

## Databehandlersaftale

Mellem

Den Dataansvarlige:

[Navn]

CVR [CVR-nummer]

[Adresse]

[Postnummer og by]

[Land]

og

Databehandleren

FrontRead ApS

CVR 25663497

Åbogade 15

8200 Aarhus N

Danmark

# 1 Indhold

2	Baggrund for Databehandleraftalen .....	4
3	Den Dataansvarliges forpligtelser og rettigheder .....	5
4	Databehandleren handler efter instruks.....	5
5	Fortrolighed.....	5
6	Behandlingssikkerhed.....	6
7	Anvendelse af Underdatabehandlere .....	6
8	Overførsel af oplysninger til tredjelande eller internationale organisationer .....	8
9	Bistand til den Dataansvarlige.....	8
10	Underretning om brud på persondatasikkerheden .....	9
11	Sletning og tilbagelevering af oplysninger .....	10
12	Tilsyn og revision .....	10
13	Parternes aftaler om andre forhold .....	11
14	Ikrafttræden og ophør.....	11
15	Kontaktpersoner/kontaktpunkter hos den Dataansvarlige og Databehandleren .....	12
Bilag A	Oplysninger om behandlingen .....	13
Bilag B	Betingelser for Databehandlerens brug af Underdatabehandlere og liste over godkendte Underdatabehandlere.....	14
B.1	Betingelser for Databehandlerens brug af eventuelle Underdatabehandlere .....	14
B.2	Godkendte Underdatabehandlere .....	14
Bilag C	Instruks vedrørende behandling af personoplysninger .....	16
C.1	Behandlingens genstand/ instruks.....	16
C.1.1	Behandlingens kategorisering.....	16
C.1.2	Behandlingens relevans .....	16
C.2	Behandlingssikkerhed .....	17
C.2.1	Inddatamateriale indeholdende persondata .....	17
C.2.2	Uddatamateriale indeholdende persondata.....	18
C.2.3	Fysisk sikring.....	18
C.2.4	Autorisation og adgangskontrol.....	19
C.2.5	Logning .....	19
C.2.6	Hjemmearbejdspladser .....	19
C.3	Opbevaringsperiode/sletterutine .....	19

C.4 Lokaltet for behandling .....	20
C.5 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelnde.....	20
C.5.1 virksomhed i udlandet.....	20
C.6 Nærmere procedurer for den Dataansvarliges tilsyn med den behandling, som foretages hos Databehandleren .....	21
C.7 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle Underdatabehandlere .....	21

## 2 Baggrund for Databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når Databehandleren foretager behandling af personoplysninger på vegne af den Dataansvarlige.
2. Aftalen 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)*, som stiller specifikke krav til indholdet af en Databehandleraftale.
3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes "hovedaftale": [Navn på hovedaftalen/ydelsen], som er indgået den [dato].
4. Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig Databehandleraftale.
5. Denne Databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "hovedaftalen".
6. Til denne aftale hører fire bilag. Bilagene fungerer som en integreret del af Databehandleraftalen.
7. Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
8. Databehandleraftalens Bilag B indeholder den Dataansvarliges betingelser for, at Databehandleren kan gøre brug af eventuelle Underdatabehandlere, samt en liste over de eventuelle Underdatabehandlere, som den Dataansvarlige har godkendt.
9. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling Databehandleren skal foretage på vegne af den Dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med Databehandleren og eventuelle Underdatabehandlere.
10. Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af Databehandleraftalen eller parternes "hovedaftale".
11. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

12. Denne Databehandleraftale frigør ikke Databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt Databehandleren.

### **3 Den Dataansvarliges forpligtelser og rettigheder**

1. Den Dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.
2. Den Dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.
3. Den Dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, 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; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

### **5 Fortrolighed**

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den Dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.
2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde Databehandlerens forpligtelser overfor den Dataansvarlige.
3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den Dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
4. Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

## 6 Behandlingsikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.
2. Ovenstående forpligtelse indebærer, at Databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:
  - 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
3. Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.
4. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den Dataansvarliges eller Databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes ”hovedaftale” eller af denne aftales Bilag D.

