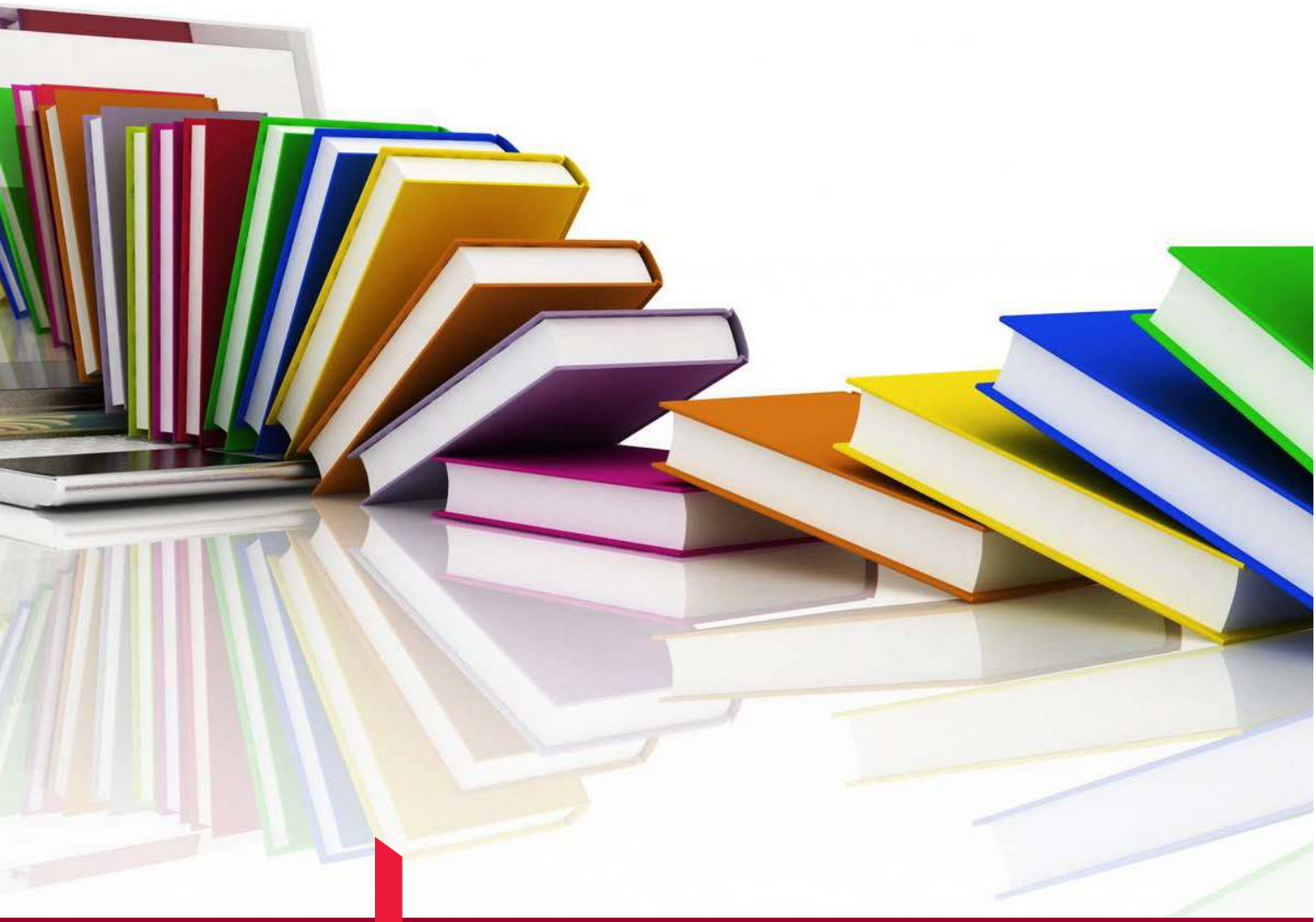

ISAE 3000-ERKLÆRING PR. 20. MARTS 2019 OM BESKRIVELSEN AF SKOLEPORTALEN OG TESTPORTALEN OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER (KONTROLLER) OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Hogrefe Psykologisk Forlag A/S

BDO

INDHOLD

REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ERKLÆRING MED SIKKERHED PR. 20. MARTS 2019 OM BESKRIVELSEN AF SKOLEPORTALEN OG TESTPORTALEN OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER (KONTROLLER) OG DERES UDFORMNING, RETTET MOD BEHANDLING AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Hogrefe Psykologisk Forlag A/S
Hogrefe Psykologisk Forlag A/S' kunder

Omfang

Vi har fået som opgave at afgive erklæring om den af Hogrefe Psykologisk Forlag A/S (databehandleren) pr. 20. marts 2019 udarbejdede beskrivelse på side 6 - 9 af skoleportalen og testportalen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller), rettet mod behandling og beskyttelse af personoplysninger i henhold til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), samt om de af databehandleren pr. 20. marts 2019 udformede tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller), der knytter sig til de kontrolmål, som er anført i forannævnte beskrivelse.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Databehandlerens ansvar

På side 4 - 5 i nærværende rapport har databehandleren afgivet en udtalelse om egnetheden af den samlede præsentation af beskrivelsen.

Databehandleren er ansvarlig for udarbejdelsen af beskrivelsen og udtalelsen, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at definere kontrolmål samt udforme og implementere kontroller for at nå disse kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen af kontroller der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformede. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet på side 4 - 5.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af skoleportalen og testportalen, som hver enkelt dataansvarlig måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

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 databehandlerens udtalelse på side 4 - 5. Det er vores opfattelse:

a. at beskrivelsen af skoleportalen og testportalen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller), rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 20. marts 2019, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger (kontrollerne), som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 20. marts 2019.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse test fremgår på side 11 - 27.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens skoleportal og testportal, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller), som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 12. april 2019

BDO Statsautoriseret revisionsaktieselskab

Per Sloth
Partner, Chef for Risk Assurance

Per Frost Jensen
Statsautoriseret revisor

HOGREFE PSYKOLOGISK FORLAG A/S' UDTALELSE

Hogrefe Psykologisk Forlag A/S (herefter Hogrefe) er ansvarlig for behandling af personoplysninger på vegne af deres kunder, som er dataansvarlige ifølge Europa-Parlamentet og Rådets forordning (EU) 2016/679 af 27. april 2016 for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) samt lov om supplerende bestemmelser til denne forordning (databeskyttelsesloven).

