Ullits & Winther

Skolevisioner ApS

Ellemosen 3

8680 Ry

CVR nr. 30 53 54 21

ISAE 3000

Uafhængige revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Skolevisioner ApS' kunder

1. juli 2024 – 30. juni 2025

Indholdsfortegnelse

1. Ledelsens udtalelse

Skolevisioner ApS behandler personoplysninger på vegne af Skolevisioner ApS' kunder og deres revisorer i henhold til databehandleraftale og i relation til indgåede aftaler mellem Skolevisioner ApS og deres kunder. Behandlingen af personoplysninger foregår i Skolevisioners software-as-a-service; Klassetrivsel.

Skolevisioner anvender kun følgende to underdatabehandlere, som ikke benytter underdatabehandlere:

- CreativeMinds ApS – udvikling og vedligehold af driftssystemer og kunderettet applikationer
- Tilaa B.V. – hostingselskab.

Medfølgende beskrivelse er udarbejdet til brug for Skolevisioner ApS' kunder, der har anvendt Klassetrivsel til skolernes trivselsarbejde, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt. Skolevisioner ApS bekræfter, at:

a) Den medfølgende beskrivelse, side 6-10, giver en retvisende beskrivelse af Klassetrivsel, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 1. juli 2024 til 30. juni 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   i) Redegør for, hvordan Klassetrivsel var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
   - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved

hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

- Kontroller, som vi med henvisning til systemernes afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

ii) Indeholder relevante oplysninger om ændringer ved databehandlerens software-as-a-service til behandling af personoplysninger foretaget i perioden fra 1. juli 2024 til 30. juni 2025

iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne software-as-a-service til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved den leverede software-as-a-service, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. juli 2024 til 30. juni 2025. Kriterierne anvendt for at give denne udtalelse var, at:

i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. juli 2024 til 30. juni 2025.

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Ry, den. 12. september 2025

Skolevisioner ApS

Lars du Jardin Nielsen
Direktør

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Skolevisioner ApS' kunder.

Til ledelsen hos Skolevisioner ApS, Skolevisioner ApS' kunder og deres revisorer.

Vi har fået som opgave at afgive erklæring om Skolevisioner ApS' systembeskrivelser i afsnit 3 "Systembeskrivelse Skolevisioner ApS" i henhold til databehandleraftalen med Skolevisioner ApS' kunder som dataansvarlig, i hele perioden fra 1. juli 2024 til 30. juni 2025 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion i erklæringen udtrykkes med høj grad af sikkerhed.

Vores erklæring og beskrivelsen af test af kontroller på side 11-33 er udelukkende tiltænkt dataansvarlige, der har anvendt Klassetrivsel, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Ledelsens ansvar

Skolevisioner ApS er ansvarlig for udarbejdelsen af beskrivelsen side 6-10, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors ansvar

Det er vores ansvar på grundlag af det udførte arbejde at udtrykke en konklusion om Skolevisioner ApS' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på, at opnå høj grad af sikkerhed for vores konklusion.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountant's internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Vores gennemgang har haft til formål at konstatere, hvorvidt beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af Klassetrivsel samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet på side 6-10.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en databehandler

Skolevisioner ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Klassetrivsel, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af Klassetrivsel, således som denne var udformet og implementeret i hele perioden fra 1. juli 2024 til 30. juni 2025, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, der knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. juli 2024 til 30. juni 2025, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. juli 2024 til 30. juni 2025.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår på side 11-33.

Viborg, den 12. september 2025

Ullits & Winther
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 09 32 72

Lasse Lei Kjærsgaard
statsautoriseret revisor
mne42772

3. Systembeskrivelse Skolevisioner ApS

3.1 Organisation og ansvar

Et medlem af direktionen er udpeget som IT-sikkerhedsansvarlig hos Skolevisioner ApS, men direktionen som helhed er øverste ansvarlig for håndtering af IT-sikkerhed og persondata i virksomheden.

De medarbejdere og konsulenter*, som varetager daglig support og kundekontakt, kan have adgang til persondata og personhenførbare oplysninger. Derfor er disse medarbejdere og konsulenter uddannet i korrekt og sikker håndtering af persondata og personhenførbare oplysninger gennem indgående kendskab til virksomhedens sikkerheds- og persondatahåndbøger samt underskrift af hemmeligholdelseserklæring.