## 7 Anvendelse af Underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden Databehandler (Underdatabehandler).
2. Databehandleren må således ikke gøre brug af en anden Databehandler (Underdatabehandler) til opfyldelse af Databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den Dataansvarlige.
3. I tilfælde af generel skriftlig godkendelse skal Databehandleren underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre

Databehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

4. Den Dataansvarliges nærmere betingelser for Databehandlerens brug af eventuelle Underdatabehandlere fremgår af denne aftales Bilag B.
5. Den Dataansvarlige har ved indgåelse af denne aftale accepteret at Databehandleren anvender de under-Databehandlere der er anført i denne aftales Bilag B.
6. Når Databehandleren har den Dataansvarliges godkendelse til at gøre brug af en under-Databehandler, sørger Databehandleren for at pålægge under-Databehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne Databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at under-Databehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

Databehandleren er således ansvarlig for – igennem indgåelsen af en under-Databehandleraftale – at pålægge en eventuel under-Databehandler mindst de forpligtelser, som Databehandleren selv er underlagt efter databeskyttelsesreglerne og denne Databehandleraftale med tilhørende bilag.

7. Under-Databehandleraftalen 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 der er indgået en gyldig aftale mellem Databehandleren og under-Databehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af under-Databehandleraftalen, skal ikke sendes til den Dataansvarlige.
8. Databehandleren skal i sin aftale med Underdatabehandleren 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 Underdatabehandleren, f.eks. så den Dataansvarlige kan instruere Underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.
9. Hvis Underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af Underdatabehandlerens forpligtelser.

## **8 Overførsel af oplysninger til tredjelande eller internationale organisationer**

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Uden den Dataansvarliges instruks eller godkendelse kan Databehandleren – indenfor rammerne af Databehandleraftalen - derfor bl.a. ikke;
  - a. videregive personoplysningerne til en Dataansvarlig i et tredjeland eller i en international organisation,
  - b. overlade behandlingen af personoplysninger til en Underdatabehandler i et tredjeland,
  - c. lade oplysningerne behandle i en anden af Databehandlerens afdelinger, som er placeret i et tredjeland.
3. Den Dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

## **9 Bistand til den Dataansvarlige**

1. På opfordring fra den Dataansvarlige, skal Databehandleren i fornødent og rimeligt omfang og under hensyn til behandlingens karakter, mod passende vederlag, bistå den Dataansvarlige med passende tekniske og organisatoriske foranstaltninger ved den Dataansvarliges opfyldelse af disse forpligtelser til registrerede ved udøvelse af disses rettigheder.

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. den registreredes indsigtsret
- d. retten til berigtigelse
- e. retten til sletning («retten til at blive glemt«)
- f. retten til begrænsning af behandling
- g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
- h. retten til dataportabilitet
- i. retten til indsigelse



- j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering
2. På opfordring fra den Dataansvarlige, skal Databehandleren i fornødent og rimeligt omfang og under hensyn til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, mod passende vederlag, bistå den Dataansvarlige med at sikre at overholdelse af forpligtelserne i henhold til:
- a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
  - b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødigt forsinkelse og om muligt senest 72 timer, efter at den Dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
  - c. forpligtelsen til – uden unødigt forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
  - d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
  - e. forpligtelsen til at høre tilsynsmyndigheden (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.

## **10 Underretning om brud på persondatasikkerheden**

1. Databehandleren underretter uden unødigt forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Databehandleren eller en eventuel Underdatabehandler.

Databehandlerens underretning til den Dataansvarlige skal om muligt ske senest 72 timer efter at denne er blevet bekendt med bruddet, sådan at den Dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 10.2., litra b, skal Databehandleren - under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den Dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden.

Det kan betyde, at Databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse til tilsynsmyndigheden:

- 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. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
- c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

## **11 Sletning og tilbagelevering af oplysninger**

1. Ved ophør af tjenesterne vedrørende behandling forpligtes Databehandleren til, efter den Dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den Dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

## **12 Tilsyn og revision**

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise Databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, 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, og som forinden er godkendt af den Dataansvarlige.
2. Den nærmere procedure for den Dataansvarliges tilsyn med Databehandleren fremgår af denne aftales Bilag C.
3. Den Dataansvarliges tilsyn med eventuelle Underdatabehandlere sker som udgangspunkt gennem Databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.
4. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den Dataansvarliges og Databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til Databehandlerens fysiske faciliteter mod behørig legitimation.
5. Databehandleren skal én gang årligt fra Hovedaftalen ikrafttrædelse vederlagsfrit til den dataansvarlige fremsende en erklæring fra en uafhængig ekspert om overholdelse af denne Hovedaftale, hvori det dokumenteres, at databehandleren og dennes eventuelle underdatabehandlere, overholder Hovedaftalen.