Den medfølgende beskrivelse er beregnet til de dataansvarlige, der anvender Hogrefes skoleportal og testportal til administration og/eller scoring af forlagets produkter (pædagogiske og psykologiske test), og som har en tilstrækkelig forståelse til at vurdere beskrivelsen i sammenhæng med dataansvarliges egne indførte tekniske og organisatoriske sikkerhedsforanstaltninger, når det vurderes om databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Hogrefe bekræfter, at den medfølgende beskrivelse på side 6 - 9 giver en retvisende beskrivelse af skoleportalen og testportalen samt de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller) pr. 20. marts 2019. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse

1. Redegør for, hvordan skoleportalen og testportalen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller) var udformet og implementeret, herunder redegør for:
   - De typer af ydelser der er leveret.
   - De processer i både it- og manuelle systemer der er anvendt til at registrere, behandle og om nødvendigt slette 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 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.
   - De kontroller, som vi med henvisning til afgrænsningen for anvendelsen af skoleportalen og testportalen 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.

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af beskrivelsen af skoleportalen og testportalen og de tilhørende tekniske og organisatoriske foranstaltninger (kontroller) 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 anvendelsen af skoleportalen og testportalen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

Hogrefe bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller) i relation til de kontrolmål, der er angivet i den medfølgende beskrivelse, er hensigtsmæssigt udformet pr. 20. marts 2019. Kriterierne anvendt for at give denne udtalelse var, at:

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

Hogrefe bekræfter, at passende tekniske og organisatoriske foranstaltninger er gennemført og vedligeholdes for at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Virum, 11. april 2019

Hogrefe Psykologisk Forlag A/S

Anne Louise Andersen
Administrerende direktør

HOGREFE PSYKOLOGISK FORLAG A/S' BESKRIVELSE

1. Overordnet beskrivelse af Hogrefe Psykologisk Forlag A/S

Hogrefe beskæftiger ca. 12 medarbejdere inden for forlagsbranchen og har kontor i Virum.

Hogrefe tilbyder som led i dets forlagsvirksomhed internetadministration og/eller -understøttelse af flere af forlagets produkter rettet primært mod det skolefaglige og psykologfaglige område. Internetadministrationen og -understøttelsen af forlagets produkter er henlagt til de to internetportaler skole.hogrefe.dk hhv. testportal.hogrefe.dk.

2. Systembeskrivelse

Hogrefe stiller internetportalerne skole.hogrefe.dk og testportal.hogrefe.dk til rådighed for de kunder, der anvender bestemte af forlagets pædagogiske prøver og psykologiske test. Via portalerne er det muligt at oprette testpersoner til at tage de ønskede prøver eller test. Prøverne/testene tages enten ved, at testpersonen logger sig på portalen og udfylder prøven/testen her, eller at testpersonen udfylder prøven/testen på papir. I begge tilfælde scores prøven/testen efterfølgende i internetportalen, og resultatet af prøven/testen kan efterfølgende opbevares her af kunden i ønsket omfang.

Hogrefe har udviklet, vedligeholder og supporterer internetportalerne i samarbejde med underdatabehandler Ashfield Nordic Aps. Forlaget har valgt at overlade hostingen og overvågningen af internetportalerne til underdatabehandler Support-IT Network (herefter SIT) med fysisk serverplads hos Interxion, Industrivej 20A, 2750 Ballerup samt hos Njanet, Ejby Industrivej, 2600 Glostrup. Medarbejdere hos Hogrefe og underdatabehandlere er instrueret i forsvarlig omgang med personoplysninger.

Hogrefe stiller standarddatabehandleraftaler til rådighed for dataansvarlige brugere af internetportalerne. Hogrefe behandler udelukkende data efter instruks fra brugerne. Brugerne af internetportalerne har ved ibrugtagning af systemerne accepteret at være dataansvarlig for de behandlede personoplysninger, herunder at Hogrefe Psykologisk Forlag A/S fungerer som databehandler på vegne af dem i forbindelse med behandlingen af personoplysninger.

Hogrefe pålægger sine underdatabehandlere samme databeskyttelsesforpligtelser, som forlaget selv er underlagt som databehandler. Hogrefes databehandleraftaler omfatter godkendelse af samtlige anvendte underdatabehandlere.

Hogrefe foretager risikostyring ved løbende at vurdere risici for manglende eller uautoriseret adgang til internetportalerne såvel som misbrug eller tab af de heri opbevarende oplysninger. Foranstaltninger til minimering og forebyggelse heraf foretages i samarbejde med underdatabehandlere.

Hogrefe foretager styring af persondatasikkerheden ved løbende afrapportering fra underdatabehandler SIT i form af daglige backup-rapporter, kvartalsrapporter for overvågning af systemer samt eksternt foranstaltede kontrolangreb. Disse tiltag fungerer sammen med SIT's ISAE 3402 type 2-erklæring som tilsyn med underdatabehandlende hostingvirksomhed. ISAE 3402 erklæringen gennemgås mindst én gang årligt af Hogrefe.

Hogrefe har etableret en procedure for registrering af sikkerhedshændelser, herunder underretning af eksterne dataansvarlige og herigennem de relevante myndigheder og registrerede. Underretning om sikkerhedsbrud omfatter type af brud, omfang og art af personoplysninger, risiko og konsekvenser for registrerede, eventuelt særlige kategorier af registrerede og/eller oplysninger, antallet af berørte personer og afhjælpende foranstaltninger.