* se underafsnittet i 'Udvikling i afsnittet 'Driftssystemer'.

3.2 Interne procedurer

Der er implementeret en række interne procedurer, der sikrer korrekt håndtering af persondata og personhenførbare oplysninger. Procedurerne er en del af virksomhedens politik for håndtering af informationssikkerhed og persondata, som er beskrevet i virksomhedens sikkerheds- og persondatahåndbog.

Virksomhedens sikkerheds- og persondatahåndbog er godkendt af direktionen, og virksomhedens politik for håndtering af informationssikkerhed og persondata tages op til revurdering af direktionen mindst én gang årligt.

3.2.1 Håndtering af persondata og personhenførbare oplysninger

Alle medarbejdere og konsulenter er underlagt procedurer, der sikrer at persondata og personhenførbare oplysninger udelukkende håndteres med legitime formål.

Al tilgang til kundernes persondata foregår kun gennem Skolevisioners ApS' udstyr og kun gennem browsere i inkognito/privat tilstand i følgende browsere:

1. *Google Chrome: Ny Inkognito-vindue (Ctrl+Shift+N)*
2. *Mozilla Firefox: Nyt privat vindue (Ctrl+Shift+P)*
3. *Safari: Start privat browsing*
4. *Microsoft Edge: Nyt InPrivate-vindue (Ctrl+Shift+N)*

Tilgang til personhenførbare oplysninger finder kun sted, såfremt kunden/dataejer er indforstået med, at oplysningerne tilgås og/eller såfremt det udelukkende er i kundens/dataejers interesse, f.eks. i forbindelse med support eller fejlfinding.

Personhenførbare oplysninger

- udleveres aldrig, med mindre dataejer har givet skriftlig instruks om denne udlevering.
- udskrives aldrig på papir
- sendes aldrig via e-mail
- gemmes aldrig i skybaserede systemer
- Benyttes aldrig i testmiljø eller til test i anden sammenhæng.

Der tildeles kun brugerrettigheder til brugere af virksomhedens systemer, når der er tilstrækkelig dokumentation, for at rettigheden er legitim.

Alle kunder informeres om krav til indgåelse af databehandleraftale med Skolevisioner ApS.

Fortrolige og personhenførbare oplysninger om hhv. ansatte i Skolevisioner ApS samt Skolevisioner ApS' samarbejdspartnere opbevares aflåst i brandsikret skab på virksomhedens adresse, som er forsynet med alarm.

3.2.2 Backup

Der er implementeret fuldautomatisk, overvåget backupsystem, der sikrer, at kritiske data automatisk kopieres dagligt fra driftssystemet til en anden fysiske lokation. 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 dagligt, om backup kan bruges til at genskabe produktionsmiljøet og kundernes data.

3.2.3 Ugentligt sikkerhedsreview

Der udføres et ugentligt sikkerhedsreview. Det ugentlige sikkerhedsreview sikrer, at de organisatoriske sikkerhedsforanstaltninger til stadighed overholdes, bl.a. at opdateringer bliver foretaget, brugen af File Shredder i forhold til sletning af downloadede filer, at antivirusprogrammer er kørende og opdaterede, samt oprydning på PC'er er foretaget.

3.2.4 Månedligt sikkerhedsreview

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.

3.2.5 Årligt sikkerhedsreview

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 Skolevisioner ApS og en teknisk ekspert med indsigt i IT-sikkerhed.

3.2.6 Beredskab

Der verificeres dagligt, at kundernes data kan genskabes fra backup og det tjekkes løbende, at produktionsmiljøet kan genetableres

Såfremt en medarbejder/konsulent opdager trusler mod eller brud på informationssikkerheden, meddeler denne dette straks direktionen. Direktionen iværksætter straks derefter de fornødne tiltag. Tiltagene er som minimum i overensstemmelse med kravene i gældende persondatalovgivning.

3.3 Internt hardware & software

Al IT-udstyr, der anvendes til håndtering af persondata, har installeret software til permanent sletning af filer med personhenførbare 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 personhenførbare oplysninger.

