Revisorerklæring

Lindhardt og Ringhof Forlag A/S

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder for perioden fra 1. februar 2023 til 31. januar 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

April 2024

Indholdsfortegnelse

Sektion 1: Lindhardt og Ringhof Forlag A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Lindhardt og Ringhof Forlag A/S' kunder, som har indgået en databehandleraftale med Lindhardt og Ringhof Forlag A/S, 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.

Lindhardt og Ringhof Forlag A/S anvender underdatabehandlerne Sentia Denmark A/S, Microsoft Ireland Operations Ltd., Egmont Administration A/S, Dixa ApS., Sli Sp. z o.o og Amazon Web Services EMEA SARL. Erklæringen omfatter ikke kontrolmål og kontroller hos disse underdatabehandlere.

Lindhardt og Ringhof Forlag A/S anvender Egmont Administration A/S som underdatabehandler til drift, hosting og administration af digitale læringsmidler. Erklæringen omfatter kontrolmål og kontroller hos Egmont IT vedrørende leverance af digitale læringsmidler i henhold til databehandleraftaler.

Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlerens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underdatabehandlere udover Egmont IT.

Enkelte af de kontrolmål, der er anført i Lindhardt og Ringhof Forlag A/S' beskrivelse i Sektion 3 af leverance af digitale læringsmidler, kan kun nås, hvis de komplementerende kontroller hos kunderne er passende designet og operationelt effektive sammen med kontrollerne hos Lindhardt og Ringhof Forlag A/S. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

Lindhardt og Ringhof Forlag A/S bekræfter, at:

a) Den medfølgende beskrivelse, Sektion 3, giver en retvisende beskrivelse af, hvordan Lindhardt og Ringhof Forlag A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 1. februar 2023 til 31. januar 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Lindhardt og Ringhof Forlag A/S' processer og kontroller relateret til databeskyttelse var designet 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 leverance af digitale læringsmidlers 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 leverance af digitale læringsmidler til behandling af personoplysninger foretaget i perioden fra 1. februar 2023 til 31. januar 2024

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne leverance af digitale læringsmidler 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 leverance af digitale læringsmidler 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 passende designet og operationelt effektive i perioden fra 1. februar 2023 til 31. januar 2024, hvis relevante kontroller hos underdatabehandlere var operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Lindhardt og Ringhof Forlag A/S' kontroller i perioden fra 1. februar 2023 til 31. januar 2024. 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 kompetencer og beføjelser i perioden fra 1. februar 2023 til 31. januar 2024

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.

København, den 19. april 2024
Lindhardt og Ringhof Forlag A/S

Kim Bjørn Tiedemann
Direktør for teknologi og udvikling

Sektion 2: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. februar 2023 til 31. januar 2024

Til Lindhardt og Ringhof Forlag A/S og Lindhardt og Ringhof Forlag A/S' kunder i rollen som dataansvarlige.

Omfang

Vi har fået som opgave at afgive erklæring med høj grad af sikkerhed om a) Lindhardt og Ringhof Forlag A/S' beskrivelse i Sektion 3 af leverancen af digitale læringsmidler i henhold til databehandleraftaler med deres kunder i perioden fra 1. februar 2023 til 31. januar 2024 og b+c) om design og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen. Lindhardt og Ringhof Forlag A/S anvender underdatabehandlerne Sentia Denmark A/S, Microsoft Ireland Operations Ltd., Egmont Administration A/S, Dixa ApS., Sli Sp. z o.o og Amazon Web Services EMEA SARL. Erklæringen omfatter ikke kontrolmål og kontroller hos disse underdatabehandlere. Lindhardt og Ringhof Forlag A/S anvender Egmont Administration A/S som underdatabehandler til drift, hosting og administration af digitale læringsmidler. Erklæringen omfatter kontrolmål og kontroller hos Egmont IT vedrørende leverance af digitale læringsmidler i henhold til databehandleraftaler. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlerens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underdatabehandlere udover Egmont IT. Enkelte af de kontrolmål, der er anført i Lindhardt og Ringhof Forlag A/S' beskrivelse i Sektion 3 af leverance af digitale læringsmidler, kan kun nås, hvis de komplementerende kontroller hos kunderne er passende designet og operationelt effektive sammen med kontrollerne hos Lindhardt og Ringhof Forlag A/S. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Lindhardt og Ringhof Forlag A/S' ansvar

Lindhardt og Ringhof Forlag A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i Sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for designet og implementeringen af operationelt effektive kontroller for at opnå de anførte kontrolmål.

