# Databehandleraftale

Mellem

Den dataansvarlige:

Xxx

(herefter Kommunen)

og

Databehandleren:

Epinion

CVR 25638670

Ryesgade 3F

2200 København N

Danmark

## Indhold

# 1 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 "samarbejdsaftale": [Samarbejdsaftale om anvendelse af talblindhedstest og tilhørende digitale løsninger], som er indgået den [dato].

4. Databehandleraftalen og "samarbejdsaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "samarbejdsaftalen" – erstattes af en anden gyldig databehandleraftale.

5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "samarbejdsaftalen".

6. Til denne aftale hører fem 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 "samarbejdsaftale".

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.

## 2 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.

## 3 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.

## 4 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.

# 5 Behandlingssikkerhed

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. Databehandleren indførte 25. maj 2018 en række nye tekniske og organisatoriske sikkerhedsforanstaltninger, der gælder for hele virksomheden i alle behandlingssituationer. Sikkerhedsforanstaltningerne har som default et "højt" beskyttelsesniveau svarende til, at der i alle tilfælde behandles personoplysninger af særlig følsom karakter. Således vil der kun i de særlige omstændigheder, hvor disse foranstaltninger vurderes utilstrækkelige, blive udarbejdet en separat risikovurdering i tilknytning til denne aftale, jf. punkt 5.2.

5. 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 "samarbejdsaftale" eller af denne aftales bilag D.

# 6 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 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 min. 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. Den dataansvarliges nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales 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 denne databehandleraftale, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren 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 underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.

5. Underdatabehandleraftalen 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 underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

## 7 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.

## 8 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 3.

    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

Det præciseres, at testresultater og scorer alene udgør et pædagogisk støtteværktøj og ikke i sig selv udgør automatiske individuelle afgørelser med retsvirkning eller tilsvarende betydelig påvirkning for den registrerede.

2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art. 28, stk. 3, litra f.

   Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   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 unødig 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 unødig 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

3. Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af parternes "samarbejdsaftale" eller af denne aftales bilag D.
4. I det omfang behandling af personoplysninger er nødvendig for den dataansvarliges opfyldelse af lovbestemte opgaver vedrørende evaluering af undervisning, jf. folkeskoleloven, samt for videnskabelige og statistiske formål, kan visse registreredes rettigheder, herunder retten til sletning efter artikel 17 GDPR, være begrænset i medfør af artikel 17, stk. 3 og artikel 89.

   Den dataansvarlige foretager en konkret vurdering af anmodninger om sletning under hensyntagen til nødvendighed og proportionalitet.

Den dataansvarlige er således berettiget til at opretholde behandling og opbevaring af personoplysninger, uanset anmodninger om sletning, i det omfang dette er nødvendigt for opfyldelse af lovbestemte opgaver samt til videnskabelige og statistiske formål, jf. artikel 17, stk. 3 og artikel 89.

## 9 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig 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 24 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 8.2., litra b, skal databehandleren - under hensyntagen 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

## 10 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 opbevaring er nødvendig eller berettiget i henhold til gældende ret, herunder til videnskabelige og statistiske formål, jf. artikel 17, stk. 3 og artikel 89. Opbevaring til videnskabelige og statistiske formål kan ske uafhængigt af databehandleraftalens ophør, i det omfang dette er nødvendigt og lovligt.

2. Ved overførsel af et datasæt til Danmarks Statistik anses databehandlerens behandling af det pågældende datasæt for afsluttet, når overførslen er gennemført og kvitteret.
   Herefter ophører databehandlerens ansvar for den videre behandling af datasættet.

## 11 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.

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.

## 12 Parternes aftale om andre forhold

1. Reguleringen af ansvar og ansvarsbegrænsninger og i aftale(r)n(e) om levering af Hovedydelserne finder anvendelse også for denne Databehandleraftale, som om denne Databehandleraftale var en integreret del heraf.

## 13 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 "samarbejdsaftale" eller af denne aftales bilag D.
5. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "samarbejdsaftalen".
6. Aftalen er gældende, så længe behandlingen består. Uanset "samarbejdsaftalens" og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.
7. Den dataansvarlige kan instruere databehandleren om at overføre personoplysninger til en ny databehandler i forbindelse med leverandørskifte.

