

Standardkontraktbestemmelser

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

mellem

CVR

herefter "den dataansvarlige"

og

Skolevisioner ApS
CVR 30535421
Ry Væksthus
Ellemosen 3
8680 Ry

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

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

1. Indhold

2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	5
7. Anvendelse af underdatabehandlere	6
8. Overførsel til tredjelande eller internationale organisationer	7
9. Bistand til den dataansvarlige	8
10. Underretning om brud på persondatasikkerheden	9
11. Sletning og returnering af oplysninger	9
12. Revision, herunder inspektion	10
13. Parternes aftale om andre forhold	10
14. Ikrafttræden og ophør	10
15. Kontaktpersoner hos den dataansvarlige og databehandleren	11
Bilag A Oplysninger om behandlingen	12
Bilag B Underdatabehandlere	14
Bilag C Instruks vedrørende behandling af personoplysninger	15
Bilag D Parternes regulering af andre forhold	22

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).
3. I forbindelse med leveringen af Klassesettrivsel.dk behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

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

5. Fortrolighed

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

6. Behandlingssikkerhed

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

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

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

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
6. 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 underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

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

9. Bistand til den dataansvarlige

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

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - c. indsigtsretten
 - d. retten til berigtigelse
 - e. retten til sletning ("retten til at blive glemt")
 - f. retten til begrænsning af behandling
 - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
 - a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

- d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 36 TIMER efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil. Ønsker Dataansvarlige en genforhandling af Bestemmelserne af andre årsager, modtager Dataansvarlige en faktura på de timer Databehandler har forbrugt på opgaven/arbejdet.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er returneret og/eller slettet til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige

Navn
Stilling
Telefonnummer
E-mail
Dato
Underskrift

På vegne af databehandleren

Navn	Lars du Jardin Nielsen
Stilling	Direktør
Telefonnummer	7199 0862
E-mail	lars@skolevisioner.dk
Dato	
Underskrift	

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Navn
Stilling
Telefonnummer
E-mail

Navn	Hjørdis Guldmand
Stilling	Administration
Telefonnummer	7199 0503
E-mail	info@klassetrivsel.dk

Bilag A Oplysninger om behandlingen

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

Indsamling af trivselsdata med henblik på at iværksætte indsatser for at forbedre trivslen.
 Behandling af Dataansvarliges oplysninger sker i henhold til formålet i Hovedaftalen.
 Databehandler må ikke anvende oplysningerne til andre formål.
 Oplysningerne må ikke behandles efter instruks fra andre en Dataansvarlige.

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

Databehandler udvikler, drifter og udbyder applikationer til arbejdet med trivsel, relationer og kvalitetsudvikling. Applikationerne udbydes som SaaS (Software-as-a-Service) og er integrerede med STIL, Styrelsen for It og Lærings UNI-Login-infotjeneste samt Styrelsen for It og Lærings UNI-Login-webservice og Brugerportalinitiativets webservices.

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

Klassetrivsel understøtter de 3 nyeste versioner af alle de almindelige desktop-browsere. Benyttes en ældre browser eller en browsertype, som ikke er på listen, kan det ikke garanteres, at klassetrivsel fungerer optimalt. Klassetrivsel understøtter ikke beta, developer, nightly, canary eller andre typer af pre-release versioner af browsere.
 Hvis en forældet browserversion benyttes, kan Klassetrivsel ikke yde support.

Understøttede browsere:

- Google Chrome
- Safari
- Edge
- Firefox

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

Medarbejdere: Navn, Uni-id, e-mailadresse og arbejdssted (Skole), evt. telefonnummer.

Elever: Navn, Uni-id, Klasse, Skole hentes via STIL og elevsvar.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Ansatte, børn og unge på Dataansvarliges institutioner.

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

Så længe Hovedaftalen mellem Skolevisioner ApS og Dataansvarlige og Dataansvarliges skoler er gældende

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Tilaa B. V.	KVK 59712309	Willemsplein 8E, 5211 AK's- Hertogenbosch, Holland	Hostingselskab
CreativeMinds ApS	3765 9223	Kærgade 33, 8940 Randers SV	Udvikling og vedligeholdelse af driftssystemer og kunderettede applikationer.