Grant Thorntons uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' 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. Grant Thornton anvender International Standard on Quality Management 1, ISQM 1, og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Lindhardt og Ringhof Forlag A/S' beskrivelse samt om designet og den operationelle effektivitet 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, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er passende designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af leverancen af digitale læringsmidler, samt for kontrollernes design og operationelle

effektivitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er passende designet eller ikke er operationelt effektive. 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 i Sektion 3.

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

Lindhardt og Ringhof Forlag A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved leverance af digitale læringsmidler, 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 leverancen af digitale læringsmidler, således som denne var designet og implementeret i perioden fra 1. februar 2023 til 31. januar 2024, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var passende designet i perioden fra 1. februar 2023 til 31. januar 2024, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underdatabehandleren var operationelt effektive, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Lindhardt og Ringhof Forlag A/S' kontroller i perioden fra 1. februar 2023 til 31. januar 2024 , 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 opnået i alle væsentlige henseender, har været operationelt effektive i perioden fra 1. februar 2023 til 31. januar 2024.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i Sektion 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Sektion 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Lindhardt og Ringhof Forlag A/S' leverance af digitale læringsmidler 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.

København, den 19. april 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
Statsautoriseret revisor

Andreas Moos
Director, CISA, CISM

Sektion 3: Lindhardt og Ringhof Forlag A/S' beskrivelse af behandlingsaktivitet for leverance af digitale læringsmidler

Introduktion

Beskrivelsen omfatter informationer om system- og kontrolmiljøet, der er etableret i forbindelse med Lindhardt og Ringhofs leverance af digitale læremidler.

Leverancerne af digitale læremidler sker via forlaget Alinea, som er en del af Lindhardt og Ringhof.

I forhold til tidligere år omfatter beskrivelsen nu også de digitale læremidler der tidligere blev leveret af Clio ApS. Clio ApS blev opkøbt af Lindhardt og Ringhof A/S i 2022 og er blevet integreret juridisk og organisatorisk i Lindhardt og Ringhof i løbet af 2023. Hvor ikke andet er angivet i beskrivelsen, dækker denne derfor både Alineas og det tidligere Clio ApS' produkter, processer, teknologier og foranstaltninger.

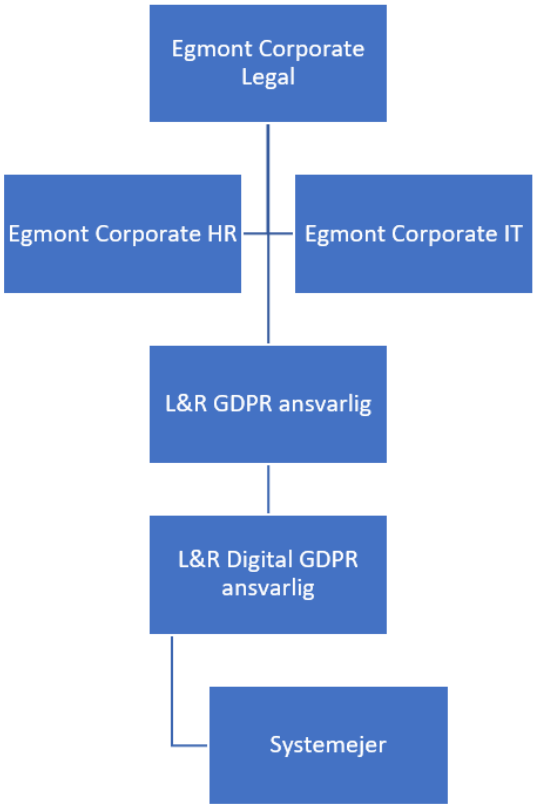
Imidlertid er der enkelte – specielt teknologi og teknologiafledte – områder, hvor der stadigvæk er visse bindinger til Clios platform. Hvor dette er tilfældet, er det eksplicit beskrevet hvilke forhold der er specifikke for "Clio-produkter".