Computere, der indeholder personhenførbare oplysninger opbevares fastlåste, i lokaler der er aflåste og forsynet med alarm, når de ikke benyttes. Drev, der indeholder persondata, slettes permanent før de kasseres eller indsendes til reparation.

Til daglig indeholder fysiske drev ikke persondata. I de tilfælde, hvor det findes nødvendigt, er der indarbejdet fast procedure for håndteringen af persondata på fysiske drev, som omfatter procedure for sletning af persondata, når det ikke længere findes nødvendigt, at de er gemt på fysiske drev. Persondata er derfor typisk kun gemt på fysiske drev i én arbejdsdag og sker udelukkende i forbindelse med support af brugere.

Al software, der installeres på servere og personlige computere, som anvendes til at håndtere personhenførbare oplysninger er godkendt af den IT sikkerhedsansvarlige.

3.4 Driftssystemer

Styresystemer på serverne opdateres mindst hver 14 dag.

3.4.1 Kryptering

Driftssystemer udveksler data med kundens browser SSL-kryptering på mindst 256 bit. Ved flytning af data til backup og i forbindelse med fejlsøgning er data altid krypteret.

3.4.2 Firewall

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. FTP-adgang, databaseadgang og øvrige porte, der er nødvendige for driften, er kun åbnet for specifikke IP-adresser. Ved fjernstyring af servere er der kun med to-faktor-login. Alle øvrige porte er blokerede i firewallen.

3.5 Kunderettede applikationer

Skolevisioner ApS udvikler og udbyder applikationer til arbejdet med trivsel, relationer og kvalitetsudvikling. Applikationerne udbydes som SaaS (Software-as-a-Service). De danske applikationer er integrerede med Styrelsen for It og Lærings UNI-Login-infotjeneste samt Styrelsen for It og Lærings UNI-Login-webservice, mens de norske applikationer på tilsvarende måde er integrerede med FEIDE/SIKT.

3.5.1 Logning

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

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

Desuden har systemet en fejl- og system-log, der indeholder tekniske informationer om systemet. Informationerne i denne log, er ikke direkte bundet op på en bruger.

Disse er alle sammen en del af backup-proceduren.

3.5.2 Håndtering af brugeradgange og passwords

Alle, der har adgang til personhenførbare oplysninger, har dette gennem en personlig brugerkonto. 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.

Passwords, der anvendes til beskyttelse af personhenførbare oplysninger, 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 foreligger 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. 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.

Hver kunde har administrationsbrugere, som kan se, hvornår de enkelte brugere har været logget ind sidst, kan deaktivere adgange og tildele roller med tilhørende rettigheder.

3.5.3 Sletning af brugere og indhold på bruger- og institutionskonti

Sletning af brugeroplysninger og sletning af alt eller udvalgt indhold på en brugerkonto eller på kundens konto/konti kan foretages af kunden selv eller af Skolevisioner ApS iht. skriftlig instruks fra kunden (brugeren/dataansvarlig).

3.5.4 Opbevaring af data

Der er sikret separation af de enkelte kunders data bl.a.

- ved at hver bruger har en personlig brugerkonto
- gennem systemets arkitektur, hvor større kunder f.eks. en kommune har eget site med egne data, mens mindre kunder f.eks. en skole er samlet i grupper på sites med tilhørende data.

Kundernes data opbevares på hostede servere hos Skolevisioner ApS' hosting partner Tilaa B.V. i Holland.

Skolevisioner ApS anvender kun hostingcentre, der kan dokumentere høj grad af sikkerhed, gennem enten en ISO 27001 certificering eller en ISAE3402 revisionserklæring. Der indgås en specifik databehandleraftale mellem hostingudbyder og Skolevisioner ApS. Der anvendes udelukkende EU/EØS-baserede hostingpartnere.

Der er indgået databehandleraftale med nuværende, og i revisionsperiodens eneste hostingpartner, Tilaa B.V., som har det krævede certificeringsniveau (https://www.tilaa.com/en/stable-and-safe).

3.6 Udvikling

Udvikling af driftssystemer og kunderettede applikationer er outsourcet til Creativeminds ApS i Randers, som har indgået databehandleraftale og udvidet hemmeligholdelsesaftale med Skolevisioner ApS. CreativeMinds ApS i Randers er og har i revisionsperioden været, Skolevisioner ApS' eneste leverandør af udviklingsressourcer, som har adgang til driftssystemer.