Alle medarbejdere hos Hogrefe har underskrevet en aftale, der forpligter dem til fortrolighed. Alle Hogrefes underdatabehandlere er underlagt en tilsvarende forpligtelse via underdatabehandleraftaler.

Hogrefes systemer er beskyttet af antivirus-systemer og firewall. Kommunikation med serverne er sikret ved kryptering. Server(e) har sikkerhedscertifikat. Servere er placeret i en aflåst celle, sikret ved redundant køling og brandslukningsanlæg og overvåget af fysisk tilstedeværende vagter døgnet rundt.

Sikkerhedskopi af filer gemmes i 60 dage, og sikkerhedskopi af SQL-databaser gemmes i 10 dage. Sikkerhedskopien opbevares i krypteret form på to forskellige lokationer under samme sikkerhedsforanstaltninger. Hvis kunder skal have genskabt fejlagtigt, slettede eller på anden vis mistede data, kan forlaget kun garantere at gøre dette ved anmodning herom inden 10 dage. Hogrefe kan først garantere, at data er endegyldigt slettet og ikke længere mulige at genskabe i nogen form efter 60 dage.

Kun relevante medarbejdere hos Hogrefe har adgang til personoplysningerne i internetportalerne. Ajourføring af adgang og roller foretages løbende og kontrolleres mindst én gang årligt. SIT har etableret medarbejderprocedurer for tildeling, skift og sletning af adgang til servere, og deres medarbejdere har skullet fremvise en ren straffeattest samt underskrive en fortrolighedserklæring. SIT får udfærdiget en ISAE 3402 type 2-erklæring omhandlende deres hostingaktiviteter.

Hogrefe modtager dagligt rapport om backup fra SIT. Forlaget får besked fra SIT, hvis belastningen af skoleportalen overstiger en vis tærskelværdi. Forlaget modtager mindst en gang hver tredje måned en afrapportering om sine systemer fra SIT, omfattende usædvanlige adgangsmønstre eller usædvanlig aktivitet på servere. Internetportalerne udsættes jævnligt og mindst én gang årligt for kontrollerede angreb.

Brugere såvel som medarbejderes adgang til systemerne er begrænset med unikt og personligt login. Efter fem afviste login-forsøg blokeres den pågældende bruger. Blokeringen kan kun ophæves ved personlig henvendelse til Hogrefe. Dette gælder dog ikke for brugere med UNI-Login, hvis login administreres af Styrelsen for It og Læring (STIL). Internetportalerne er opsat med selvstændig logning af brugerlogin, supportlogin foretaget af forlagets medarbejdere samt forbrug af forlagets produkter i portalerne. Loggen opbevares i mindst seks måneder.

Brugere kan tildeles forskellige roller i skoleportalen afhængigt af deres formål med anvendelse af systemet; administratorer kan oprette andre brugere og tilgå log for deres institution, brugere kan tildele test og se resultater heraf, og konsulenter kan se resultater på gruppeniveau.

Hogrefe bistår dataansvarlige med opfyldelse af registreredes rettigheder, revision, inspektion samt overholdelse af særlige krav i databeskyttelsesforordningen. Forlaget fører fortegnelse over behandlingsaktiviteter, herunder indgåede databehandleraftaler, og har udarbejdet en beredskabsplan for registrering af sikkerhedshændelser, herunder underretning om brud på persondatasikkerheden.

3. Beskrivelse af kontrolmål og kontroller med link til kontrolskemaet

Artikel	Hovedområde	Område
Artikel 28, stk. 1	Databehandlerens garantier	• Ekspertise, pålidelighed og ressourcer hos databehandleren, herunder de garantier som databehandleren stiller over for den dataansvarlige • Rekruttering og uddannelse af medarbejdere • Instruktion og oplæring af medarbejdere i kravene til behandling og beskyttelse af personoplysninger
Artikel 28, stk. 3	Databehandleraftaler med dataansvarlige	• Databehandleraftale med den dataansvarlige • Styring af underdatabehandlere
Artikel 28, 29 og 32	Instruks for behandling af personoplysninger	• Dokumenteret instruks for behandling af personoplysninger • Underretning af den dataansvarlige i forhold til ulovlig instruks

Artikel	Hovedområde	Område
Artikel 28, stk. 2 Artikel 28, stk. 3, litra d og h Artikel 28, stk. 4 Artikel 29 Artikel 32, stk. 4	Databehandleraftaler med underdatabehandlere, herunder dokumenteret instruks	• Databehandleraftale med Support-IT Network A/S for hosting services • Styring af underdatabehandlerens brug af databehandlere • Dokumenteret tilsyn med Support-IT Network A/S, baseret på en risikovurdering
Artikel 28, stk. 3, litra b	Tavsheds- og fortrolighedsaftaler	• Tavsheds- og fortrolighedsaftale med medarbejdere • Fortrolighedsaftale med leverandører, der ikke er underdatabehandlere
Artikel 28, stk. 3, litra c	Tekniske og organisatoriske sikkerhedsforanstaltninger i håndtering af personhenførbare data.	• Vurdering af sikkerhedsmæssige risici ud fra sandsynlighed og konsekvens (risikovurdering) • Overvågning af skoleportalen og testportalen • Adgangssikkerhed, herunder brugerrettighedsstyring, autorisationer, sletning af brugere og logisk adgangskontrol • Datafortrolighed • Backup og opbevaring af hostingserver • Test af sikkerhed på skoleportalen og testportalen • Information om kundens egen forpligtelser
Artikel 25	Databeskyttelse gennem design og standardindstillinger	• Databeskyttelse i udviklingsprocessen, herunder ved ændringer. • Databeskyttelse af kundedata og ved kundesupport.
Artikel 28, stk. 3, litra g	Sletning og tilbagelevering af personoplysninger	• Sletning og tilbagelevering af personoplysninger i henhold til indgåede databehandleraftale
Artikel 28, stk. 3, litra e, f og h	Bistand til dataansvarlige	• Bistand – registreredes rettigheder • Bistand – overholdelse af forpligtelser • Bistand – revision og inspektion
Artikel 30, stk. 2, 3 og 4	Fortegnelse over behandlingsaktiviteter	• Fortegnelse over dataansvarlige med angivelse af behandlingsaktiviteter
Artikel 33, stk. 2	Brud på persondatasikkerheden	• Registrering og underretning om brud på persondatasikkerheden

Kontrolmål og kontrolaktiviteter for disse områder fremgår af kontrolskemaet, der er en integreret del af denne beskrivelse.