Lindhardt og Ringhofs ydelser

Lindhardt og Ringhof udvikler, administrerer og servicerer en vifte af digitale læremidler for en lang række kommuner, virksomheder og skoler i Danmark. De digitale læremidler tilbydes som Software-as-a-Service, hvor kunderne køber adgang til de digitale læremidler (platform og indhold).

Lindhardt og Ringhof governance organisation

Ansvar og organisering i forbindelse med at være GDPR-compliant fremgår af nedenstående organisation. Beskrivelserne af ansvar og opgaver for hver rolle i overensstemmelse med Egmonts persondatapolitik.



Egmont Corporate Compliance-team

Egmont Legal, HR og IT er ansvarlig for at udvikle og vedligeholde Egmonts persondatapolitik, herunder; overvågning af lovgivning og praksis, vedligehold af standarddokumenter og tekster, samt oprettelse og gennemførelse af uddannelse/træning for medarbejdere.

Lindhardt og Ringhof GDPR-ansvarlig

Ansvarlig for, at databehandlingsaktiviteter overholder Egmonts politikker, og GDPR-revisioner bliver udført. Rollen er også ansvarlig for håndtering af databrud. Herunder ansvarlig for, at der er etableret kontroller og procedurer samt sikre tilstrækkelig forankring af de delegerede roller.

Ansvarlig: Forlagsdirektør.

Lindhardt og Ringhof digital GDPR-ansvarlig

Skal sikre forankring af kontroller og procedurer samt rettidig rapportering og revisionsaktiviteter.

Ansvarlig: Direktør for teknologi og udvikling.

Systemejer

Har ansvar for, at krævede databehandlingsaftaler er på plads samt udføre revision af dataprocesser og foretage risikovurderinger. Afhængig af systemets størrelse og projekters omfang, så bliver der også udpeget en "systemadministrator" – alternativt varetages nedenstående roller af "systemejer".

Systemadministrator

Ansvarlig for bruger- og adgangsstyring samt sikrer og udfører de nødvendige opgaver for at sikre, at den daglige systemoperation overholder politikker, herunder registrering af passende logning, overvågningsrutiner og backup.

Lindhardt og Ringhofs produkter

Alle digitale læremidler til grundskolen solgt til kommuner og privatskoler er med i scopet for den årlige revisionserklæring. Herunder støttesystemer for leverance af disse ydelser, dvs. licenssystem og single-sign-on.

Alinea produkter
Licenssystem og Single-Sign-On (anvendes af både Alinea & Clio) Håndtering af brugere og adgange.
Portaler Alle Alineas portaler til alle klassetrin/fag med en række forskellige undervisningsforløb.
Onlineprøver Alle Alineas onlineprøver til at teste elevernes færdigheder i lytning, læsning, sprog og sprogbrug og skriftlig fremstilling.
Træning Alineas træningsprodukter til dansk, matematik og sprog. Herunder Matematikfessor, CampMat, Camp-Engelsk og CampStavning.
Læsning Produkter til alle klassetrin: Superbog, Superreaders og i-bøger.

Alinea produkter
Træningswebsites til grundsystemer Diverse websites til grundsystemer med opgaver, fx PS PraktiskSprog, ”Den første læsning”, Mitformat.dk og Stavevejen.
Ressource websites til grundsystemer Diverse websites til grundsystemer (“Har du bog, har du web!”) med diverse digitale ressourcer, fx format.alinea.dk, kontext.alinea.dk m.fl.

Clio produkter
Portaler Alle Clios portaler til alle klassetrin/fag med en række forskellige undervisningsforløb.
Online øvelser og prøver Alle Clios online øvelser og -prøver til at forbedre og teste elevernes færdigheder i lytning, læsning, sprog og sprogbrug og skriftlig fremstilling.
Træning Clios træningsprodukter til dansk, matematik og sprog.