3.7 Tilsyn med underdatabehandlere

Skolevisioner ApS anvender, som nævnt i afsnit 3.5.4 "Opbevaring af data" og afsnit 3.6 "Udvikling", Tilaa B.V. og CreativeMinds ApS som underdatabehandlere.

Tilaa B.V. tillader ikke adgang til deres fysiske faciliteter af hensyn til sikkerheden. Skolevisioner ApS har derfor ikke mulighed for at føre fysisk tilsyn med Tilaa B.V. Skolevisioner ApS kontrollerer årligt, at Tilaa B.V. er ISO 27001 certificeret.

Skolevisioner ApS udfører, i overensstemmelse med Bilag B i den indgåede underdatabehandleraftale med CreativeMinds ApS, minimum et årligt fysisk tilsyn omkring overholdelse af indgået underdatabehandleraftale. En repræsentant fra CreativeMinds ApS deltager desuden i Skolevisioner ApS månedlige og årlige sikkerhedsreviews.

3.8 Persondataforordning

25. maj 2018 trådte den nye EU-forordning om håndtering af Persondata (GDPR) i kraft. Skolevisioner ApS har i perioden op til ikrafttrædelsen af forordningen, implementeret denne, således at kravene i forordningen er efterlevet fra ikrafttrædelsen af forordningen.

I denne forbindelse har Skolevisioner ApS benyttet sig af assistance og rådgivning fra REVI-IT, som er et statsautoriseret revisionsfirma med speciale i IT-revision og overholdelse af databeskyttelsesforordningen.

Revi-IT gennemgik og vurderede Skolevisioner ApS' produktstandard, sikkerhedsprocedurer samt behandling af personoplysninger op mod kravene i databeskyttelsesforordningen. Herudfra blev der også foretaget en vurdering af, hvorvidt Skolevisioner ApS bør og/eller er forpligtet til at udpege en databeskyttelsesrådgiver iht. databeskyttelsesforordningen. Skolevisioner ApS blev rådet til ikke at udpege en databeskyttelsesrådgiver, idet Skolevisioner ApS, i rollen som databehandler, udelukkende behandler personoplysninger iht. en instruks fra dataansvarlig, som ikke medfører opfyldelse af betingelserne for krav om en databeskyttelsesrådgiver. Ej heller i rollen som dataansvarlig opfylder Skolevisioner ApS betingelserne.

4. Kontrolmål og test af kontrolmål

Kontrolmål A **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. Der er implementeret politik der sikrer at tilgang til og redigering af personoplysninger udelukkende finder sted i kundens direkte interesse.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks og at instruks findes i databehandleraftalerne. Vi har inspiceret, at Persondatahåndbogen og årsreview dokument indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Vi har inspiceret, at Persondatahåndbogen er opdateret den 4.6.2025 og årsreview dokumentet er opdateret den 5.6.2025. Vi har forespurgt og inspiceret, at der i virksomheden er implementeret en politik omkring tilgang og manipulation af personhenførbare oplysninger. Vi finder denne politik hensigtsmæssig beskrevet i persondata håndbogen.	Ingen afvigelser konstateret.