### 13 Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af Databehandleraftalen vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.
2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes "hovedaftale".

### 14 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift heraf.
2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.
3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.
3. Opsigelse af Databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "hovedaftalen".
4. Aftalen er gældende, så længe behandlingen består. Uanset "hovedaftalens" og/eller Databehandleraftalens opsigelse, vil Databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos Databehandleren og eventuelle Underdatabehandlere.

#### 5. Underskrift

På vegne af den Dataansvarlige

Navn: [Angiv navn]

Stilling: [Angiv stilling]

Dato: [Angiv dato]

Underskrift: [Anfør underskrift]

På vegne af Databehandleren

Navn: Kim Høgskilde

Stilling: Administrerende direktør

Dato: 07-07-2021

Underskrift:



## 15 Kontaktpersoner/kontaktpunkter hos den Dataansvarlige og Databasehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter:
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Navn: [Angiv navn]

Stilling: [Angiv stilling]

Telefonnummer: [Angiv telefonnummer]

Email: [Angiv email]

Navn: Kim Høgskilde

Stilling: Administrerende direktør

Telefonnummer: 29994502

Email: kah@frontread.dk

## **Bilag A    Oplysninger om behandlingen**

**Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige er:**

- At den Dataansvarlige kan anvende FrontRead platformen, som ejes og administreres af Databehandleren, til at indsamle og behandle oplysninger om den Dataansvarliges skoleelever og lærere.

**Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige drejer sig primært om (karakteren af behandlingen):**

- At Databehandleren til FrontRead platformen står til rådighed for den Dataansvarlige og herigennem opbevarer personoplysninger om den Dataansvarliges skoleelever og lærere på virksomhedens servere.

**Behandlingen omfatter følgende typer af personoplysninger om de registrerede:**

- Institutionsnummer, navn og unilgin samt e-mailadresser

**Behandlingen omfatter følgende kategorier af registrerede:**

- Personer, som er elever eller lærere på skolerne.

**Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:**

- Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

## **Bilag B      Betingelser for Databehandlerens brug af Underdatabehandlere og liste over godkendte Underdatabehandlere**

### **B.1      Betingelser for Databehandlerens brug af eventuelle Underdatabehandlere**

Databehandleren har den Dataansvarliges generelle godkendelse til at gøre brug af Underdatabehandlere. Databehandleren skal dog underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre Databehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den Dataansvarlige i hænde minimum 2 måneder før anvendelsen eller ændringen skal træde i kraft. Såfremt den Dataansvarlige har indsigelser mod ændringerne, skal den Dataansvarlige give meddelelse herom til Databehandleren inden 1 måned efter modtagelsen af underretningen. Den Dataansvarlige kan alene gøre indsigelse, såfremt den Dataansvarlige har rimelige, konkrete årsager hertil.”

### **B.2      Godkendte Underdatabehandlere**

Den Dataansvarlige har ved Databehandleraftalens ikrafttræden godkendt anvendelsen af følgende Underdatabehandlere:

Navn	CVR-nr	Adresse	Beskrivelse af behandling
SE Cloud Factory	CVR nr. 35393692	Vestergade 4, 6800 Varde	SE Cloud Factory hoster FrontReads serverpark

Den Dataansvarlige har ved Databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte Underdatabehandlere til netop den behandling, som er beskrevet ud for parten. Databehandleren kan ikke – uden den Dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte Underdatabehandler til en ”anden” behandling and aftalt eller lade en anden Underdatabehandler foretage den beskrevne behandling.

## Bilag C Instruks vedrørende behandling af personoplysninger

FrontRead er i overensstemmelse med Databeskyttelsesforordningen (2016/679) ansvarlige for behandling af persondata i jf. lovgivningen beskrevet heri.

Punkt C.2.1, C.2.2, C.2.3, C.2.4, C.2.5 og C.2.6 er beskrevet ud fra tidligere gældende Sikkerhedsbekendtgørelse (2000/528) af Persondataloven (2000/429), men da disse ikke er gældende længere og ikke bliver direkte erstattet af en lignende lovgivning, henviser førnævnte punkter til retmæssige anbefalinger fra Datatilsynet.