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

Link til databehandleraftale med underdatabehandlere:

<https://skolevisioner.dk/downloads/underdatabehandlere/>

B.2. Varsel for godkendelse af underdatabehandlere

Planlagte ændringer vedrørende tilføjelser eller udskiftning af underdatabehandlere meddeles den dataansvarlige med mindst 30 dages varsel jf. bestemmelse 7.3.

Der skal foreligge en konkret saglig begrundelse for ikke at godkende en udskiftning af en underdatabehandler.

Underdatabehandleraftaler findes her:

<https://skolevisioner.dk/downloads/underdatabehandlere/>

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

- Medarbejder kan opsætte undersøgelser
- Eleverne besvarer spørgsmål
- Databehandler illustrerer besvarelsener i forskellige diagramtyper
- Data slettes af brugeren eller databehandler efter en given aftale opbevaringsperiode.
- Derudover kan der dannes grupper ud fra gennemførte undersøgelser

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

- Typerne af behandlede personoplysninger og kategorierne af registrerede personer jf. Punkt A.3 og A.4
- Omfanget af personoplysninger (antal oplysninger pr. registrerede samt antallet af registrerede)
- Behandlingens karakter jf. punkt A.2
- Varigheden af behandlingen jf. Punkt A.5

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

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

Risikovurdering

Databehandler skal kunne dokumentere en regelmæssigt opdateret risikovurdering i forhold til den databehandling, som foretages for den dataansvarlige.

Databehandler skal minimum én gang årligt gennemgå risikovurderingen og vurdere og evaluere effekten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

Risikovurderingen skal som minimum opdateres i forbindelse med forestående ændringer af egne organisatoriske forhold, forestående ændringer af en eventuel underleverandørs forhold eller forestående ændringer af anvendt teknologi og infrastruktur herunder udstyr.

Autorisation og adgangskontrol

Databehandleren skal sikre, at kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles på vegne af den dataansvarlige.

Databehandleren må kun autorisere personer, der er beskæftiget med de formål, hvortil oplysningerne behandles jf. punkt C.1. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har specifikt behov for i forbindelse med aftalens opfyldelse. Databehandler skal løbende sikre og dokumentere, at de autoriserede brugere fortsat opfylder dette krav. Kontrol heraf skal foretages mindst én gang hvert halve år.

Ud over ovennævnte må databehandleren endvidere autorisere brugere, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver i forbindelse med aftalens opfyldelse.

Databehandleren skal ved medarbejderes fratrædelse have en procedure, der sikrer, at brugernes systemrettigheder ophører, herunder at it-udstyr inddrages.

Databehandlerens overholdelse af ovenstående skal dokumenteres.

Adgangskoder

Databehandleren skal have formelle procedurer for udstedelse og håndtering af adgangskoder for adgang til personoplysninger, der behandles i henhold til denne aftale.

Den autoriserede bruger udstyres med en personlig brugeridentifikation og en personlig adgangskode, der skal anvendes hver gang, brugerne får adgang til databehandlingen. Adgangskoder skal have en tilstrækkelig længde og kompleksitet og skal skiftes minimum hvert halve år.

Databehandleren skal have procedure for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

Awareness

Databehandleren skal sørge for, at dennes medarbejdere modtager den tilstrækkelige uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Databehandlerens politikker og procedurer herfor.

Beredskabsplaner

Databehandleren forpligter sig til at have et beredskab, der sikrer, at konsekvenserne af driftsafbrydelser som følge af eksempelvis et DDos-angreb eller nedbrud på forsyningsnetværket begrænses mest muligt.

Interne sikkerhedsbestemmelser

Databehandlerens interne sikkerhedsbestemmelser skal omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Databehandleren skal endvidere fastsætte instrukser, som fastlægger ansvaret for og beskriver behandlingen og destruktion af ind- og uddatamaterialer samt anvendelse af it-udstyr. Desuden skal Databehandleren fastsætte retningslinjer for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, som er fastsat.

Adgang til oplysninger via internettet

It-systemer eller portaler med netadgang, som indeholder følsomme eller fortrolige personoplysninger, skal have to-faktor-validering og relevant kryptering.

Ved netværkssikkerhedsbrud har databehandleren indberetningspligt til den dataansvarlige strakt der opdages virusangreb, uautoriseret indtrængen (hacking) eller ændring af data.