A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. Der er indgået databehandleraftaler med alle kunder.	Vi har inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Systemet Klassetrivsel er opbygget sådan at det er kunden selv som foretager behandling af persondata. Skolevisioner behandler kun persondata efter instruks ved support og dette udføres som udgangspunkt i pseudonymiseret form. Vi har ved en stikprøve i systemet Audit trail inspiceret, at afgivne instrukser fra dataansvarlig logges. Det er ved stikprøve inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks i databehandleraftaler. Vi har ved stikprøve inspiceret, at der er indgået databehandleraftaler med alle kunder. Dette oplyses endvidere i betingelserne, bl.a. abonnementsvilkår for brug af Skolevisioner ApS produkter. Vi har ved stikprøver i databehandleraftaler inspiceret at det fremgår at databehandling kun foretages efter instruks.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har forespurgt og inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har på forespørgsel fået oplyst, at der ikke har været en situation, hvor en instruks har være i strid med databeskyttelsesforordningen, hvorfor procedure ikke kan efterprøves.	Ingen afvigelser konstateret. Ingen situation. Derfor ikke muligt at efterprøve.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**B**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos relevante personer. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Vi har inspiceret at procedurerne i Persondatahåndbogen er opdaterede, og at opdatering senest er foretaget 4.6.2025. Vi har ved en stikprøve på databehandleraftaler inspiceret, at der er etableret de aftalte sikringsforanstaltninger.	Ingen afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Vi har inspiceret, at den foretagne risikovurdering er opdateret juni 2025 og at risikoniveau findes ved at gange sandsynligheden med konsekvens og omfatter den aktuelle behandling af personoplysninger. Vi har inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Vi har gennemgået forretningsgang for sikkerhedsforanstaltninger Vi har ved stikprøve inspiceret at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**B**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B2.1	Databehandleren har etableret en fortegnelse over behandlingsaktiviteter. Fortegnelsen opdateres løbende, dog min. en gang årligt.	Vi har inspiceret fortegnelsen over behandlingsaktiviteter og observeret, at den indeholder de krævede oplysninger. Vi har inspiceret at årsreview indeholder procedure der sikrer at fortegnelsen min. en gang årligt opdateres. Fortegnelsen er senest opdateres 27.5.2025.	Ingen afvigelser konstateret.
B.3	Der er installeret et anerkendt antivirusprogram på alle personlige computere, der anvendes til håndtering af personhenførbare oplysninger.	Vi har observeret, at der er installeret anerkendt antivirusprogram på personlige computere samt forespurgt medarbejdere om den daglige anvendelse af programmet- Vi har observeret, at antivirus software er opdateret, og har fået oplyst, at nyeste version automatisk opdateres på alle maskiner.	Ingen afvigelser konstateret.
B.4	Der er implementeret firewall på driftsservere, der sikrer, at der kun er åbnet op for relevante porte og IP-adresser.	Vi har observeret opsætningen af firewall, samt gennem forespørgsel sikret os, at der kun er åbnet op for relevante porte og IP-adresser.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har udført forespørgsel hos relevante personer. Vi har observeret i siteadmin, at systemet er opdelt i selvstændige systemer, så hver kunder kun har adgang til egne data via segmentering på subdomæner og top-domæner.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**B**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor. Driftssystemer kræver anvendelse af avancerede passwords af brugerne. Der kan i driftssystemerne ikke anvendes "Husk Mig" funktioner. Brugerpasswords i produktionssystemer gemmes i krypteret form, der umuliggør genskabelse.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger, og at der løbende sker opfølgning på rette adgange til rette brugere. Vi har observeret og sikret os, at virksomhedens driftssystemer kræver anvendelse af avancerede password. Vi har forespurgt og observeret, at virksomhedens driftssystemer ikke anvender "Husk Mig" funktioner. Vi har forespurgt og observeret, at brugerpasswords gemmes i krypteret form, samt at den krypteringsform umuliggør genskabelse.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har observeret, at systemet har eventlog og request log, som altid er aktiv. Vi har ved inspektion set eksempler på alarmer. Vi er på forespørgsel blevet informeret om, at der ikke har været en situation, hvor den dataansvarlige skulle informeres om en alarm, hvorfor procedure ikke kan efterprøves	Ingen afvigelser konstateret Ingen hændelse. Derfor ikke muligt at efterprøve.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail. Driftssystemer fungerer ved hjælp af en krypteret forbindelse.	Vi har inspiceret, at informationssikkerhedspolitikken fastsætter, at dataudveksling af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**B**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Vi har forespurgt og fået oplyst, at der ikke anvendes trådløse forbindelser. Ledelsen har overfor os bekræftet, at al udveksling med den dataansvarlige browser foregår med SSL-kryptering på mindst 256 bit. Vi har forespurgt om og fået bekræftet, at løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Vi er informeret om, at der ikke har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden.	
