om behandlingen**

Behandling af personoplysninger sker i henhold til formålet i hovedaftalen om databehandlerens levering af et digitalt læringsmiddel til den dataansvarlige.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end den dataansvarlige.

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

Læringsmidler:

Formålet med behandlingen er at lade den dataansvarliges brugere benytte digitale læremidler i henhold til hovedaftalen og instruksen. Se C1 nedenfor.

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

Systemet indsamler og behandler persondata om den dataansvarliges (institutionens) lærere og elever for at kunne levere, beskytte og forbedre FrontReads læremidler. Med forbedring menes her alene forbedring af brugernes egne sider, så de er mest relevante for brugerne. Alle behandlingsaktiviteter, registreringer og beskrivelse af persondatabehandlingens karakter er udførligt præsenteret i bilag D og E nedenfor.

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

Der behandles følgende oplysninger:

Elever: Navn, UNI-login brugernavn, klasse, skole, øvelsesresultater.

Lærere: Navn, e-mailadresse, telefonnummer, UNI-login brugernavn, klasse, skole, øvelsesresultater.

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

Vi har følgende registrerede:

- Lærer
- Elever

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

Behandlingen er tidsbegrænset og varer indtil Hovedaftalen ophører, hvorefter databehandleren sletter personoplysningerne i overensstemmelse med vilkårene i hoveddokumentets punkt 11, medmindre den dataansvarlige forinden har instrueret databehandleren i at forlænge behandlingsperioden.

**Bilag B Underdatabehandlere****B.1. Godkendte underdatabehandlere**

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
SE Cloud Factory	35393692	Vestergade 4, 6800 Varde	SE Cloud Factory hoster FrontReads serverpark uden adgang til data

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

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

Databehandleren er forpligtet til at varsle som angivet i punkt 6.3.



## 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:

Den dataansvarlige instruerer hermed FrontRead om at foretage behandling af den dataansvarliges oplysninger til brug for levering af adgang til digitale læremidler på kommunens folkeskoler, herunder adgang og holdoprettelse, så elever og lærere kan arbejde i FrontReads digitale læremidler med deres egne, unikke UNI-Login-baserede brugere. Endelig instrueres FrontRead til at foretage nødvendig support telefonisk og per mail for den dataansvarliges brugere.

Overlader databehandleren behandling af den dataansvarliges oplysninger til underdatabehandlere, er databehandleren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse. Databehandleren er ansvarlig for, at den dataansvarliges instruks fremsendes til eventuelle underdatabehandlere.

### C.2. Behandlingssikkerhed

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:

Databehandleren skal behandle personoplysningerne i overensstemmelse med nærværende Databehandleraftale og de bestemmelser i henholdsvis databeskyttelsesloven eller databeskyttelsesforordningen, der er gældende for databehandler. Derudover fremgår krav til databehandleren af hovedaftalen inkl. bilag.

Ansatte hos databehandleren, der er beskæftiget med behandling af personoplysninger under denne databehandleraftale, er underlagt tavshedspligt. Alene personale, som autoriseres hertil, må have adgang til de personoplysninger, der behandles under aftalen. Hvis det følger af hovedaftalen, at særlige sikkerhedsgodkendelser er påkrævet for personale, der er beskæftiget med behandling af den dataansvarlige personoplysninger, skal databehandleren sikre, at disse godkendelser tilvejebringes.

Databehandleren skal sikre, at dennes medarbejdere modtager tilstrækkelig uddannelse og instruktioner.

Databehandleren skal sikre restriktioner for adgang til områder, hvor der sker behandling af personoplysninger - hvad enten dette er manuelt eller elektronisk. Sådanne områder skal ved adgangskontrolmekanismer være adskilt fra områder, hvortil der er generel adgang. Adgangskontrolmekanismerne kan f.eks. omfatte systemer til fysisk adgangskontrol, låse, personsluser, sikkerhedspersonale og overvågningsudstyr.

Databehandleren skal sikre begrænsninger på adgangsrettigheder til personoplysninger og et system til adgangskontrol. Adgang til personoplysninger skal være begrænset til medarbejdere, og hvor det er relevant, andre leverandører, med et arbejdsbetinget behov og tildeles efter forudgående godkendelse fra databehandleren. Adgang skal tilbagekaldes, når en bruger ikke længere opfylder kriterierne for at have adgang. Databehandleren skal varetage autorisation for egne medarbejdere og i det omfang det er særskilt aftalt i hovedaftalen, for den dataansvarliges medarbejdere. Adgangsrettigheder skal gennemgås periodisk. Databehandleren



skal anvende passende logiske autentifikationsmekanismer, eksempelvis adgangskoder, biometri eller lignende. De anvendte autentifikationsmekanismer skal efterleve, hvad der kan opfattes som god skik på området (eksempelvis krav til adgangskoders længde og kompleksitet).