### C.1 Behandlingens genstand/ instruks

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker ved, at Databehandleren udfører følgende:

- Integration til UNI-login, hvorved der opnås adgang til de nødvendige data.

FrontReads produkt er afhængig af, at kende til udvalgte personoplysninger omkring brugeren og administratoren. Disse oplysninger er af ikke-følsom karakter, og begrænses til at kende persondata omhandlende;

- Institutionsnummer
  - a. Bruges til automatisk at placere dem det rigtige sted i databasen, når de logger på første gang, og til at tildele dem licens
- Bruger ID
  - b. Bruges til at authenticate dem ved log-in
- Navn
  - c. Bruges til at identificere dem i administrationsmodulet
- Om vedkommende er *Elev*, *Ansæt* eller *Ekstern*
  - d. Bruges til at se om de skal have administrationsrettigheder i administrationsmodulet

#### C.1.1 Behandlingens kategorisering

De gældende persondataoplysninger, som FrontRead indsamler og opbevare, er ikke indbefattet i bestemmelsen af 'følsomme' persondata jf. Databeskyttelsesforordningen (2016/679) betragtning (51) samt artikel 9 stk. 1.

#### C.1.2 Behandlingens relevans

FrontRead har *Instnr*, *brugered* og *navn* direkte i databasen, og man kan ud fra administrationsrettighederne se, om brugeren er Elev eller Ansæt. Derudover opbevarer FrontRead kun data som viser, hvor langt brugeren er i dennes FrontRead-forløb samt hvordan udviklingen ser ud i samme forløb.



Herunder oplystes de datainformationer, som FrontRead har indsigt i og opbevarer;

1. Brugerens gruppe (manuelt navngivet af en administrator, ofte navngivet efter deres klassetrin og klassens navn, eg. 7. a)
2. Hvilken tekstpakke, deres underviser har givet dem (hvilket kan give et indtryk af om de er stærke eller svage læsere)
3. Antal ord pr. minut, brugeren læser (læsehastighed)
4. Hvor meget deres læsehastighed har forbedret sig siden de startede forløbet
5. Hvor mange rigtige svar de har haft i gennemførte og ikke-gennemførte øvelser
6. Hvor mange gange de har været gennem læseøvelserne

FrontRead har gennem afsøgning af forskellige løsninger vurderet, at brugen af WS22 - wsi-INST.hentInstBruger er mest formålstjenlig i brugen af samt med formålet om at opnå optimal udnyttelse af FrontReads løsning. Der anvendes endvidere WS17 lille til at sikre automatisk sletning af elevdata, når eleven forlader den dataansvarliges område (folkeskoler i kommunen).

## **C.2 Behandlingsikkerhed**

Jf. Bilag C punkt C.1.1 er de personoplysninger, som det for FrontRead er nødvendigt at gøre brug af, ikke kategoriseret som direkte personfølsomme jf. Databeskyttelsesforordningen (2016/679) artikel 9 stk. 1. Således tilpasses sikkerhedsniveauet for behandlingssikkerheden de gældende oplysningers grad af følsomhed.

I overensstemmelse med Databeskyttelsesforordningen (2016/679) artikel 31 vedtager FrontRead, at gennemføre passende tekniske samt organisatoriske foranstaltninger for at sikre, at det kun er den mest nødvendige persondata der behandles i samtlige aktiviteter. De ændringer, som FrontRead op og indtil Databeskyttelsesforordningens ikrafttræden har foretaget med henblik på at være kompatibel (compliant) med lovkravene, varetages fremadrettet af udvalgte nøglepersoner, herunder CEO og CPO.

### **C.2.1 Inddatamateriale indeholdende persondata**

I overensstemmelse med anbefalinger af Datatilsynet behandler FrontRead Inddatamateriale af autoriserede funktioner. Såfremt der forekommer inddata, som ikke længere anvendes til de givne formål, skal disse inddata slettes eller tilintetgøres. Dette gøres af en Softwareudvikler-funktion. Herigennem sikrer Softwareudvikler-funktionen samtidig, at inddata tilintetgøres i overensstemmelse med anbefalingerne fra Datatilsynet.