B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold: ● Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder ● Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende ● Der foretages logning af tilgang til personhenførbare oplysninger i produktionssystemer ● Brugerkontoer låses ved gentagne fejlslagne loginforsøg ● Administrator-brugere hos kunder har oversigt over hvilke brugere der har adgang, og har mulighed for at deaktivere adgangen for udvalgte brugere	Vi har inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Vi har observeret og efter gennemgang med medarbejdere og ledelse sikret os, at der sker logning i forbindelse med tilgang til personhenførbare oplysninger. Al aktivitet i forbindelse med personhenførbare oplysninger bliver logget	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**B**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Vi har observeret og sikret os, at brugerkonti låses ved gentagne fejlslagne loginforsøg. Vi har forespurgt medarbejdere og ledelsen om de systemrettigheder og -funktioner (handlinger), der er for administratorbrugere hos kunderne.	
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form eller via egne testdata. Vi har observeret, at test foretages med egne testdata, og har fået oplyst, at den dataansvarliges persondata aldrig anvendes til test. Vi er informeret om, at der efter instruks og i pseudonymiseret form anvendes persondata til support og fejlretning. Vi har observeret, at data kan anvendes i pseudonymiseret form.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**B**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Vi har forespurgt og fået bekræftet, at sårbarhedsscanning gennemføres. Vi har inspiceret resultater for disse tests.	
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Vi har inspiceret, at hostingpartner har indgået databehandleraftale. Vi har inspiceret, hostingpartner Tilaas ISO 9001 certificering og ISO 27001 certificering, hvor alle kontrolområder er godkendt.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har ved stikprøve observeret på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendte, og at der er et arbejdsbetinget behov. Vi har forespurgt om fratrådte medarbejderes adgange til systemer og databaser er rettidigt nedlagt i erklæringsperioden. Vi har observeret, at det for den ene fratrådte medarbejder i perioden er slettet brugeradgang. Vi har inspiceret, at der foreligger månedlig procedure for vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**B**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Vi har observeret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Computere hos Skolevisioner, der indeholder personhenførebare oplysninger, er fastlåste og anbragt i rum der er forsynede med alarm og aflåste, når de ikke benyttes.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til Skolevisioners lokaler, hvori der opbevares og behandles personoplysninger. Vi har inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden. Vi har fysisk observeret kontorlokaler og set dokumentationsvideoer om den fysiske sikkerhed. Vi har forespurgt medarbejdere og ledelse, og har fået bekræftet, at dørene til kontorer altid låses, når kontoret er ubemandet. Vi har inspiceret, at computere er forsvarligt aflåste, og at virksomhedens kontorlokaler er forsynet med alarmsystem. Ledelsen har oplyst, at procedurerne omkring anvendelsen af låse og alarmsystemet fungerer tilfredsstillende.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			**C**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret databehandlerens informationssikkerhedspolitik, som ledelsen har behandlet og godkendt. Seneste er den gennemgået og godkendt den 4.6.2025. Vi har inspiceret checkliste for årsreview og observeret at gennemgang af informationssikkerhedspolitikken sker årligt. Vi har forespurgt alle medarbejdere, og har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til og gennemgået af alle medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Vi har ved en stikprøve på fire databehandleraftaler inspiceret, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Databehandleren udfører baggrundscheck af potentielle medarbejdere inden ansættelse.	Vi har inspiceret, at der foreligger formaliserede procedurer til efterprøvning af medarbejdere i forbindelse med ansættelse og er oplyst, at dette gøres efter vurderet behov. Vi er informeret om, at det ikke er et aftalekrav i databehandleraftalen. Vi har inspiceret, at alle medarbejderne har underskriver tavshedserklæring og hemmeligholdelseserklæring.	Ingen afvigelser konstateret.

