,

DATABEHANDLERAFTALE

Mellem

Kundens Navn:_____

Kundens Adresse: _____

Kundens CVR. NR:_____
(herefter Kunden)

og

Skolevisioner ApS
Ry Væksthus
Ellemosen 3
8680 Ry
CVR.NR. 30535421
(herefter Leverandøren)

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om Leverandørens behandling af personoplysninger på vegne af Kunden:

Databehandleraftale vedrørende onlinetjenesten Klassetrivsel

1. Formål

Kunden er dataansvarlig og Leverandøren er databehandler.

Leverandøren behandler i medfør af aftale med Kunden om Kundens anvendelse af Klassetrivsel fra Skolevisioner APS (herefter "Abonnementsaftalen") personoplysninger for Kunden, hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

2. Generelt

2.1.
Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen).

2.2.
I Aftalen er indarbejdet de krav, som Databeskyttelsesforordningen stiller til databehandleraftaler.

2.3
Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

3. Kundens rettigheder og forpligtelser

3.1
Kunden er dataansvarlig for de personoplysninger, som Kunden instruerer Leverandøren om at behandle. Kunden har ansvaret for, at de personoplysninger, som Kunden instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Kundens opgavevaretagelse. Kunden er ligeledes ansvarlig for at, der er gyldig hjemmel til alle de formål Klassetrivsel anvendes til hos Kunden.

3.2
Kunden har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. aftalens pkt. 2.1 og 2.2.

3.3
Kunden er forpligtet til at orientere Leverandøren i tilfælde af Kundens eventuelle skærpede it-sikkerhedsregler og ved ændringer i Kundens it-sikkerhedspolitik og it-sikkerhedsregulativ.

4. Leverandørens forpligtelser

4.1
Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Kunden, jf. pkt. 6 og bilag 3. Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. aftalens pkt. 2.1 og 2.2.

4.2
Leverandøren behandler alene de overladte personoplysninger efter instruks fra Kunden, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Abonnementsaftalen.

4.3.
Leverandøren skal føre fortegnelser over behandlingen af personoplysninger samt fortegnelser over alle brud på persondatasikkerheden.

4.4
Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, jf. bilag 1 – Sikkerhed.

4.5
Leverandøren skal på opfordring fra Kunden hjælpe med at opfylde Kundens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger om indsigt i egne oplysninger, udlevering af registreredes oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af registreredes oplysninger, samt Kundens forpligtelser i forhold til underretning af den registrerede ved brud på persondatasikkerheden i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

4.6
Leverandøren skal hjælpe Kunden med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36. jf. Databeskyttelsesforordningens artikel 28, stk. 3, litra f.

4.7.
Leverandøren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Kundens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

4.8.
Leverandøren er forpligtet til at oplyse, med præcise adresseangivelser, hvor Kundens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Kunden ved enhver ændring.

5. Underleverandør (underdatabehandler)

5.1
Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Kunden.

5.2
Leverandøren må ikke uden udtrykkelig skriftlig godkendelse fra Kunden anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Kunden har overladt til Leverandøren i medfør af Abonnementsaftalen. Kunden kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre der foreligger en konkret saglig begrundelse herfor.

5.3.
Hvis Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.

5.4
Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5.5
Når Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kunden ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.

5.6
Kunden kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Kunden.

5.7
Al kommunikation mellem Kunden og underdatabehandler sker via Leverandøren.

6. Instrukser

6.1
Leverandørens behandling af personoplysninger på vegne af Kunden sker udelukkende efter dokumenteret instruks, jf. bilag 3. medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Leverandøren er underlagt; i så fald underretter Leverandøren Kunden om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser. Det er Leverandørens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt. 5.3, får tilsendt Kundens instruks, jf. bilag 3.

6.2
Leverandøren giver omgående besked til Kunden, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 2.2.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1
Leverandøren skal jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

7.2.
Leverandøren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 7.1 samt bilag 1.

7.3.
Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

7.4
Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Kundens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt. 9.