Beskyttelse af oplysninger under transmission

Databehandleren må kun anvende eksterne kommunikationsforbindelser til behandling af personoplysninger for den dataansvarlige, hvis der træffes tilstrækkelige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til oplysningerne

Databehandleren anvender HTTPS som end-to-end kryptering ved beskyttelse af oplysninger under transmission.

Beskyttelse af oplysninger under opbevaring

Der skal være etableret antivirus og firewall på databehandlerens udstyr og disse skal løbende holdes opdaterede gennem fastlagte procedurer.

Databehandleren bør som udgangspunkt ikke benytte bærbare medier herunder USB-nøgler eller eksterne harddiske. Såfremt det ikke kan undgås, skal databehandleren sikre, at det bærbare medie er passende krypteret.

Test og udvikling

Personoplysninger behandles aldrig i udviklings- og testmiljøer. Fravigelse herfra kræver særskilt aftal med den dataansvarlige.

Fysisk sikring

Databehandler skal sikre, at uvedkommende ikke får adgang til lokaliteter, hvor der behandles personoplysninger på vegne af den dataansvarlige.

Hjemmearbejdspladser

Databehandleren skal fastsætte særlige retningslinjer for behandling af personoplysninger, der finder sted på en arbejdsplads uden for databehandleren lokaliteter (fjernarbejdsplads), herunder kryptering, VPN og/eller to-faktor-autentifikation.

Backup og logning

Databehandler sikrer passende backup af data, der behandles på den dataansvarliges vegne, så risikoen for tab minimeres. Det skal regelmæssigt sikres, at backups kan genindlæses.

Databehandler har en proces, der sikrer at personoplysninger kan slettes fra backuppen eller som minimum en proces, der sikrer, at backuppen ikke kan genindlæses uden at sikre fornyet sletning af personoplysningerne.

Der gælder samme instruks for backups som for al anden behandling af personoplysninger i medfør af denne aftale.

Databehandleren skal foretage logning af alle anvendelser, adgange, ændringer og søgninger af personoplysninger i relation til aftalens opfyldelse med angivelse af tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører eller det anvendte søgekriterium.

Loggen skal efter aftale kunne stilles til rådighed for den dataansvarlige i et umiddelbart læsbart format.

Logningen skal opbevares i 6 måneder, med mindre andet er aftalt med den dataansvarlige. Databehandleren skal på anmodning uden unødigt ophold levere logdata til den dataansvarlige eller til Datatilsynet.

C.3 Bistand til den dataansvarlige

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

Databehandler skal hjælpe den dataansvarlige med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36, jf. Databeskyttelsesforordningens artikel 28, stk. 3, litra f.

Den registreredes rettigheder

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

Sikkerhedsbrud

Databehandleren skal have etableret en procedure for rapportering af sikkerhedshændelser, der sikrer, at databehandler kan rapportere hændelsen til den dataansvarlige inden for 36 timer efter at databehandler har fået kendskab til hændelsen.

C.4 Opbevaringsperiode/sletterutine

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

Databehandleren kan i en periode på op til 3 måneder efter databehandlingens ophør afvente sletning af backupsystemer. Databehandleren må i denne periode ikke genindlæse data. Eventuel backup skal slettes senest 3 måneder efter databehandlingens ophør. Logfiler skal slettes senest 6 måneder efter sidste behandling.

C.5 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden forudgående orientering af den Dataansvarlige ske på andre lokaliteter end følgende:

Databehandler:

Skolevisioner ApS

Ry Væksthus, Ellemosen 3, 8680 Ry

Underdatabehandlere:

CreativeMinds ApS

Kærgade 33, 8940 Randers SV

Tilaa B.V:

J.W. Lacasweg 35, 2031BE, Haarlem, Holland

Kabelweg 48, 1014BB, Amsterdam, Holland

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandler overfører ikke data til tredjelande.

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

Databehandleren skal én gang 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 revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE 3000

Revisionserklæringen fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i revisionserklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

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 har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt.

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

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

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

Databehandleren skal føre relevant tilsyn med underdatabehandlere.

Dokumentation for tilsyn med underdatabehandlere skal kunne fremvises for den dataansvarlige i forbindelse med dennes tilsyn med databehandler.

Baseret på resultaterne af tilsynet 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.

Dokumentation for tilsyn kan hentes på <https://skolevisioner.dk/downloads/revision-og-certificeringer/>. Den Dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Den Dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser.

Bilag D Parternes regulering af andre forhold