Kontrolmål **C** **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger. Eksterne konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har inspiceret, at alle ansatte medarbejdere i erklæringsperioden har underskrevet deres ansættelsesaftale inklusiv fortrolighedsaftale og en hemmeligholdelsesaftale, samt har underskrevet, at persondatahåndbog og informationssikkerhedspolitik er gennemgået. Vi har forespurgt ledelsen om der har været nyansættelser i perioden og fået oplyst at der har være en nyansættelse. Vi er oplyst, at nyansatte medarbejdere i henhold til procedure bliver introduceret til: ● Persondatahåndbogen ● Informationssikkerhedspolitikken ● Procedurer vedrørende databehandling, samt anden relevant information Vi har forespurgt ledelse om der er indgået aftaler med eksterne konsulenter i erklæringsperioden og blevet informeret om, at der er indgået aftaler med en ekstern konsulent. Det er kontrolleret, at tavshedserklæring er underskrevet.	Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. Inddrages. En medarbejder er fratrådt i perioden.	Ingen afvigelser konstateret.

Kontrolmål **C** **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og på generel tavshedspligt. Vi har inspiceret dette for den ene fratrådte medarbejder, og at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning. Der er gennemført udviklingsdage. hvor GDPR og it-sikkerhed er drøftet.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.**			**D**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. Der anvendes software til permanent sletning af filer, når der slettes filer indeholdende persondata. Alle fysiske drev, der indeholder personhenførebare oplysninger slettes permanent på en måde der umuliggør genskabelse af data, før drevene kasseres eller sendes til reparation.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at systemet er opbygget således, at en bruger hos kunde med rette rolle selv kan slette på det tidspunkt det ønskes, men data slette automatisk, når de rammer udløb af opbevaringsperioden (max opbevaringstid) som er aftalt med kunden. Skolevisioner har månedsprocedure hvor der følges op på sletninger. Efter instruks kan Skolevisioner varetage sletning. Procedurerne er senest opdateret den 28.5.2025- Vi har forespurgt ledelsen om forretningsgange ved håndtering af personhenførebare oplysninger, samt inspiceret kontorlokaler, herunder gennemgået 2 videoer af kontorlandskab, sikkerhedstiltag og adgangskontrol procedurer. Vi har inspiceret procedure, der beskriver at personhenførbare oplysninger ikke må udskrives på papir, sendes via mail eller gemmes i Dropbox eller lign. Vi har gennemgået proceduren med ledelsen og observeret, at der anvendes File Shredder, som er et godkendt programmer til sletning af filer. Vi har forespurgt ledelsen og har fået bekræftet, at der er implementeret forretningsgange, som sikrer, at fysiske drev, der	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.**			**D**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		indeholder personhenførebare oplysninger slettes på en sådan måde, at genskabelse af data umuliggøres.	
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: ● Der er implementeret et backupsystem, der sikrer at backup foretages dagligt og at de slettes igen efter interne retningslinjer. Desuden månedlig test af, at de kan gendannes	Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Vi har forespurgt på virksomhedens backupsystemer og inspiceret, at der foreligger procedurer omkring backup. Vi finder virksomhedens backupsystemer og procedurer hensigtsmæssig.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: ● Tilbageleveret til den dataansvarlige og/eller ● Slettet, hvor det ikke er i modstrid med anden lovgivning	Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har ved en stikprøve på ophørte databehandlinger i erklæringsperioden observeret, at den aftalte sletning er udført. Vi har inspiceret, at den dataansvarlige selv kan kopiere eller slette data, og at databehandler efter instruks på vegne af den dataansvarlige kan kopiere eller slette data. Undersøgelser slettes efter aftaler eller efter 48 måneder. Data slettes 14 dage efter abonnements ophør.	Ingen afvigelser konstateret.

Kontrolmål **E** **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne - senest opdateret 5.6.2025. Vi har inspiceret, at procedurerne er opdateret, og ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen afvigelser konstateret.

Kontrolmål **E** **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Vi har forespurgt ledelsen og fået bekræftet, at databehandling alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål **F** **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks Vi har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige. Alle underleverandører, som har adgang til personhenførebare oplysninger, har underskrevet en databehandleraftale.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har forespurgt ledelsen og fået bekræftet, at de underdatabehandlere som anvendes, svare til de underdatabehandlere som fremgår af bilag B i databehandleraftalerne. Vi har inspiceret, at der foreligger underskrevne, databehandler aftaler på underleverandører, som har adgang til personhenførebare oplysninger.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer og aftale i DBA for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Vi er informeret om, at der ikke har være udskiftning i underdatabehandlerne i erklæringsperioden, hvorfor procedure ikke kan efterprøves.	Ingen afvigelser konstateret. Ingen udskiftning. Derfor ikke muligt at efterprøve.