7.5.
Leverandøren er forpligtet til straks at underrette Kunden om ethvert brud på persondatasikkerheden samt ved:

(i) enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed, medmindre orienteringen af Kunden er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,

(ii) anden manglende overholdelse af Leverandørens, samt eventuelle underdatabehandleres forpligtelser

uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

7.6
Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, jf. pkt. 7.5, uden forudgående skriftlig aftale med Kunden om indholdet af en sådan kommunikation, medmindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

8.1
Leverandørens overførsel af personoplysninger til tredjelande (ikke-EU/EØS lande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Kundens instruks herfor, jf. bilag 3.

8.2
Ved overførsel til tredjelande er Leverandøren og Kunden i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.

9. Tavshedspligt og fortrolighed

9.1
Leverandøren er - under og efter Abonnementsaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.

9.2
Leverandøren skal sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

10.1
Leverandøren er forpligtet til at give Kunden nødvendige oplysninger til, at Kunden kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.

10.2
Kunden, en repræsentant for Kunden eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale.

10.3
Leverandøren fremviser årligt Kunden dokumentation på at sikkerhedsforanstaltningerne er iværksat og at der føres tilsyn med at de overholdes, i form af en ISAE 3402 erklæring fra en registreret revisor, jf. bilag 1 punkt 2. Find seneste revisionserklæring her: https://skolevisioner.dk/downloads/revision-og-certificeringer/

10.4
Leverandøren inviterer mindst en gang årligt Kunden til et besøg på Leverandørens adresse. Sammen med Leverandørens øvrige Kunder, vil Kunden få en gennemgang af Leverandørens sikkerhedslogbog og procedurer for det seneste år. Kunden vil i forbindelse med sit besøg kunne foretage en inspektion, stille Leverandøren relevante spørgsmål og komme i dialog med andre af Leverandørens Kunder. Udover Kundens transportudgifter og tidsforbrug er besøget uden yderligere omkostninger for Kunden.

11. Ændringer i Aftalen

11.1
I det omfang ændringer i lovgivningen, jf. pkt. 2.1 og 2.2, eller tilhørende praksis, giver anledning til dette, er Kunden med et varsel på 90 dage og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen.

12. Sletning af data

12.1
Kunden træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Abonnementsaftalen.

12.2
Kunden skal senest 90 dage inden Abonnementsaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal tilbageleveres til Kunden inden sletning. I det tilfælde, hvor personoplysningerne tilbageleveres til Kunden, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Kundens meddelelse. Kundens brugere kan selv hente data i pdf/Word/excel-format.

13. Misligholdelse og tvistigheder

13.1
Misligholdelse og tvistigheder er reguleret i Abonnementsaftalen.

14.Erstatning og forsikring

14.1
Erstatning og forsikring er reguleret i Abonnementsaftalen.

15. Ikrafttræden og varighed

15.1
Aftalen indgås ved begge parters underskrift og løber indtil ophør af Abonnementsaftalen.

16. Formkrav

16.1
Aftalen skal foreligge skriftligt, herunder elektronisk, hos Kunden og Leverandøren.

For Kunden, dato: _____	**For Leverandøren, dato: _____**
Navn:	Navn:
Stilling:	Stilling: Direktør
Tlf. nr.:	Tlf. nr.: 71 99 05 03
Email:	Email: info@klassetrivsel.dk
Underskrift:	Underskrift:
_____	_____

Bilag:
Bilag 1 – Sikkerhed
Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)
Bilag 3 – Instruks

Bilag 1 - Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

2. Sikkerhedskrav

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Det aktuelle tekniske niveau
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)
4. Konsekvenserne for borgerne ved brud på persondatasikkerheden.

5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
    a) tilintetgørelse af oplysningerne
    b) tab af oplysningerne
    c) ændring af oplysningerne
    d) uautoriseret videregivelse af oplysningerne
    e) uautoriseret adgang til oplysningerne

Leverandøren har implementeret en række interne procedurer, der sikrer korrekt håndtering af persondata og personfølsomme oplysninger. Procedurerne er en del af Leverandørens politik for håndtering af informationssikkerhed og persondata, som er godkendt af Leverandørens direktion og som tages op til revurdering af direktionen mindst én gang årligt.