Databehandling

Inddata

Lindhardt og Ringhof behandler følgende data:

- Almindelige persondata (herunder elever/læreres UNI-login ID, skole, klassetrin m.v.). Lindhardt og Ringhof behandler ikke følsomme persondata.
- Systemanvendelse: Brugerens anvendelse af læremidlerne (klik og tidsforbrug) opsamles til brug for analyse og personalisering af indholdet, herunder præsentation af statistik for brugerne.
- Noter og besvarelser: Brugernes besvarelser på opgaver gemmes. Data bruges til lærerevaluering og tilpasning af indhold og opgaver. Brugerne kan tage noter i læremidlerne. Noterne kan deles med lærere i samme institution.

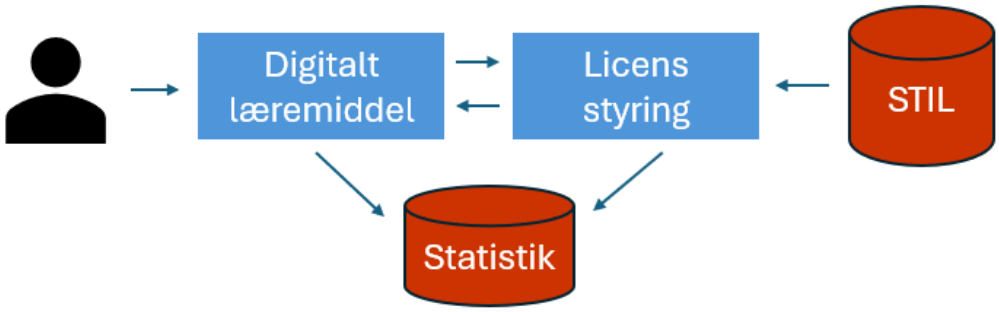
Lindhardt og Ringhof sletter eller anonymiserer data automatisk og højst seks måneder efter, at data om eleven ikke længere modtages fra Styrelsen for IT og Læring (STIL). Data er lagret i et fysisk datamiljø, der er sikret og adgangskontrolleret via hosting partner. Hvor det er muligt, er persondata i Lindhardt og Ringhofs fagportaler og træningsprodukter pseudonymiseret. Data om brugeren (klasse, navn m.v.) er placeret i et licenssystem, og opsamlede elevdata og adfærd er placeret i læremidlet. Koblingen mellem disse er udelukkende på ID-nummer, som ikke er direkte personhenførbart.

For Clio produkternes vedkommende, foretages der automatisk sletning 60 dage efter en bruger er inaktiv i licensmæssig sammenhæng og i STILs UniLogin.

Uddata

Lindhardt og Ringhof sender ikke data med personoplysninger til 3. part, som ikke er beskrevet i databehandleraftaler, eller hvor individer ikke har givet accept.

Dataflow



Brugeren

Brugeren logger på Lindhardt og Ringhofs produkter med UNI-login, som udbydes af STIL. Lindhardt og Ringhof har ikke kontrol over passwords, mislykkede loginforsøg m.v. Kun brugeren fra institution med gyldig ws17-aftale kan logge på.

Digitalt læremiddel

Kan være en webportal eller App, hvori elever/lærere arbejder med undervisningen.

Licensstyring

Lindhardt og Ringhof har licenssystemer, som styrer adgange til kommuner/skoler. Når en bruger forsøger at tilgå et læremiddel og efter autentificering i UNI-login, bliver denne tjekket i et licenssystem på baggrund af institutionsnummer/klassetrin. For Alineas vedkommende er licenssystemet ”LSMS” og for Clio produkter er licenssystemet ”ZERO”.

STIL

Persondata på elever, lærere m.v. trækkes fra STIL webservice WS17. Opdateringer af personoplysninger sker udelukkende via STIL og sendes automatisk til Lindhardt og Ringhofs systemer, når ændringer foreligger. Den dataansvarlige vedligeholder selv data i STIL på baggrund af behørig behandlingshjemmel.