Databehandleren skal sikre passende tekniske foranstaltninger til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode i systemet. Sådanne foranstaltninger skal omfatte, firewalls, anti-virus software og malware-beskyttelse. Databehandleren skal have procedurer til sikring af, at sikkerhedssystemerne holdes opdaterede.

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

I det omfang det er et krav i medfør af gældende lovgivning eller i øvrigt er omfattet af hovedaftalen med den dataansvarlige, skal databehandleren anvende relevante krypteringsteknologier og andre tilsvarende foranstaltninger.

I det omfang at det følger af hovedaftalen, skal databehandleren foranstalte, at systemer og data sikkerhedskopieres, samt at sikkerhedskopier opbevares betryggende og i overensstemmelse med det i hovedaftalen anførte.

Databehandleren skal foretage logning af personoplysninger i overensstemmelse med det i hovedaftalen indeholdt. Den dataansvarlige er ansvarlig for selv at kontrollere egne medarbejders og samarbejdspartners adgang til og behandling af personoplysninger.

Databehandleren skal foretage registrering af afviste adgangsforsøg og blokering for yderligere forsøg efter et nærmere antal på hinanden følgende afviste adgangsforsøg, jf. hovedaftalen.

Databehandleren skal have processer for håndtering af brud på datasikkerheden og sikre, at der sker sletning af data inden udstyr, overgives til tredjepart eller i øvrigt bortskaffes.

Databehandleren er i øvrigt 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.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 skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de nødvendige sikkerhedsforanstaltninger til stadighed er iagttaget.

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

Personoplysninger opbevares i kontraktens løbetid og op til 5 år herefter, hvorefter de slettes hos databehandleren, medmindre den dataansvarlige forud herfor kræver sletning.



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

Databehandleren skal ligeledes sikre, at der løbende kan ske sletning, mens systemet anvendes. Persondata slettes automatisk i FrontRead når en elev forlader skolen, og databehandleren har meldt dette ind i de administrative systemer.

### **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:

Behandlingen finder sted hos FrontRead ApS, Aabogade 15, 8200 Aarhus N.

### **C.6 Instruks vedrørende overførsel af personoplysninger til tredjelände**

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

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

Databehandleren skal årligt fremsende en statusrapport til den dataansvarlige, der dækker alle de krav der er beskrevet i databehandleraftalen, og andre relevante områder (f.eks. organisatoriske eller produktmæssige ændringer).

Databehandleren afholder selv eventuelle udgifter, der måtte være forbundet med udarbejdelsen af statusrapport(er).

Databehandleren fremsender al relevant tilsynsmateriale til den dataansvarlige via kontaktpersonen, angivet i pkt. 15.

Første statusrapport skal sendes til den dataansvarlige senest 6 måneder efter indgåelse af databehandleraftalen.

Dækker statusrapporten ikke alle krav der er beskrevet i databehandleraftalen, kan den dataansvarlige eller en repræsentant for den dataansvarlige foretage skriftlig inspektion, f.eks. i form af spørgeskema, af databehandlerens behandling af personoplysninger, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Denne aftale.

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

Den dataansvarlige forbeholder sig retten til at eskalere sit tilsyn med databehandleren i overensstemmelse med tilsynskoncepter 4-6, hvis den dataansvarlige via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, evt. får indtryk af problemer hos databehandleren.

Hvis den dataansvarlige vælger at eskalere sin tilsynsform med databehandleren til et andet tilsynskoncept, efter tilsynskoncept 4-6, skal rammerne for tilsynet udarbejdes som et tillæg til den eksisterende databehandleraftale.





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

Databehandleren træffer som udgangspunkt valg om, hvordan revision af underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og underdatabehandleraftalen foretages, herunder hvilket format, der vælges, herunder for eksempel revisionserklæring, inspektionsrapport, tro- og loveerklæring og/eller besvarelse af spørgsmål. Typen og omfanget af revisionen skal afspejle karakteren af den behandling af personoplysninger, som underdatabehandleren foretager, og tilsynet med underdatabehandleren skal være i overensstemmelse med anbefalingerne fra Datatilsynet, jf. Datatilsynets 'Vejledning om tilsyn med databehandlere – Pointskala og seks tilsynskoncepter' fra oktober 2021.

Databehandleren skal sikre tilstrækkeligt tilsyn med underdatabehandlere.

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