Leverandørens medarbejdere og konsulenter/underleverandører med adgang til personoplysninger, er uddannet i korrekt og sikker håndtering gennem indgående kendskab til virksomhedens sikkerheds- og persondatahåndbøger samt underskrift af hemmeligholdelseserklæring. Alle Leverandørens medarbejdere og konsulenter er underlagt procedurer, der sikrer at personoplysninger udelukkende håndteres med legitime formål.

Al IT-udstyr, der anvendes til håndtering af personoplysninger har installeret software til permanent sletning af filer med personfølsomme oplysninger. Al trådløs kommunikation på interne netværk er krypteret, og der er installeret anti-virus-programmer på alle personlige computere, der anvendes til at håndtere personfølsomme oplysninger. Computere, der indeholder personfølsomme oplysninger opbevares fastlåste, i lokaler der er aflåste og forsynede med alarm, når de ikke benyttes. Drev, der indeholder persondata, slettes permanent før de kasseres eller indsendes til reparation. Al software, der installeres på servere og personlige computere, som anvendes til at håndtere personfølsomme oplysninger er godkendt af den IT sikkerhedsansvarlige. Styresystemer på serverne opdateres mindst hver 14 dag.

Der verificeres minimum hver 30. dag, at produktionsmiljøet og kundernes data kan genskabes. Såfremt en medarbejder hos Leverandøren opdager trusler mod eller brud på informationssikkerheden, meddeler denne dette straks direktionen, som straks derefter iværksætter de fornødne tiltag. Tiltagene er som minimum i overensstemmelse med kravene i gældende persondatalovgivning og sikkerhedsbekendtgørelse.

Der er implementeret fuldautomatisk, overvåget backupsystem, der sikrer at kritiske data automatisk kopieres dagligt fra driftssystemet til mindst 2 andre fysiske lokationer. Backup af data gemmes i mindst 30 dage og slettes efter 3 måneder. Håndtering af backup er omfattet af de samme sikkerhedskrav som resten af systemet. Der testes månedligt, om backup kan bruges til at genskabe produktionsmiljøet.

Der udføres hver måned et sikkerhedsreview, som efterser backup-procedurer, serverkapacitet, sikkerhedsopdateringer og beredskab, samt at der foreligger gyldige og aktuelle aftaler med henholdsvis medarbejdere, konsulenter, samarbejdspartnere og kunder, og at disse er i overensstemmelse med gældende persondatalovgivning.

Der udføres hvert år et sikkerhedsreview, hvor systemer og IT-sikkerhed gennemgås og vurderes i forhold til nye trusler og nyeste viden: Sikkerhedsreviewet indeholder gennemgang af hhv. seneste "OWASP top 10", checkliste til årligt sikkerhedsreview samt en ROS analyse (Risiko- og sårbarhedsanalyse). Deltagerne i det årlige sikkerhedsreview er som minimum den IT-sikkerhedsansvarlige for Leverandøren og en teknisk ekspert med indsigt i IT-sikkerhed.

Der udføres årligt en ekstern revision af sikkerheden hos Leverandøren, som munder ud i en ISAE 3402 Type 2 revisionserklæring – seneste revisionserklæring her:
https://skolevisioner.dk/downloads/revision-og-certificeringer/

Autorisation og adgangskontrol
Alle Leverandørens medarbejdere og konsulenter er underlagt procedurer, der sikrer at personoplysninger udelukkende håndteres med legitime formål. Al tilgang til personoplysninger foregår i inkognito/privat tilstand, i enten Google Chrome, (ny Inkognito-fane (Ctrl+Shift+N)), Mozilla Firefox (nyt privat vindue (Ctrl+Shift+P)), Safari (start privat browsing) eller Internet Explorer (new tab + Start InPrivate Browsing).

Tilgang til personoplysninger finder kun sted, såfremt brugeren er indforstået med at oplysningerne tilgås og/eller såfremt det udelukkende er i Kundens interesse, f.eks. i forbindelse med support eller fejlfinding. Personoplysninger

- udleveres aldrig, med mindre Kunden har givet skriftlig instruks om denne udlevering
- udskrives aldrig på papir
- sendes aldrig via e-mail
- gemmes aldrig i skybaserede systemer.

Der tildeles kun brugerrettigheder når der er tilstrækkelig dokumentation for at rettigheden er legitim.