Statistik

Brugerens anvendelse af læremidlerne (klik og tidsforbrug) opsamles til brug for analyse, statistik og personalisering i nogle læremidler. Statistikken med anonymiserede data er tilgængelig for kommuner og skoler bag login.

Hosting og samarbejdspartnere

Underdatabehandlere Sentia og Egmont IT (Microsoft Azure) varetager hosting af Lindhardt og Ringhofs digitale læremidler. I en overgangsperiode bliver de tidligere Clio-produkter hostet hos underdatabehandleren Amazon Web Services (AWS). Hosting omfatter vedligehold af servere, backup, sikkerhed m.v. Hosting sker i hostingcentre i EU. Sentia og Egmont IT benytter ikke data til andre formål.

Hostingen hos Sentia omfatter kun ganske få produkter. Kendetegnende for disse produkter er, at der truffet beslutning om en udfasning og/eller migrering til Microsoft Azure platformen, der forventes gennemført inden sommerferien 2024. I lyset af den meget begrænsede og ophørende anvendelse, har Alineas ledelse valgt at udelade aktiviteterne hos Sentia i revisionserklæringen for 2024.

Risikostyring (IT Governance)

Risikostyring gennemføres i Lindhardt og Ringhof på flere områder og niveauer. Der gennemføres en årlig risikovurdering, der sigter mod udvalgte læremidler. Input til denne vurdering indhentes fra relevante niveauer i organisationen. Processen faciliteres af ansvarlige og ledere, der udarbejder udkast til Lindhardt og Ringhofs ledelse. Efter intern bearbejdning godkendes vurderingen af Lindhardt og Ringhofs ledelse.

Lindhardt og Ringhof har etableret formaliseret risikostyring, som omfatter de processer i virksomheden, der anvendes i leverancen af digitale læremidler og/eller er omfattet af GDPR. Der følges op på risikovurderingen minimum én gang årligt. Arbejdet med risici er dokumenteret i et dokument, hvori både impact og sandsynlighed kan ses sammen med den samlede vægtning af hver enkelt risiko og de dertil knyttede foranstaltninger. Der benyttes en metode som er anerkendt af Datatilsynet.

Kontrolrammer, kontrolstruktur og kriterier for kontrolimplementering

Lindhardt og Ringhof har – indenfor rammerne af Egmont koncernens it-sikkerhedspolitik - etableret processer og kontroller der omfatter ydelser og systemer, der tilbydes kunderne. Følgende væsentlige kontrolområder indgår i det samlede kontrolmiljø:

- Informationssikkerhed
- Adgangsforhold
- Kommunikation med kunder og dataforespørgsel
- Drift og overvågning
- Databrud
- Anvendelsen af underdatabehandlere
- Overførsel af personoplysninger til tredjeland

Hvert enkelt område er beskrevet i de efterfølgende afsnit.

Informationssikkerhed
Lindhardt og Ringhof identificerer og afdækker relevante risici ved de digitale læremidler. Dette varetages gennem en løbende risikovurdering, dels i forbindelse med udviklingsprojekter og ændringer i systemmiljøer, dels ved:

- samlet risikovurdering
- risikovurdering af databehandlere og underdatabehandlere.
- løbende sikkerheds- og kodetests
- etablering af høj sikkerhed på tekniske platforme og i applikationer, herunder procedurer for etablering og vedligeholdelse af tekniske foranstaltninger.

Kontroltidspunkt og dokumentation

Risikoanalysen, privatlivspolitikken og procedurer samt tilsynsmateriale hvad angår hosting partnere revurderes mindst én gang årligt i forbindelse med udførelse af løbende intern audit og forberedelse til ekstern audit og udarbejdelse af erklæring.

Fysisk sikkerhed
Lindhardt og Ringhofs medarbejdere har ikke fysisk adgang til systemer og data. Kun medarbejdere hos hosting partnere har adgang og denne er begrænset til personer med godkendt behov. Lindhardt og Ringhof har sikret at hosting partnere har udarbejdet godkendte procedurer og kontroller for adgangsstyring, alarmsystemer, og at datacenters serverrum er beskyttet mod miljømæssige hændelser som brand og/eller tab af strømforsyning.