Databehandleren er i så fald forpligtet til at medvirke til en sikker og kontrolleret overdragelse af data, herunder i et struktureret og almindeligt anvendt format.
Overdragelsen forudsætter, at den nye databehandler er behørigt databeskyttelsesretligt reguleret.
Databehandlerens forpligtelser efter denne aftale ophører for de overdragne data ved gennemført overdragelse.

8. Underskrift

| På vegne af den dataansvarlige | | På vegne af databehandleren | |
|---|---|---|---|
| Navn: | [Angiv navn] | Navn: | [Angiv navn] |
| Stilling: | [Angiv stilling] | Stilling: | [Angiv stilling] |
| Dato: | [Angiv dato] | Dato: | [Angiv dato] |
| Underskrift: | [Anfør underskrift] | Underskrift: | [Anfør underskrift] |

## 14 Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

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] | Navn: | [Angiv navn] |
| Stilling: | [Angiv stilling] | Stilling: | [Angiv stilling] |
| Telefonnummer: | [Angiv telefonnummer] | Telefonnummer: | [Angiv telefonnummer] |
| Email: | [Angiv email] | Email: | [Angiv email] |

# Bilag A Oplysninger om behandlingen

A1. Formål

**Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:**

- at den dataansvarlige kan anvende en digital løsning til **screening og testning af elever i grundskolen (2.–10. klassetrin)** med henblik på identifikation af elever i risiko for talblindhed,
- at understøtte den dataansvarliges **løbende evaluering og opfølgning på elevernes udbytte af undervisningen** i henhold til gældende lovgivning for kommunale undervisningstilbud, herunder folkeskoleloven, ungdomsskoleloven og relevant speciallovgivning,
- at indgå som et supplement til det samlede pædagogiske vurderingsgrundlag.

Behandlingen sker som led i udførelsen af en opgave i samfundets interesse, jf. artikel 6, stk. 1, litra e i Databeskyttelsesforordningen.

Herudover skal behandlingen i overensstemmelse med denne aftale kunne danne grundlag for videnskabelige og statistiske formål, herunder udvikling, validering og kvalitetssikring af test og analysemetoder, jf. artikel 89.

**A.2 Karakteren af behandlingen**

Databehandlerens behandling består i at stille en digital test- og rapporteringsløsning til rådighed samt at foretage behandling af personoplysninger i den forbindelse.

Behandlingen omfatter navnlig:

- identifikation af elever og relevante brugere via UniLogin
- gennemførelse af digitale testforløb
- registrering af testbesvarelser
- automatisk scoring og beregning af testresultater
- lagring og strukturering af data
- generering af rapportering på elev-, klasse- og skoleniveau
- tilgængeliggørelse af resultater for relevante fagpersoner

Behandlingen sker udelukkende efter instruks fra den dataansvarlige.

Identifikation af elever sker via UniLogin. Efterfølgende kobling til personidentifikation (fx CPR) foretages ikke af databehandleren, men håndteres af Danmarks Statistik i overensstemmelse med gældende regler.

### A.3 Typer af personoplysninger

**Behandlingen omfatter følgende typer af personoplysninger:**

**Personoplysninger** (jf. Databeskyttelsesforordningens artikel 6):

**Elever:**

- UniLogin-oplysninger
- navn
- køn (hvis registreret)
- skole
- klassetrin og klasse

**Lærere og brugere:**

- UniLogin-oplysninger
- navn
- e-mailadresse
- tilknytning til skole

**Test- og systemdata:**

- testbesvarelser
- opgavebesvarelser
- testresultater og scorer
- tidsstempler (fx tidspunkt for besvarelse)
- metadata (fx klassetrin, testforløb, brugerrelationer)

**Særlige kategorier af personoplysninger** (jf. Databeskyttelsesforordningens artikel 9):

Der behandles **ikke** særlige kategorier af personoplysninger.

**Oplysninger om CPR-nummer** (jf. Databeskyttelseslovens § 11):

Der behandles **ikke** CPR-numre.

### A.4 Kategorier af registrerede

**Behandlingen omfatter følgende kategorier af registrerede:**

- elever i grundskolen (2.–10. klassetrin)
- lærere
- øvrige brugere med adgang til systemet (fx kontaktpersoner i kommuner og på skoler, herunder systemadministratorer)

**A.5 Varighed**

**Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige påbegyndes ved denne aftales ikrafttræden** og sker, så længe aftalen er gældende.