Alle, der har adgang til personoplysninger, har dette gennem en personlig brugerkonto, som tilhører en institutionskonto. Der er indbyggede mekanismer der sikrer, at den enkelte brugerkonto kun kan tilgå relevante informationer. Den personlige brugerkonto kan tilgås via personligt unilogin (UNI-brugerrolle: 'ansatte på institution') med og/eller personligt brugernavn og password, som oprettes af brugeren i forbindelse med første indlogning med unilogin.

Brugernavne og passwords skal skrives hver gang man som bruger logger ind. Ved gentagne fejlslagne forsøg på login for en brugerkonto låses brugerkontoen i et tidsrum. Passwords, skal bestå af mindst 8 tegn, og indeholde mindst 3 ud af de fire følgende typer tegn: Små bogstaver, store bogstaver, tal og tegn. Brugerpasswords forelægger ikke i klartekst, dvs. password gemmes

krypteret, på en måde der forhindrer, at passwords kan genskabes. Der er ikke mulighed for at anvende "Husk mig" funktioner.

En administrationsbruger på den enkelte institutionskonto har adgang til en liste over brugere på institutionen. Administrationsbrugeren kan se, hvornår de enkelte brugere har været logget ind sidst og kan deaktivere adgange.

Ind- og uddatamateriale som indeholder personoplysninger
Leverandøren leverer en Software-as-a-Service, hvorigennem Kundes medarbejdere (=brugerne af tjenesten) selv administrerer og håndterer ind- og uddatamateriale gennem deres respektive brugerkonti.

Sletning af indhold, herunder personoplysninger, på den enkelte brugerkonto kan udføres af brugeren* selv eller af Leverandøren efter skriftlig instruks fra brugeren / institutionskonto-administrator / Kunden.

Sletning af indhold, herunder personoplysninger på den enkelte institutionskonto foretages af institutionskonto-administrator hos kunden eller af Leverandøren efter skriftlig instruks fra institutionskonto-administrator / Kunden.

Sletning af brugeroplysninger foretages af Leverandøren efter skriftlig instruks fra brugeren / institutionskonto-administrator / Kunden.

*Indhold på en brugerkonto slettes automatisk på slettedato. Slettedatoen sættes automatisk ved oprettelse til 4 år fra oprettelsesdato. Brugeren kan når som helst slette eget indhold eller ændre slettedato for eget indhold. Brugeren kan ikke sætte dato for sletning til mere end 5 år ud i fremtiden eller mindre end dags dato + 1 dag.

Eksterne kommunikationsforbindelser
Leverandørens driftssystemer udveksler data med kundens browser med en SSL-kryptering på mindst 256 bit TLS 1.2. Flytning af data til backup og i forbindelse med fejlsøgning foregår ligeledes altid via en krypteret forbindelse.

Der er opsat firewall på alle driftsservere, der sikrer at der er minimal 'attack-surface' på systemet. Der er lukket for alle unødvendige porte. Øvrige porte er kun åbne for nødvendige IP-adresser. Web-servere er åbne for alle IP-adresser, men kun via SSL-kryptering på mindst 256 bit. Fjernstyring af servere, FTP-adgang, databaseadgang og øvrige porte, der er nødvendige for driften, er kun åbnet for specifikke IP-adresser. Alle øvrige porte er blokerede i firewallen.

Kontrol med afviste adgangsforsøg
Brugernavne og passwords skal skrives hver gang man som bruger logger ind. Ved gentagne fejlslagne forsøg på login for en brugerkonto låses brugerkontoen i et tidsrum. Driftssystemer gemmer brugerpasswords krypteret, på en måde der forhindrer at passwords kan genskabes.

Logning
Der foregår logning af al aktivitet i Leverandørens systemer, inkl. IP-adresser, som aktiviteten foregår fra. Følgende hændelser logges i specifik logfil:

1) Administratorer, der tilgår personfølsomme oplysninger.
2) Brugere, der tilgår personfølsomme oplysninger.

Fejl- og system-logning er bygget ind i systemet. Der logges til en række filer dagligt. Disse filer er delt op i 5 typer: Debug, Error, Event, Performance, ParticipantLogin.
Disse er alle sammen en del af backup-proceduren. Logfiler opbevares i 6 måneder.