Kontrolmål **F** **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Vi har ved en stikprøve på underdatabehandleraftaler inspiceret, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: ● Navn ● CVR-nr. ● Adresse ● Beskrivelse af behandlingen	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt (bilag B) over anvendte og godkendte underdatabehandlere. Vi har inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren. *Fysisk og miljømæssig sikkerhed hos Tilaa B.V hosting (datacenter i Holland).*	Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Vi har inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Vi er informeret om, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos	Ingen afvigelser konstateret.

Kontrolmål **F** **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	Hosting partnere har dokumentation for sikkerhed i form af nødstrøm, adgangskontrol, brandsikring, overvågning og alarmsystemer.	de anvendte underdatabehandlere, at tredjelands overførsel ikke foregår og lignende. Vi har inspiceret ISO 27001 certificering fra hosting partner Tilaa dateret 1.10.2024 med udløb 30.9.2026 samt ISO 9001 certificering dateret 1.10.2023 med udløb 30.9.2026.	

Kontrolmål **G** **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. Der udføres årligt tilsyn med underdatabehandlernes overholdelse af indgåede underdatabehandleraftaler.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger **ikke** overføres til tredjelande eller internationale organisationer i overensstemmelse med databehandlerens interne regler. Vi har inspiceret, at procedurerne er opdateret. Vi har forespurgt direktionen om procedure for tilsyn med underdatabehandlere.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Der overføres **ikke** oplysninger til tredjelande eller internationale organisationer, hvorfor dette ikke er efterprøve.	Ingen overførelse. Derfor ikke muligt at efterprøve.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Der overføres **ikke** oplysninger til tredjelande eller internationale organisationer, hvorfor dette ikke er efterprøve.	Ingen overførelse. Derfor ikke muligt at efterprøve.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.**			**G**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*

Kontrolmål **H** **Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdateret 4.6.2025	Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: ● Udlevering af oplysninger ● Rettelse af oplysninger ● Sletning af oplysninger ● Begrænsning af behandling af personoplysninger ● Oplysning om behandling af personoplysninger til den registrerede. Vi har forespurgt og fået oplyst, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer, idet den dataansvarlige selv kan udtrække fra systemet eller Skolevisioner foretager dette ved instruks. Vi har fået oplyst at der ikke har været henvendelse fra dataansvarlig med ønske om bistand.	Ingen afvigelser konstateret.

Kontrolmål **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			**I**
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer i Beredskabsplanen, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden samt inspiceret, at beredskabsplan senest er opdateret 11.12.2024.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: ● Awareness hos medarbejdere ● Overvågning af netværkstrafik ● Opfølgning på logning af tilgang til personoplysninger	Vi har inspiceret, at databehandler udbyder awareness- træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Vi er ved forespørgsel informeret om, hvordan overvågning foretages og finder denne hensigtsmæssig. Vi har inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har forespurgt og fået oplyst, at der har været et driftsnedbrud med manglende tilgængelighed i en kortere periode hos en underdatabehandler.	Ingen afvigelser konstateret. Der har været et driftsnedbrud med manglende tilgængelighed i en kortere periode.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Der har ikke har været andre brud hos databehandler eller underdatabehandler i erklæringsperioden.	Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: ● Karakteren af bruddet på persondatasikkerheden ● Sandsynlige konsekvenser af bruddet på persondatasikkerheden ● Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden	Vi har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: ● Beskrivelse af karakteren af bruddet på persondatasikkerheden ● Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden ● Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Vi har inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.

Dette dokument er underskrevet af nedenstående parter, der med deres underskrift har bekræftet dokumentets indhold samt alle datoer i dokumentet.

Lars du Jardin Nielsen

Navn returneret af MitId: Lars du Jardin Nielsen
Direktør
ID: 39dfc6e6-c8ad-4f49-b13a-072c8937ce42
IP-adresse: 212.10.124.148:43664:43664
CPR-match med MitId
Dato for underskrift: 17-09-2025 19:17:14 CEST (+02:00)
Underskrevet med MitID

Lasse Lei Kjærsgaard

Navn returneret af MitId: Lasse Lei Kjærsgaard
Revisor
ID: 3fd2ec7e-c26e-4c33-b5d2-7a81ce078e3e
IP-adresse: 104.28.45.4:21327:21327
CVR-match med MitId
Dato for underskrift: 17-09-2025 22:03:01 CEST (+02:00)
Underskrevet med MitID Erhverv