Behandlingen er baseret på, at den enkelte elevs resultater kan **følges og sammenstilles over tid**. Dette indebærer, at testresultater og øvrige relevante oplysninger opbevares, således at det er muligt at analysere og vurdere elevens progression.

Opbevaringen af personoplysninger er således en **forudsætning for at kunne måle progression** og indgår som en integreret del af den dataansvarliges opgave med løbende evaluering af elevernes udbytte af undervisningen.

Personoplysninger opbevares i aftaleperioden med henblik på at følge elevens progression.

Ved aftalens ophør slettes eller anonymiseres personoplysninger senest 6 måneder efter ophør, medmindre:

- den dataansvarlige instruerer om fortsat behandling, eller
- opbevaring er nødvendig i henhold til gældende ret, herunder til videnskabelige og statistiske formål, jf. artikel 17, stk. 3 og artikel 89.

Ved aftalens ophør:

- slettes eller tilbageleveres personoplysninger til den dataansvarlige efter dennes instruks, eller

- anonymiseres oplysningerne, således at de kan anvendes til statistiske og videnskabelige formål,

medmindre opbevaring er nødvendig i henhold til gældende ret, herunder for opgaver i samfundets interesse samt til videnskabelige og statistiske formål, jf. artikel 17, stk. 3 og artikel 89 i Databeskyttelsesforordningen.

# Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

**Godkendte underdatabehandlere**
Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

| Navn | CVR-nr | Adresse | Beskrivelse af behandling |
|---|---|---|---|
| Itm8 \| AddPro | 32563600 | Tonsbakken 16, 3., 2740 Skovlunde | Datacenter: Hosting og drift af servere (backup, overvågning, vedligehold og support) |
| Microsoft | 13612870 | Microsoft Netherlands BV: Naritaweg 165, Amsterdam, 1043 BW, Netherlands Kontoradresse: Kanalvej 7 2800 kgs. Lyngby | Drift af Microsoft 365 softwarepakke, herunder e-mail og Office-pakken |
| Brevo | 498 019 298 | 17 Rue de Salneuve, 75017 Paris, France | Mailudsendelses-service |

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 end aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

### 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 underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal som udgangspunkt være den dataansvarlige i hænde minimum 30 dage før

anvendelsen eller ændringen skal træde i kraft så vidt dette er muligt. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 14 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

Uanset ovenstående accepterer den dataansvarlige, at der kan være særlige tilfælde, hvor der kan opstå et konkret behov for, at ændringen vedrørende tilføjelse eller erstatning af underdatabehandlere sker med kortere varsel eller straks. I sådanne tilfælde vil databehandleren underrette den dataansvarlige om ændringen snarest muligt.

# Bilag C Instruks vedrørende behandling af personoplysninger

### C.1 Behandlingens genstand/ instruks

Databehandleren stiller en digital løsning til rådighed for den dataansvarlige med henblik på:

- gennemførelse af talblindhedstest
- registrering af elevernes testbesvarelser
- beregning af testresultater
- tilgængeliggørelse af resultater til skolen på elev- og klasseniveau

Løsningen anvendes som et pædagogisk redskab til brug for:

- vurdering af den enkelte elevs niveau
- opfølgning på elevens udvikling over tid
- understøttelse af undervisning og pædagogisk tilrettelæggelse

Databehandleren foretager ikke analyser eller sammenstillinger på tværs af skoler eller kommuner med henblik på benchmarking, tilsyn eller andre administrative eller styringsmæssige formål. Databehandleren stiller ikke selvstændige analysetjenester, rådgivning eller datagrundlag til brug for ledelsesinformation eller tilsyn til rådighed for den dataansvarlige.

#### C.1.1 Afgrænsning af behandlingen

Behandlingen efter denne databehandleraftale omfatter behandling af personoplysninger til brug for den dataansvarliges evaluering af elevernes udbytte af undervisningen samt skolens pædagogiske arbejde, herunder på elev- og klasseniveau, samt den sideordnede behandling til statistiske og videnskabelige formål som beskrevet i punkt C.1.2.