4. Beskrivelse af komplementerende kontroller hos Hogrefe Psykologisk Forlag A/S' kunder

Ved indgåelse af databehandleraftale med Hogrefe erklærer den dataansvarlige sig enig i, at Hogrefes tekniske og organisatoriske foranstaltninger som udgangspunkt er tilstrækkelige og passende i henhold til kravene i databeskyttelsesforordningen. Den dataansvarlige indvilliger endvidere i, at Hogrefe fungerer som databehandler og i forbindelse hermed benytter sig af underdatabehandlere.

Hogrefes dataansvarlige kunder har adgang til udfærdiget It-revionserklæring om persondatabehandlingen i internetportalerne samt til selvstændigt at foretage inspektioner på forlagets adresse og af forlagets behandling af personoplysningerne.

Det er brugerne af internetportalerne selv, der opretter registrerede heri og indsamler personoplysninger herfra. Det er ligeledes brugerne af internetportalernes ansvar at sikre lovhjemmel til behandlingen af personoplysninger samt at slette disse, når formålet med behandlingen er udtjent.

Dataansvarlige kunder har ansvaret for opfyldelse af registreredes rettigheder efter databeskyttelsesforordningen. Hogrefe henviser anmodninger fra registrerede til brugerne af internetportalerne. Forlaget er desuden kunderne behjælpelige med opfyldelse af disses forpligtelser til at besvare anmodninger fra registrerede.

Hogrefe kan behandle data uden for rammerne af instruksen, hvis det er påkrævet i henhold til EU-ret eller national ret.

KONTROLMÅL, KONTROLLER, TEST OG RESULTAT AF TEST

I nærværende testskema er relevante kontrolmål og indførte kontrolaktiviteter udformet til at nå kontrolmålene, beskrevet og udvalgt af Hogrefe Psykologisk Forlag A/S.

I testskemaet har vi beskrevet de udførte test, som blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og de tilhørende kontroller er hensigtsmæssigt udformet.

Test af kontrollernes design og implementering er udført ved forespørgsel, inspektion og observation.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale hos Hogrefe Psykologisk Forlag A/S er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.

For de ydelser, som Support-IT Network A/S har leveret, har vi fra uafhængig revisor modtaget en ISAE 3402 type 2-erklæring om kontroller relateret til drift af hostingplatformen, backup og support for perioden fra 1. april 2017 til 31. marts 2018.

Denne underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Hogrefe Psykologisk Forlag A/S beskrivelse af skoleportalen og testportalen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger. Vi har således alene foretaget inspektion af det ovenfor anførte dokument og testet de kontroller hos Hogrefe Psykologisk Forlag A/S, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Artikel 28, stk. 1 – Databehandler		
Kontrolmål • *At sikre databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Politikker og procedurer • Databehandleren har udarbejdet og implementeret en databeskyttelsespolitik. • Databehandlerens politik bliver gennemgået og ajourført mindst én gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databeskyttelsespolitik og observeret, at den senest er blevet gennemgået og opdateret den 1. marts 2019. Vi har observeret, at databeskyttelsespolitikken er godkendt af ledelsen. Vi har inspiceret databehandlerens rekrutteringsprocedure og observeret, at alle medarbejdere bliver gjort bekendt med databehandlerens databeskyttelsespolitik. Vi har inspiceret databehandlerens årshjul og observeret, at databeskyttelsespolitikken gennemgås og ajourføres en gang om året.	Ingen afvigelser konstateret.
Rekruttering • Databehandler har en procedure for ansættelse af medarbejdere	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for rekruttering af potentielle medarbejdere før ansættelse. Vi har observeret, at rekrutteringsproceduren er godkendt af ledelsen. Vi har observeret, at databehandleren har foretaget baggrundstjek før ansættelse af medarbejdere.	Ingen afvigelser konstateret.
Awareness-uddannelse • Databehandleren har instrueret medarbejdere i lovgivning og databeskyttelsespolitikken samt instruerer løbende nye medarbejdere heri.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens awareness-materiale og observeret, at databehandleren løbende foretager awareness-træning for medarbejdere. Vi har observeret, at uddannelse og awareness er udført, og at nye medarbejdere instrueres i databehandlerens databeskyttelsespolitik.	Ingen afvigelser konstateret.

Artikel 28, stk. 3 – Databehandleraftale

Kontrolmål

- *At sikre databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Databehandleraftaler • Databehandleren indgår databehandleraftaler med alle relevante dataansvarlige. • Databehandleraftaler underskrives og arkiveres elektronisk. • Databehandleraftaler omfatter instruks og information om underdatabehandlere. • Adgang til skoleportal forudsætter indgåelse af skoleaftale med den dataansvarlige institution samt brugersamtykke. • Adgang til testportal kræver brugersamtykke.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved en gennemgang af databehandlerens skoleportal og testportal, observeret at de dataansvarlige kan hente databehandlerens skabelon til databehandleraftale ved oprettelse i skoleportalen og testportalen. Vi har inspiceret databehandlerens databeskyttelsespolitik og skabelon for databehandleraftale. Vi har observeret, at skabelon for databehandleraftale opfylder kravene til indhold af databehandleraftale i henhold til databeskyttelsesforordningens artikel 28, stk. 3, herunder instruks og informationer om brugen af underdatabehandlere. Vi har inspiceret databehandlerens fortegnelse over kategorier af behandlingsaktiviteter og stikprøvevis udvalgte databehandleraftaler. Vi har i den forbindelse observeret: • at databehandleraftalerne er i overensstemmelse med de ydelser som databehandleren leverer og følger skabelon for databehandleraftale. • at databehandleraftalerne er underskrevet af begge parter, og at de opbevares elektronisk. • at databehandleraftalerne indeholder en instruks, der inkluderer om brugen af underdatabehandlere fra den dataansvarlige. Vi har for en stikprøve inspiceret databehandlerens skoleaftale og brugersamtykke for skoleportalen og testportalen. Vi har i den forbindelse observeret: • at skoleaftalen er underskrevet af begge parter, og at den opbevares elektronisk. • at brugersamtykke er accepteret og arkiveret. Vi har observeret en testoprettelse af en kunde på testportalen, hvor vi har observeret, at brugersamtykket ved oprettelsen skal accepteres.	Ingen afvigelser konstateret.