Hjemmearbejdspladser
Leverandørens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser:
□ Ja
X Nej

Bilag 2 - Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen
Der er sikret separation af de enkelte kunders data, som opbevares på hostede servere hos Leverandøren hosting partner Tilaa B.V., Westdam 3-J, 3441 GA, Woerden, Holland. Se pkt. 2.

Driftssystemer og applikationer udvikles i samarbejde med CreativeMinds IVS. Se pkt. 2.

Leverandørens medarbejdere håndterer brugersupport og fejlfinding fra Leverandørens adresse: Skolevisioner ApS, Ry Væksthus, Ellemosen 3, 8680 Ry.

2. Underdatabehandlere
Leverandøren anvender kun hostingcentre, der kan dokumentere høj grad af sikkerhed, gennem enten en ISO 27001 certificering eller en ISAE3402 revisionserklæring.

Der indgås databehandleraftale mellem hostingudbyder og Leverandøren. Der anvendes udelukkende EU-baserede hostingpartnere.

Leverandøren har indgået databehandleraftale med den nuværende hosting partner, Tilaa, som har det krævede certificeringsniveau https://skolevisioner.dk/downloads/revision-og-certificeringer/

Udvikling af driftssystemer og kunderettede applikationer udføres i samarbejde med CreativeMinds IVS i Randers, som derfor har indgået databehandleraftale og udvidet hemmeligholdelsesaftale med Leverandøren.

Underdatabehandleraftaler findes her: https://skolevisioner.dk/downloads/underdatabehandlere/

Bilag 3 - Instruks

Kunden instruerer hermed Leverandøren om at foretage behandling af Kundens oplysninger til brug for drift og levering af Klassetrivsel, jf. Abonnementsaftale om abonnement på Klassetrivsel. Leverandøren er ansvarlig for, at Kundens instruks fremsendes til eventuelle underdatabehandlere.

1.1 Behandlingens formål
Behandling af Kundens oplysninger sker i henhold til formålet i Abonnementsaftalen. Leverandøren må ikke anvende oplysningerne til andre formål. Oplysningerne må ikke behandles efter instruks fra andre end Kunden.

1.2 Generel beskrivelse af behandlingen
Leverandøren udvikler, drifter og udbyder applikationer til arbejdet med trivsel, relationer og kvalitetsudvikling. Applikationerne udbydes som SaaS (Software-as-a-Service) og er integrerede med Styrelsen for It og Lærings UNI-Login-infotjeneste samt Styrelsen for It og Lærings UNI-Login-webservice.

Al behandling af personoplysninger omfattet af denne aftale sker gennem Software-as-a-Service-systemet Klassetrivsel - et digitalt trivselsværktøj, som anvendes af Kundens medarbejdere, og som Kundens medarbejdere tilgår med personligt login og gennem medarbejderens browser. Iht. Abonnementsaftalen bruges Klassetrivsel af Kundens medarbejdere til gennemførsel af trivselsundersøgelser.

Hvor Abonnementsaftalen omfatter det, benytter Kunden desuden Klassetrivsel til gennemførsel af den nationale trivselsmåling iht. BEK nr. 1167 af 12/10/2015: Bekendtgørelse om måling af elevernes trivsel i folkeskolen (https://www.retsinformation.dk/Forms/R0710.aspx?id=174664). Leverandøren indsender derfor de til den nationale trivselsmåling indsamlede trivselsdata til Styrelsen for IT og Læring iht. instruks i bekendtgørelsens bilag 3:
https://www.retsinformation.dk/Forms/R0710.aspx?id=174664#id022b531c-d08f-4027-954c-d1decc8ce341

1.3 Typen af personoplysninger
Behandlingerne kan indeholde personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Almindelige personoplysninger jf. Persondatalovens § 6, jf. Databeskyttelsesforordningens artikel 6)
X Almindelige personoplysninger

1.4 Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede: Ansatte, børn og unge på Kundens institutioner.

1.5 Tredjelande (ikke-EU/EØS-medlemslande)
Leverandøren overfører ikke personoplysninger til tredjelande.