#### C.1.2 Sideordnet behandling til forskningsformål

Databehandleren er berettiget og forpligtet til løbende at overføre relevante datasæt til Danmarks Statistik med henblik på videnskabelige og statistiske formål, herunder forskningsprojekter gennemført af Aarhus Universitet. Overførslen sker som en integreret del af den behandling, som den dataansvarlige ved indgåelse af denne aftale har instrueret databehandleren i.

Den dataansvarlige kan ikke ved særskilt instruks begrænse eller undlade denne overførsel, så længe aftalen er i kraft.

Overførslen kan omfatte personhenførbare mikrodata, herunder:

- identifikation via UniLogin
- testbesvarelser
- testresultater og beregnede scorer

Overførslen sker løbende som en integreret del af den behandling, der er fastlagt i denne aftale.

Ved overførsel til Danmarks Statistik sker identifikation af elever via UniLogin. Eventuel efterfølgende kobling til personidentifikation (herunder CPR) foretages ikke af databehandleren, men håndteres af Danmarks Statistik i overensstemmelse med gældende regler. Overførslen sker i overensstemmelse med gældende lovgivning og Danmarks Statistiks regler for databehandling og datasikkerhed. Databehandleren deltager ikke i den efterfølgende behandling eller analyse af data hos Danmarks Statistik.

### C.2 Behandlingssikkerhed

Sikkerhedsniveauet hos databehandleren er som standard etableret som "højt" sikkerhedsniveau upåagtet typen af personoplysninger, der behandles.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne.

Databehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

**Lagring og udveksling af data**

Databehandleren anvender SharePoint-løsning til lagring og udveksling af data. SharePoint sikrer løbende backup, så filer og data kan genskabes i tilfælde af nedbrud. Tilsvarende gemmes logfiler, så der er transparens i forhold til hvem, der arbejder med data fx i tilfælde af databrud. Endelig giver SharePoint mulighed for at anvende 2-faktor validering i udvekslingen af data med eksterne parter, herunder den dataansvarlige, således det sikres, at kun navngivne parter får adgang til data.

I SharePoint er der opsat adgangsbegrænsning på projektmapper, så der alene er adgang til persondata for relevant personale. Det er projektlederens pligt at sikre, at kun relevante personer internt og evt. eksternt har adgang til data. Adgangsbegrænsningen ophæves tidligst, når projektet er overleveret til kommunen, og data er anonymiseret eller slettet.

I forbindelse med en senere automatiseret løsning (fase 2) vil personoplysninger endvidere blive behandlet og opbevaret i en applikation med tilhørende database, hvor data registreres, lagres og stilles til rådighed for den dataansvarlige.

Adgang til løsningen vil ske via Uni-login, og der vil være etableret rollebaseret adgangsstyring, således at brugere alene har adgang til oplysninger om egne elever og egen skole. Der logges adgang og anvendelse i systemet med henblik på sporbarhed og sikkerhed.
Behandlingen i den automatiserede løsning vil ske under tilsvarende krav til sikkerhed, adgangsstyring og logning som beskrevet ovenfor.

**Backup datacenter**
Der foretages change backup af alle data på servere én gang i timen, som gemmes 30 dage. Change backup kan til enhver tid enten restores til test eller til produktion, så det vil være muligt at teste og genskabe data med maksimalt 1 times gammelt data. Én gang i døgnet foretages en fuld backup, som flyttes til andet datacenter væk fra produktionsdata, og dette gemmes også som standard i 30 dage.

**Sikkerhedstests datacenter**
Der foretages relevante periodiske sikkerhedstests af egen IT-infrastruktur. Sikkerhedstests afdækker relevante angrebsflader og angrebsscenarier under hensyntagen til den selvdefinerede trusselsmodel. Sikkerhedstestning udføres af uvildigt kvalificeret personale i overensstemmelse med anerkendte standarder for sikkerhedstests.

**Incident Management datacenter**
Incident Management dækker hændelser (Incidents), der påvirker serverdriften. Disse håndteres på baggrund af prædefinerede reaktionstider, og formålet med processen er at genskabe normal drift så hurtigt som muligt og minimere indvirkningen på de forretningsmæssige aktiviteter, således at den højst mulige grad af servicekvalitet og tilgængelighed bliver opretholdt. Incidents registreres i et ITSM-system, så incidents kan analyseres og forebygges.