Artikel 28, 29 og 32 – Instruks for behandling af personoplysninger		
Kontrolmål • *At sikre databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* • *At sikre databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Indhentning af instruks • Databehandler behandler udelukkende data efter instruks fra kunden. • Databehandler har udfærdiget og implementeret retningslinjer for modtagelse og dokumentation af instrukser.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databeskyttelsespolitik og skabelon for databehandleraftale. Vi har observeret, at databehandleren har en procedure for modtagelse og dokumentation af instrukser, herunder en skabelon for databehandleraftale, som indeholder instruks. Vi ved inspektion af de stikprøvevis udvalgte databehandleraftaler observeret, at databehandleraftalerne indeholder en instruks fra den dataansvarlige, som databehandleren følger ved enhver behandling af personoplysninger på vegne af den dataansvarlige.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige • Databehandleren gør dataansvarlige opmærksomme på en eventuelt ulovlig instruks.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databeskyttelsespolitik og skabelon for databehandleraftale. Vi har observeret, at databehandleren har en procedure og skabelon for, at databehandleraftaler indeholder vilkår om underretning af den dataansvarlige i tilfælde af en ulovlig instruks. Vi har ved inspektion af de stikprøvevis udvalgte databehandleraftaler observeret, at databehandleraftalerne fastlægger, at databehandleren underretter den dataansvarlige i tilfælde af, at en given instruks er ulovlig.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4 – Underdatabehandlere og leverandører		
Kontrolmål • *At sikre underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.* • *At sikre den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.* • *At sikre underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underdatabehandlere • Databehandler har indgået databehandleraftaler med underdatabehandlere. • Underdatabehandlere er indskrevet i databehandleraftaler med dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for databehandleraftale med dataansvarlige, hvoraf fremgår informationer om brugen af underdatabehandlere. Vi har ved inspektion af stikprøvevis udvalgte databehandleraftaler med dataansvarlige observeret dette. Vi har inspiceret databehandleraftale med Support-IT Network A/S. Vi har ved gennemgang af stikprøvevis udvalgte databehandleraftaler med dataansvarlige observeret, at de er anført som underdatabehandler.	Ingen afvigelser konstateret.
Styring af underdatabehandlerens databehandlere • Underdatabehandleren pålægges de samme databeskyttelsesretlige forpligtelser, som databehandleren er pålagt af de dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandleraftale med Support-IT Network. Vi har ved gennemgang af stikprøvevis udvalgte databehandleraftaler med dataansvarlige observeret, at databehandleraftalen med underdatabehandleren er i overensstemmelse med de forpligtelser og vilkår i databehandleraftalerne med de dataansvarlige.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere • Underdatabehandler med hostingansvar er underlagt selvstændig revision én gang årligt. • Databehandler fører tilsyn med underdatabehandler i form af rapporter. • Underdatabehandlere har forpligtet sig til fortrolighed i databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at tilsynet med underdatabehandleren er udført på baggrund af en risikovurdering af den behandling, som databehandleren har overladt til underdatabehandleren. Vi har inspiceret Support-IT Network A/S' ISAE 3402-erklæring.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4 – Underdatabehandlere og leverandører		
Kontrolmål • *At sikre underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.* • *At sikre den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.* • *At sikre underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret den indhentede dokumentation i tilsynet med underdatabehandleren. Vi har observeret, at databehandleren har udført tilsyn med underdatabehandleren ved at indhente og gennemgå ISAE 3402 type 2-erklæring fra Support-IT Network A/S om drift af hostingplatformen, backup og support for perioden fra 1. april 2017 til 31. marts 2018, dateret den 30. april 2018.	

Artikel 28, stk. 3, litra b – Tavsheds- og fortrolighedsaftale		
Kontrolmål • *At sikre, at alle relevante medarbejdere har forpligtet sig til fortrolighed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Medarbejdere • Alle nuværende medarbejdere og eksterne konsulenter har underskrevet fortrolighedsaftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af en stikprøvevis udvalgt fortrolighedsaftale. Vi har observeret, at fortrolighedsaftalen er underskrevet, og at medarbejderen forpligter sig til at behandle både interne personoplysninger og personoplysninger, som Hogrefe behandler som databehandler for dataansvarlige, fortroligt. Vi har inspiceret databehandleraftalerne med underdatabehandlerne. Vi har observeret, at de har forpligtet sig til fortrolighed i databehandleraftalen. Vi har modtaget og inspiceret tavshedspligt på relevant medarbejder hos Ashfield Nordic ApS og observeret, at tavshedspligten er underskrevet.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c – Tekniske og organisatoriske foranstaltninger