FrontRead benytter forskellig personidentificerbar datainformation afhængigt af brugeren,. Således specificeres brugertyperne *UNI-Login Bruger* og *Andre Brugere*. Ved UNI-Login Brugeren, som enten er lærer eller elev ved en institution, er det nødvendigt at bruge inddata indeholdende navn, UNI-Login, brugertype og institutionsnummer. Ved Andre Brugere behøves inddata indeholdende brugerens navn og mailadresse.

FrontRead modtager inddata fra UNI-Login, disse omfatter institutionsnummer, bruger ID, navn eller navnetitlen "F E" el.lign. i tilfælde af navnebeskyttelse, brugertype og rolle. Disse data opbevares og behandles på samme vilkår i overensstemmelse med anbefalinger fra Datatilsynet.

Den data, som FrontRead indsamler er nødvendige for at kunne generere indsigtsfulde og valide resultater til brugeren. Inddata behandles udelukkende af FrontReads autoriserede funktioner, herunder Softwareudvikler- og Support-funktionen.

### **C.2.2 Uddatamateriale indeholdende persondata**

I overensstemmelse med anbefalinger fra Datatilsynet anvendes FrontReads uddatamateriale udelukkende af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages. Disse personer bærer funktionerne Softwareudvikler, Salg og Support.

FrontRead behandler data i form af de resultater, som brugeren gennem brug af løsningen, opnår. FrontRead bruger uddatamateriale til, at give relevante brugere indsigt i de resultater, som en given bruger har opnået.

Uddata findes på administrationsmodulet "Partner" tilknyttet FrontRead-plattformen, som alle brugere og administratorer har adgang til, dog har alle ikke lige adgang (se afsnittet vedrørende Autorisation og adgangskontrol).

Det er udelukkende FrontReads Softwareudvikler- og Support-funktion der har direkte adgang til samtlige uddata, og disse opbevares i en database. Uddata må ikke gemmes eller logges lokalt på en FrontRead medarbejders computer.

Når data ikke er nødvendig og af relevans for FrontRead længere, tilintetgøres de pågældende data i FrontReads database.

### **C.2.3 Fysisk sikring**

I overensstemmelse med anbefalinger fra Datatilsynet beskriver FrontRead i hvilken udstrækning der foretages sikkerhedsforanstaltninger i det fysiske rum.

På FrontReads egen lokation er der truffet bestemmelse om, at der altid er mindst én medarbejder til stede i åbningstiden. I tilfælde af det modsatte, aflåses kontordørene og vinduer holdes lukkede. Samme aflukningsprocedure skal foretages udenfor åbningstid.

For at forhindre indbrud i FrontReads computere placeret på FrontReads lokalitet, installeres samtlige computere med krypteret passwords og antivirus programmene.

#### **C.2.4 Autorisation og adgangskontrol**

FrontRead begrænser adgangen til brugernes persondata til et minimum, denne opgave varetages af Softwareudvikler- og Support-funktionen jf. anbefalinger fra Datatilsynet.

FrontRead agerer *Super Administrator.*, og har herigennem adgang til al tilgængelig data i FrontReads platform. Superadministratorer-funktionen hos FrontRead begrænser sig her til Softwareudvikler- og Support-funktionen.

#### **C.2.5 Logning**

I overensstemmelse med retmæssige anbefalinger fra Datatilsynet foretager FrontRead maskinel registrering (logning) af alle anvendelser af personoplysninger.

FrontRead bruger Loggen til at overvåge og analyserer hvilke elementer på hjemmesiden, der bliver brugt samt hvor meget af individuelle elementer der benyttes.

I henhold til anbefalinger fra Datatilsynet slettes loggen ikke, da den data, der forefindes heri, behandles med henblik på statistisk og videnskabelig undersøgelse, hvor identifikationsoplysningerne forinden er blevet krypteret. FrontRead foretager maskinel logning af både bruger og tidspunkt for behandlingen.

Logning af FrontReads hjemmesidedata foretages af hjemmeside hosting-leverandøren. Logningen af FrontReads persondata via FrontReads platform foretages af serveren hos FrontReads hosting leverandør.

#### **C.2.6 Hjemmearbejdspladser**

FrontRead behandler personoplysninger på hjemmearbejdspladser i overensstemmelse med Datatilsynets anbefalinger vedr. hjemmearbejdspladser. Denne behandling finder sted på en pc-arbejdsplads, der fysisk udenfor FrontReads lokalitet.