**Logning datacenter**
Logning er en integreret del af databehandlerens driftsplatform. Der logges bl.a. Performance logs, systemlogs, database logs, backup logs, event logs og access logs. Dette sker for at sikre sporbarhed og dokumentation. Der anvendes som udgangspunkt danske NTP servere til synkronisering af tid på tværs af systemer.

**Adgang via internettet datacenter**
Alle servere er beskyttet via en firewall. Det vil kun være de servere, som skal kunne tilgås fra Internettet, der vil være mulige at tilgå (IIS, FTP mv.) Det vil ikke være muligt at tilgå andre servere fra Internettet. Serveren er segmenter i netværk (LAN & DMZ), således servere, der kan tilgås fra Internettet, ikke står på samme netværk som interne servere.

**Fysisk sikring datacenter**
Fysisk sikring ift. adgang til servere består af hærdede ståldøre og vægge m.v. Herudover kommer bl.a. også tiltag som strømsystem bestående af UPS og dieselgenerator, redundante køleanlæg samt brandsikringsanlæg, som kan kvæle enhver ild uden at ødelægge infrastrukturen. Alle vitale

områder fx temperatur, fugt, fysisk indtrængen overvåges og alarmerer 24/7/365 relevant personale eller eksterne partnere.

Sikkerhedsafgrænsninger (barrierer som fx vægge, kortstyrede indgangsporte eller bemandede receptioner) anvendes til at beskytte områder, der indeholder informationer og informationsbehandlingsfaciliteter. Kun autoriseret personale har mulighed for at skaffe sig adgang til datacentret efter forudgående clearing. Personer, der ikke er ansat i datacentret, kan kun få adgang til udstyr, hvis det er strengt nødvendigt, og de bliver ledsaget af en ansvarlig medarbejder samt registreres i en logbog ved ind- og udgang.

**Fysisk sikring kontorer**
Der er alene adgang til Databehandlerens fysiske kontorer via en bemandet reception. Gæster må kun forlade receptionsområdet under ledsagelse af en ansat fra Databehandleren. Alle medarbejdere er instrueret i at stoppe eventuelle uledsagede gæster og hjælpe dem med at finde den rette kontaktperson eller forlade Databehandlerens lokaler. Den sidste medarbejder, der forlader kontoret om aftenen, skal sikre sig, at alle vinduer er lukkede, yderdøre låst og at alarmen aktiveres.

**Tavshedspligt og fortrolighed**
Databehandlerens medarbejdere er forpligtet til at holde al viden om kommunen og skolers forhold fortrolige både under og efter projekters afslutning. Dette fremgår både af Databehandlerens personalehåndbog og af de enkelte medarbejderes ansættelseskontrakter. Underleverandører er underlagt tilsvarende tavshedsforpligtelser. Tavshedspligten gælder for alt materiale og viden, som er kommet Databehandleren i hænde i projektforløbet, medmindre andet aftales eksplicit med den dataansvarlige; fx at Databehandleren har lov til at anvende den dataansvarlige som reference.

**IT-politikker for medarbejdere**
Databehandlerens medarbejdere er instrueret i at gøre sig løbende overvejelser om databeskyttelse gennem dataminimering, pseudonymisering og anonymisering, så vidt muligt.

De er ligeledes instrueret i, hvordan man sikrer korrekt udveksling af data, og at minimere brugen af flytbare enheder til datatransmission. Evt. ekstraordinær brug af USB til datatransmission skal gå via IT, der sikrer kryptering, såfremt data skal forlade Databehandlerens lokaler. Eventuelle ønsker om brug af særligt hard- eller software skal godkendes af IT forud for installation.

Databehandleren gennemfører løbende PC-standardisering målrettet på at skabe ensartede brugerprofiler og systemer på tværs af virksomheden, herunder sikre kryptering af alle PC'er i tilfælde af tab. PC'er opdateres centralt fra IT-afdelingen, dette gælder både operativsystem og 3 parts software.

Databehandleren har begrænset brugen af administrative konti, og der anvendes alene individuelle bruger-id'er og adgangskoder. I informationssikkerhedsprocedurer er beskrevet krav til stærke adgangskoder, og alle systemejere og medarbejdere er gjort bekendt med dette.