Kontrolmål

- *At sikre databehandleren har implementeret passende tekniske og organisatoriske foranstaltninger, 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 (risikovurdering).*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre, at genoprettelse af tilgængeligheden af og adgangen til personoplysninger sker rettidigt i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre fortrolighed, integritet og tilgængelighed, ved at effektiviteten af foranstaltningerne regelmæssigt afprøves, vurderes og evalueres.*
- *At sikre, foranstaltningerne er revideret og løbende ajourføres.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurderinger og konklusioner • Databehandler har udfærdiget risikovurdering, beredskabsplan og retningslinjer for databehandling og omgang med adgangskoder. • Databehandler har implementeret tekniske og organisatoriske foranstaltninger til at imødegå vurderede risici i samarbejde med underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens risikovurdering, beredskabsplan og databeskyttelsespolitik samt passwordpolitik. Vi har observeret, at risikovurderingen og databeskyttelsespolitikken indeholder relevante områder. Vi har observeret, at beredskabsplanen indeholder relevante oplysninger og eskaleringsproces, herunder hvor it-sikkerhedshændelser registreres. Vi har ved udtræk af Password Policy, Policy for skærmlås og brugere fra netværksoperativsystemet observeret, at omgang med adgangskoder overholdes i henhold til databehandlerens retningslinjer herfor.	Ingen afvigelser konstateret.
Overvågning af sikkerhedsforanstaltninger • Skoleportalen og testportalen overvåges løbende af underdatabehandler med hostingansvar, der dagligt sender en backup-rapport og hvert kvartal en statusrapport til den data- og it-ansvarlige hos databehandleren. • Underdatabehandler med hostingansvar informerer den data- og it-ansvarlige hos databehandleren i tilfælde af truende belastning af skoleportalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret indgåede aftaler og databehandleraftaler med underdatabehandlere. Vi har inspiceret sikkerhedsforanstaltninger for databehandlerens skoleportal og testportal, herunder statusrapport fra underdatabehandler fra første kvartal 2019 og den daglige verificeringsbackup-rapport samt dokumentation for udført restoretest. Vi har observeret, at backup er sikret med kryptering.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c – Tekniske og organisatoriske foranstaltninger

Kontrolmål

- *At sikre databehandleren har implementeret passende tekniske og organisatoriske foranstaltninger, 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 (risikovurdering).*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre, at genoprettelse af tilgængeligheden af og adgangen til personoplysninger sker rettidigt i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre fortrolighed, integritet og tilgængelighed, ved at effektiviteten af foranstaltningerne regelmæssigt afprøves, vurderes og evalueres.*
- *At sikre, foranstaltningerne er revideret og løbende ajourføres.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har observeret, at underdatabehandleren overvåger databehandlerens internetportaler 24/7/365 og informerer databehandlerens data- og it-ansvarlige i tilfælde af truende belastning af internetportalerne.	
Adgangskontrol • Kun autoriserede medarbejdere har adgang til kundernes data med personlige og fortrolige adgangskoder, og adgang logges • Databehandler har etableret procedurer for adgangstildeling ved ansættelse, fratrædelse og rolleskift; oversigt over medarbejderes systemadgange gennemgås mindst én gang årligt • Udefrakommende har ikke adgang til arbejdsstationer eller arkiver med personoplysninger på kontoret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret udtræk af administratorer i henholdsvis skole- og testportalen. Vi har observeret rettighedsstyring og adgangskontrol i skole- og testportalen. Vi har observeret, at bruger-, support- og testadgange logges. Vi har inspiceret konfiguration af logs og observeret, at der foretages en kørsel hver aften, der sikrer at log slettes efter 180 dage. Vi har observeret, at adgange og support logges, og at loggen bliver slettet efter 180 dage. Vi har inspiceret procedure for oprettelse og nedlæggelse af medarbejderkonti og for systemadgange med årlig kontrol. Vi har inspiceret dokumentation for oprettelse af ny medarbejder og observeret, at dette foretages i henhold til proceduren herfor. Det har ikke været muligt at inspicere dokumentation for nedlæggelse af medarbejdere, idet der ikke har været fratrædelser i 2019.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c – Tekniske og organisatoriske foranstaltninger

Kontrolmål

- *At sikre databehandleren har implementeret passende tekniske og organisatoriske foranstaltninger, 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 (risikovurdering).*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre, at genoprettelse af tilgængeligheden af og adgangen til personoplysninger sker rettidigt i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre fortrolighed, integritet og tilgængelighed, ved at effektiviteten af foranstaltningerne regelmæssigt afprøves, vurderes og evalueres.*
- *At sikre, foranstaltningerne er revideret og løbende ajourføres.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har observeret, ved besøg på databehandlerens adresse, at receptionen modtager gæster og udefrakommende, hvorefter medarbejderen henter vedkommende, der har en aftale, til sikring af, at besøgende ikke har uhindret adgang til arbejdsstationer og følsomme personoplysninger.	
Datafortrolighed • Personalebrugerkonti skærmlåses efter 10 minutters inaktivitet. • Kommunikation med hostingserver er sikret med kryptering. • Hostingserver har sikkerhedscertifikat og er udstyret med firewall og antivirus samt foranstaltninger mod fysiske skader og ulykker.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved udtræk af Policy for skærmlås observeret, at skærmlåsen aktiveres efter 10 minutters inaktivitet. Vi har inspiceret krypteringscertifikater for henholdsvis skole- og testportal og observeret, at kommunikation til hostingserverne er sikret med kryptering. Vi har inspiceret konfiguration af firewall og antivirusprogrammet. Vi har inspiceret indgåede aftaler med underdatabehandlere om outsourcing af den fysiske sikkerhed.	Ingen afvigelser konstateret.
Backup og opbevaring • To separate sikkerhedskopier af hostingserver foretages, for at sikre, at data kan gendannes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret backup-konfigurationen og observeret, at der foretages redundant sikkerhedskopiering, der opbevares på to fysisk adskilte adresser. Vi har observeret at retention perioden er i overensstemmelse med indgåede aftaler herfor.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c – Tekniske og organisatoriske foranstaltninger

Kontrolmål

- *At sikre databehandleren har implementeret passende tekniske og organisatoriske foranstaltninger, 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 (risikovurdering).*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre, at genoprettelse af tilgængeligheden af og adgangen til personoplysninger sker rettidigt i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre fortrolighed, integritet og tilgængelighed, ved at effektiviteten af foranstaltningerne regelmæssigt afprøves, vurderes og evalueres.*
- *At sikre, foranstaltningerne er revideret og løbende ajourføres.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Andre kontrolaktiviteter • Databehandler udsætter skole- og testportaler for kontrollerede angreb mindst én gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for seneste kontrollerede angreb af skole- og testportalen, udført den 15. februar 2019.	Ingen afvigelser konstateret.
Tilrettelæggelse af kundens forpligtelser • Databehandleren har informeret kunden om, at det er kundens egen forpligtigelse at sikre sletning af data i skole- og testportal.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for databehandleraftale. Vi har observeret, at de dataansvarlige er ansvarlige for sletning og tilbagelevering af personoplysninger. Vi har inspiceret databehandlerens vejledning til skole- og testportalen, og observeret at dataansvarlige er informeret om deres ansvar vedrørende sletning og tilbagelevering af personoplysninger.	Ingen afvigelser konstateret.