Kontroltidspunkt og dokumentation
Hosting partneres månedlige statusrapportering og årlige revisionserklæringer.

Adgangsforhold
For så vidt angår brugere – som IKKE er brugere tilknyttet Lindhardt og Ringhofs kunder - gælder det at adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med Lindhardt og Ringhofs retningslinjer opdelt i to områder:

- Lindhardt og Ringhof medarbejdere
- Medarbejdere hos tredjeparter

Lindhardt og Ringhof medarbejdere

For Lindhardt og Ringhofs interne medarbejdere er informationssikkerhedsmæssige roller og ansvarsområder fordelt, og medarbejderne bliver gjort bekendt med deres ansvar ved tiltrædelse. Rettigheder til interne brugere hos Lindhardt og Ringhof oprettes kun på baggrund af en formel godkendelse.

For interne medarbejdere er der udarbejdet formelle retningslinjer vedrørende sletning af brugeradgange. Disse sikrer blandet andet, at en fratrådt medarbejders adgang ved arbejdsophør hos Lindhardt og Ringhof spærres for login. Alt ovenstående er del af Egmonts sikkerhedspolitik, som Lindhardt og Ringhof er underlagt. Der foretages ligeledes en årlig kontrol af validiteten af de oprettede brugerkonti på Lindhardt og Ringhofs interne systemer.

Adgang til web-server og databaser
Privilegeret adgang til databaser og driftssystemer er begrænset til udvalgte administratorer og specialister, og adgangene bliver revideret løbende. Privilegerede adgange kan kun tildeles af ledere. Adgangskontrol til servere styres igennem Active Directory, hvilket også inkluderer VPN-adgang. Medarbejdere med adgang til domain-controller er specifikke, separat navngivne brugere, hvis handlinger bliver logget.

For adgang til Clios miljøer gælder det at adgange administreres manuelt og der benyttes MFA. Der er tale om fire medarbejdere.

Adgang til licenssystemer
Adgang til licenssystemer er begrænset til udvalgte medarbejdere i udvikling og kundeservice. Adgangene bliver revideret løbende og kan kun tildeles af ledere.

Kontroltidspunkt og dokumentation
Kontrollen vedrørende brugeroprettelser sker hver gang, Lindhardt og Ringhof har en intern ansættelse eller fratrædelse, idet denne kontrol varetages af Egmont IT når der er tale om til- eller fratrædelser på koncernniveau. Kontrollen vedrørende inaktive brugere og brugere med administrative rettigheder foregår årligt. Driftsafdelingen ved Lindhardt og Ringhof har ansvaret for, at adgangsprocedurerne bliver overholdt, og dokumentation vedrørende Lindhardt og Ringhofs medarbejdere gemmes i et relevant værktøj.

Medarbejdere hos tredjeparter

Egmont IT (Microsoft Azure og Amazon Web Services)
Egmont administration A/S (Egmont IT) varetager en række forskellige opgaver for virksomheder i Egmont koncernen. Af disse opgaver er følgende af betydning for Lindhardt og Ringhofs kontrolmiljø i forbindelse med leverancerne af digitale læremidler:

- Administration af bygninger og kontorlokaler, herunder administration af fysiske adgange til Egmont koncernens hovedsæde i Vognmagergade, København, hvor Lindhardt og Ringhof har til huse.
- Administration af Egmont koncernens leverandøraftaler om internet og cloudløsninger, som Lindhardt og Ringhof er bruger af.
- Administration af fysiske endpoints og Egmont koncernens Active Directory, som Lindhardt og Ringhof er bruger af.
- Sikkerhedsmæssig konfiguration og administration af Egmont koncernens Microsoft Azure tenant og AWS organisations. Lindhardt og Ringhof har ansvar for sikkerhedsmæssig konfiguration af indhold i egne Azure subscriptions hhv. AWS organisations.
- Behandling af supporthenvendelser fra koncernens, herunder Lindhardt og Ringhofs brugere.
- Juridisk og HR-mæssig støtte til koncernens virksomheder, herunder Lindhardt og Ringhof,

Privilegeret adgang til Microsoft Azure og AWS (herunder databaser og driftssystemer) er begrænset til udvalgte administratorer og specialister, og adgangene bliver revideret løbende. Privilegerede adgange kan kun tildeles af ledere. Egmonts procedurer for adgangskontrol er underlagt årligt tilsyn af Lindhardt og Ringhof.