Når databehandlerens medarbejdere opholder sig uden for databehandlerens kontorer fx. Hjemmearbejdsplads, kan servere udelukkende tilgås via VPN forbindelse.

**Compliance setup**
Databehandlerens informationssikkerheds-setup er beskrevet i privatlivspolitik samt informationssikkerhedspolitik og -håndbog med tilhørende procedurer, vejledninger og kontroller. Heri er fastlagt roller og ansvar i forhold til informationssikkerhed for alle i Databehandlerens organisation.

Databehandleren gennemfører månedlige, kvartalsvise og årlige kontroller af compliance med informationssikkerhedsframework, hvis resultater forelægges Databehandlerens Commercial Management Team. Der gennemføres løbende awareness kampagner for alle medarbejdere, som ligeledes årligt certificeres inden for Cyber Security og GDPR.

Endelig har Databehandleren udpeget en databeskyttelsesrådgiver, DPO, som varetager løbende kvalitetssikring og kontroller af Databehandlerens interne procedurer samt sikrer datasubjekternes rettigheder.

Man kan læse mere om, hvordan Databehandleren beskytter data i privatlivs- og informationssikkerhedspolitik på hjemmesiden: https://epinionglobal.com/da/privatlivspolitik-for-epinion/

### C.3 Opbevaringsperiode/sletterutine
Personoplysningerne opbevares i udgangspunktet i hele aftaleperioden, idet behandlingen er baseret på, at elevens resultater kan følges og sammenstilles over tid med henblik på at vurdere progression.

Sletning eller anonymisering sker ved aftalens ophør eller efter den dataansvarliges instruks, medmindre opbevaring er nødvendig i henhold til gældende ret eller til videnskabelige og statistiske formål, jf. artikel 17, stk. 3 og artikel 89.

### C.4 Lokalitet for behandling
Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de følgende:

- *Epinion Danmark (København-afdeling), Ryesgade 3F, 2200 København N, Danmark*
- *Epinion Danmark (Aarhus-afdeling), Mariane Thomsens Gade 4B, 2. 8000 Aarhus C*
- Andre lokaliteter, hvor det er nødvendigt og relevant for Epinion Danmark at behandle personoplysninger i forbindelse med leveringen af ydelsen til den dataansvarlige, f.eks.

i forbindelse med gennemførelse af interviews, observationer mv., fremtidige adresser i Danmark eller vores underdatabehandleres behandlingslokaliteter jf. Bilag B.1.

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

Databehandleren overfører ikke data omfattet af persondataforordningen til tredjelande, hvor der ikke foreligger et gyldigt overførselsgrundlag

Hvis den dataansvarlige ikke i dette afsnit eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må databehandleren ikke indenfor rammerne af databehandleraftalen foretage en sådan overførsel.

### C.6 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Databehandleren skal årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæring kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE-3000 erklæring

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Baseret på resultaterne af revisionserklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige kan herudover foretage et årligt, fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos databehandleren.

Udover det fysiske tilsyn, kan der føres skriftligt tilsyn med databehandleren, 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 (hovedsageligt 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

Databehandleren eller en repræsentant for databehandleren kan foretage et årligt, fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos underdatabehandleren, medmindre der foreligger en erklæring fra en uafhængig 3. part for underdatabehandlerens overholdelse af databehandleraftalen.

Udover det fysiske tilsyn, kan der føres skriftligt tilsyn med underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.

Dokumentation for de afholdte tilsyn sendes snarest muligt til orientering hos den dataansvarlige.

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.

## Bilag D Parternes regulering af andre forhold

Databehandlerens bistand vedrørende registreredes rettigheder sker under hensyntagen til begrænsninger i artikel 17, stk. 3 og artikel 89, når behandling er nødvendig for opgaver i samfundets interesse samt til videnskabelige og statistiske formål.

## Bilag E Omfattede institutioner

Databehandleraftalen omfatter alene de institutioner, som den dataansvarlige har autoriseret til deltagelse i løsningen.

Den dataansvarlige kan til enhver tid ændre kredsen af omfattede institutioner.

Databehandleren må alene behandle personoplysninger vedrørende de institutioner, som er omfattet.