Artikel 25 – Databeskyttelse gennem design og standardindstillinger

Kontrolmål

- *At sikre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Udvikling og ændringer • Der foretages risikovurdering af programudvikling eller -ændring vedrørende sikring af persondatabeskyttelse. • Udviklingsprocessen kræver medarbejdere med udvidet sikkerhedsgodkendelse til at kontrollere og godkende ændringer. • Den person, der skal kontrollere og godkende forandringerne, må aldrig være den samme. • Enhver ændring afprøves under og efter kontrollen og godkendelsen. • Ændringer af skoleportalen og testportalen medførende ændringer eller tab af persondata kan kun implementeres med den data- eller it-ansvarliges tilladelse. • Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer og indeholder anonyme produktionsdata. • Alle ændringer er registreret. • Nye ændringer udføres kun af medarbejdere med den nødvendige ekspertise. • Nye ændringer kræver en tilbagekaldelsespolitik, hvis ændringen ikke er tilfredsstillende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret risikovurderingen og observeret at databehandleren har foretaget risikovurdering vedrørende programudvikling og -ændringer. Vi har inspiceret procedure for test af udvikling og for it-projekt- og afprøvningsplan 2019. Vi har fået oplyst, at det alene er medarbejdere som er godkendte hertil, der kan kontrollere og godkende ændringer, samt at alle ændringer godkendes af administrerende direktør før endelig frigivelse. Vi har observeret, at godkendelse af udvikling og ændringer sker ved 2 i forening. Vi har observeret, at testmiljøet er adskilt fra produktionsmiljøet, samt at testmiljøet alene indeholde anonyme testdata. Vi har observeret, at udviklingsmiljøet er adskilt fra produktions- og testmiljøet, samt at udviklingsmiljøet alene indeholder anonyme data. Udviklingen varetages af ekstern udvikler hos Ashfield Nordic ApS, som har underskrevet tavsheds- og fortrolighedserklæring. Vi har fået oplyst, at der for alle nye tiltag udarbejdes en projekt- og afprøvningsplan, der vurderes og godkendes i redaktionsgruppen og af udviklingschef og/eller administrerende direktør. Mindre rettelser og bugs kan godkendes og idriftsættes af it-ansvarlig med efterfølgende dokumentation og godkendelse. Vi har observeret, at ændringer i skole- og testportalerne først implementeres efter tilladelse af den data- eller it-ansvarliges tilladelse samt at disse er godkendt af den administrerende direktør. Vi har fået oplyst, at Ashfield Nordic ApS' procedure for udvikling understøtter rollback.	Ingen afvigelser konstateret.