I tilfælde af, at medarbejdere med autoriseret hensigt opretter pc-arbejdsplads udenfor FrontReads lokalitet, benytter medarbejderen en til formålet oprettet testdatabase. Således forhindres det, at den reelle persondatabase udsættes for usikre forbindelser.

Hjemmearbejdet foregår altid via en af virksomheden godkendt computer, hvortil brugeren aldrig opretter eller gemmer relevante kodeord på andre computere. Derudover skal de tilknyttede computere til hjemmearbejdspladsen altid være installeret med antivirus programmel jf. datatilsynets retmæssige anbefalinger.

#### **C.3 Opbevaringsperiode/sletterutine**

I overensstemmelse med Databeskyttelsesordningen (2016/679) artikel 5 stk. 1 (C) behandler FrontRead persondata ud fra princippet 'dataminimering'. FrontRead opbevarer personoplysninger indtil den Dataansvarlige opsig aftalen med FrontRead og/eller i tilfælde af, at Dataansvarlige anmoder FrontRead om at få oplysningerne slettet.

#### **C.4 Lokaltet for behandling**

Behandling af de i aftalen omfattede personoplysninger sker på nedenstående lokaliteter.:

- FrontRead ApS, Åbogade 15, 8200 Aarhus N
  - Databehandler
- SE Cloud Factory, Vestergade 4, 6800 Varde
  - Underdatabehandler til FrontRead

Såfremt én af ovenstående lokaliteter skifter, forpligter FrontRead sig til at informere de dataansvarlige. Endvidere se punkt C.5

#### **C.5 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande**

##### **C.5.1. Overførsel af personoplysninger til tredjelande**

Databehandleren må ikke overføre Kommunens personoplysninger til tredjelande.

Hvis Kommunen 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.

##### **C.5.2 virksomhed i udlandet**

FrontRead driver virksomhed i Tyskland gennem eget selskab, som hedder FrontRead - Institut für Lesen und Lernen GmbH. FrontReads fysiske lokation i Tyskland er hos Youngstar (DSA youngstar GmbH, Friedrich-Ebert-Damm 111, 22047 Hamburg, Tyskland). DSA Youngstars medarbejdere arbejder for FrontRead, og begge virksomheder er derfor underlagt gældende regler af den givne tyske tilsynsmyndighed jf. Databeskyttelsesforordningen (2016/679) artikel 51. Da Youngstar er partner, og FrontReads hovedsæde er beliggende i Danmark, gælder Datatilsynets regler for tilsyn, auditing og påbud jf. Databeskyttelsesforordningen (2016/679) artikel 58. FrontRead forventer i tilfælde af opstået behov, at den tyske tilsynsmyndighed samarbejder med den danske tilsynsmyndighed (Datatilsynet, red.) i overensstemmelse med Databeskyttelsesforordningen (2016/679) artikel 61. Ingen af medarbejderne i DSA eller FrontRead GmbH har adgang til persondata vedr. danske skoleelever eller lærere.

### **C.6 Nærmere procedurer for den Dataansvarliges tilsyn med den behandling, som foretages hos Databehandleren**

Den Dataansvarlige eller en repræsentant for den Dataansvarlige har herudover adgang til at føre tilsyn, herunder fysisk tilsyn, hos FrontRead, når der efter den Dataansvarliges vurdering opstår et behov herfor.

Den Dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den Dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsagligt den tid), der er nødvendig for, at den Dataansvarlige kan gennemføre sit tilsyn.

### **C.7 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle Underdatabehandlere**

Den Dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos Underdatabehandleren. Dette kan blive aktuelt, såfremt den Dataansvarlige vurderer, at Databehandlerens tilsyn med Underdatabehandleren ikke har givet den Dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos Underdatabehandleren sker i overensstemmelse med denne Databehandleraftale.

Den Dataansvarliges eventuelle deltagelse i et tilsyn hos Underdatabehandleren ændrer ikke ved, at Databehandleren også herefter har det fulde ansvar for Underdatabehandlerens overholdelse af databeskyttelseslovgivningen og denne Databehandleraftale.

Databehandlerens og Underdatabehandlerens eventuelle udgifter i forbindelse med afholdelse af et fysisk tilsyn/en inspektion hos Underdatabehandleren er den Dataansvarlige uvedkommende – uanset at den Dataansvarlige har initieret og eventuelt deltaget på et sådant tilsyn.