Artikel 25 – Databeskyttelse gennem design og standardindstillinger		
Kontrolmål • *At sikre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Kundedata og support • Databehandlerens medarbejdere har kun adgang til kunders data i forbindelse med support (lokal instruks) eller statistiske formål (aftalt instruks). • Kunde- og elevadgang i skoleportalen sker som udgangspunkt med UNI-login. • I skoleportalen er der opsat funktionalitet for rettighedsstyring, således at kundeadministrator hos den dataansvarlige selv foretager oprettelse og sletning af brugere og har ansvar herfor.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandlerens medarbejdere kun har adgang til kunders data i forbindelse med support efter tilladelse fra kunden og i henhold til databehandleraftale og instruks. Vi har observeret, at kunde- og elevadgang til skoleportalen så vidt det er muligt sker via UNI-login, der håndteres af UNI-C. Vi har observeret, at de skoler, som anvender skole- og/eller testportalen, oprettes med en kundeadministrator, der har ansvaret for oprettelse og vedligeholdelse af brugere, samt tildeling af rettigheder der sikrer den nødvendige funktionsadskillelse.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g – Sletning og tilbagelevering af personoplysninger		
Kontrolmål • *At sikre, databehandleren kan slette og tilbagelevere personoplysninger efter instruks fra den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning • Kunder er selv ansvarlige for sletning af data • Databehandler kan manuelt slette og/eller tilbagelevere data efter aftale med den enkelte kunde	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for databehandleraftale og databeskyttelsespolitik. Vi har observeret, at de dataansvarlige selv er ansvarlige for sletning af personoplysninger via skoleportalen og testportalen, og at databehandler efter aftale med dataansvarlige kan bistå med at slette eller tilbagelevere personoplysninger til dataansvarlige. Vi har inspiceret databehandlerens vejledning til skole- og testportalen, og vi har observeret, at de dataansvarlige er informeret om deres ansvar i forhold til sletning og tilbagelevering af personoplysninger.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, h og f – Bistand til den dataansvarlige		
Kontrolmål • *At sikre databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.* • *At sikre databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.* • *At sikre databehandleren kan bistå den dataansvarlige i forhold til overholdelse af særlige krav i forordningen, herunder bistand i forhold til artikel 32 – 36.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Bistand – den registreredes rettigheder • Databehandler har udfærdiget retningslinjer for behandling af henvendelser fra registrerede og dataansvarlige	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for databehandleraftale, hvoraf fremgår, at databehandleren forpligter sig til at bistå de dataansvarlige ved anmodninger om de registreredes rettigheder. Vi har inspiceret databehandlerens databeskyttelsespolitik, hvoraf en procedure ved henvendelser fra registrerede og dataansvarlige fremgår. Vi har observeret, at databehandlerens procedure er i overensstemmelse med forpligtelserne i skabelon for databehandleraftalerne samt de udtagne stikprøver af databehandleraftaler. Vi har observeret, at databehandleren på erklæringstidspunktet ikke er blevet anmodet om at bistå med anførte forpligtelser, hvorfor vi ikke har kunnet inspicere eller observere indførte kontroller.	Ingen afvigelser konstateret.
Bistand – revision og inspektion • Databehandleren forpligter sig i databehandleraftalerne til årligt at indhente ISAE 3000-erklæring samt revision og inspektion til brug for den dataansvarliges tilsyn med databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for databehandleraftale, hvoraf fremgår, at databehandleren forpligter sig til at bistå de dataansvarlige i forbindelse med disses forpligtelser til at føre tilsyn med databehandleren, herunder indhentelse af revisionserklæring efter anerkendte branchestandarder på området. Vi har inspiceret databehandlerens databeskyttelsespolitik, hvoraf en procedure vedrørende indhentelse af en revisionserklæring efter anerkendte branchestandarder på området fremgår.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, h og f – Bistand til den dataansvarlige		
Kontrolmål • *At sikre databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.* • *At sikre databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.* • *At sikre databehandleren kan bistå den dataansvarlige i forhold til overholdelse af særlige krav i forordningen, herunder bistand i forhold til artikel 32 – 36.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har endvidere foretaget inspektion af stikprøvevis udvalgte indgåede databehandleraftaler. Vi har observeret, at disse databehandleraftaler indeholder forpligtelsen til at bistå den dataansvarlige.	
Bistand – overholdelse af særlige forpligtelser • Databehandler har herunder udfærdiget retningslinjer for bistand til dataansvarlige med overholdelse af særlige krav i forordningen	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for databehandleraftale, hvoraf fremgår, at databehandleren forpligter sig til at bistå de dataansvarlige med disses forpligtelser efter databeskyttelsesforordningens artikel 32-36. Vi har inspiceret databehandlerens databeskyttelsespolitik, hvoraf en procedure for bistand til den dataansvarlige med overholdelse af særlige krav i forordningen fremgår. Vi har foretaget inspektion af stikprøvevis udvalgte indgåede databehandleraftaler. Vi har observeret, at disse databehandleraftaler indeholder forpligtelserne at bistå til den dataansvarlige. Vi har observeret, at databehandlerens procedure er i overensstemmelse med forpligtelserne i skabelon for databehandleraftalerne samt de udtagne stikprøver af databehandleraftaler. Vi har observeret, at databehandleren på erklæringstidspunktet ikke er blevet anmodet om at bistå med anførte forpligtelser, hvorfor vi ikke har kunnet inspicere eller observere indførte kontroller.	Ingen afvigelser konstateret.

Artikel 33, stk. 2 – Underretning af brud på persondatasikkerheden		
Kontrolmål • *At sikre databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.* • *At sikre den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Håndtering af brud på persondatasikkerheden • Databehandler har udfærdiget procedure for behandling af sikkerhedshændelser.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databeskyttelsespolitik, hvoraf fremgår, at eventuelle brud på persondatasikkerheden vil blive underrettet til de dataansvarlige hurtigst muligt og dokumenteres i fortegnelsen. Derudover indeholder databeskyttelsespolitikken en angivelse af, hvilke oplysninger en sådan underretning skal indeholde. Vi har observeret, at der på erklæringstidspunktet ikke har været tilfælde af brud på persondatasikkerheden, hvorfor vi ikke har kunnet inspicere eller observere de indførte kontroller.	Ingen afvigelser konstateret.
Meddelelse om brud på persondatasikkerheden • Sikkerhedsbrud rapporteres til dataansvarlige så hurtigt som muligt og senest efter 48 timer fra opdagelse heraf. • Underretning om sikkerhedsbrud omfatter type, art og omfang, risikovurdering, konsekvenser for registrerede, særlige registrerede eller kategorier af oplysninger, antallet af berørte samt afhjælpende foranstaltninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databeskyttelsespolitik, hvoraf proceduren for brud på persondatasikkerheden fremgår. Vi har hertil inspiceret databehandlerens skema til registrering af sikkerhedsbrud. Vi har observeret at underretningen og registreringen er brud på persondatasikkerheden er i overensstemmelse med databehandleraftalen og databeskyttelsesforordningens artikel 33, stk. 2. Vi har fået oplyst, at databehandleren underretter de dataansvarlige uden unødig forsinkelse eller så hurtigt som muligt. Vi har observeret, at der på erklæringstidspunktet ikke har været tilfælde af brud på persondatasikkerheden, hvorfor vi ikke har kunnet inspicere eller observere de indførte kontroller.	Ingen afvigelser konstateret.

Artikel 30, stk. 2, 3 og 4 – Fortegnelse over behandlingsaktiviteter		
Kontrolmål • *At sikre databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.* • *At sikre databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fortegnelse • Databehandler fører fortegnelse over databehandleraftaler og behandlingsaktiviteter. • Fortegnelsen opbevares elektronisk. • Fortegnelsen opdateres løbende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren har udarbejdet en fortegnelse over kategorier af behandlingsaktiviteter, som databehandleren foretager på vegne af de dataansvarlige. Vi har inspiceret den omtalte fortegnelse. Ved gennemgangen har vi observeret, at fortegnelsen indeholder de elementer, som kræves efter databeskyttelsesforordningens artikel 30, stk. 2 og opbevares elektronisk. Vi har på forespørgsel fået oplyst, at fortegnelsen vedligeholdes og opdateres løbende.	Ingen afvigelser konstateret.
Tilgængelighed til myndighederne • Fortegnelsen er tilgængelig for revision og inspektion.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at fortegnelsen efter anmodning stilles til rådighed ved revision og for Datatilsynet.	Ingen afvigelser konstateret.

BDO Statsautoriseret revisionsaktieselskab

Havneholmen 29
DK-1561 København V
CVR-nr. 20 22 26 70