I forbindelse med udarbejdelse af revisionserklæringen, er der foretaget revision hos Egmont af de væsentligste kontroller som Egmont Administration A/S varetager på vegne af Lindhardt og Ringhof A/S og/eller har betydning for opnåelsen af visse af Lindhardt og Ringhofs kontrolmål. Det drejer sig om følgende kontroller.

- B.6: Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.
- B.13: Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.
- C.5: Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.
- 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, som databehandleren udfører for de dataansvarlige.

SII

Udviklere hos SII har adgang til udviklingsversioner af Licenssystem og data som hostes i Microsoft Azure. Privilegerede adgange tildeles ad-hoc af Lindhardt og Ringhofs udviklingschef såfremt behov herfor opstår. SII's adgangsrettigheder er underlagt årlig kontrol og tilsyn af Lindhardt og Ringhof.

Dixa

Privilegerede administratorer hos Dixa har adgang til data (sager i sagsstyringssystem). Dixas procedurer for adgangskontrol er underlagt årligt tilsyn af Lindhardt og Ringhof.

Øvrige samarbejdspartnere
Udover Sentia, har Lindhardt og Ringhofs øvrige samarbejdspartnere ikke adgang til produktionsmiljøer eller behandler persondata i forhold til leverance af digitale læremidler. For så vi angår Sentia er der tale om server hosting hvor kun få produkter under udfasning hostes.

Styring af kommunikation med kunder
Kundeservices håndtering af de enkelte kunder er baseret på et sæt skriftlige procedurer på de relevante områder. Support til bruger sker via e-mail, telefon og eventuelle fjernstyringsværktøjer. Dokumentation for henvendelser og udførelse af opgaver for kunderne sker i Lindhardt og Ringhofs sagsstyringssystem.

Incident-håndtering

Lindhardt og Ringhof anvender et sagsstyringssystem (Service Desk) til registrering og håndtering af incidents, og der noteres følgende i sagen:

- Fejl
- Hvad der er gjort for afhjælpning af fejl
- Hvem der har udført opgaver
- Tidsregistrering (om det er ifølge driftsaftale, eller det skal faktureres)

Ledelsen af udviklingsafdelingen er ansvarlig for overvågning af, at indkomne henvendelser i Service Desk prioriteres og tildeles ressourcer.

Kontroltidspunkt og dokumentation
Incident håndtering sker inden for de aftalte SLA-tider med kunderne. Håndteringen af incidents udføres af Lindhardt og Ringhofs driftsafdeling, og uden for normal arbejdstid udføres den af Egmont IT. Dokumentation for incidents og udførelse af incidents for kunderne sker i Lindhardt og Ringhofs sagsstyringssystem.

Dataforespørgsel (GDPR)

Lindhardt og Ringhof anvender et sagsstyringssystem til registrering og håndtering af henvendelser omkring udlevering af personrelateret data, og der noteres følgende i sagen:

- Type af data
- Produkt og periode
- Hvem der har udført opgaver
- Tidsstempling for, hvad tid der er noteret i sagen
- Tidsregistrering (om det er ifølge driftsaftale, eller det skal faktureres)

GDPR ansvarlig i Lindhardt og Ringhof Digital er ansvarlig for overvågning af, at indkomne GDPR henvendelser i Service Desk bliver behandlet. Lindhardt og Ringhof sender en bekræftelse til kunden inden for én hverdag og behandler sagen inden for max fire uger.

Kontroltidspunkt og dokumentation
Dataforespørgsler håndteres inden for aftalte frister i databehandleraftalerne. Proceduren for dataforespørgsler gennemgås årligt, og forespørgsler arkiveres i sagsstyringssystemet.

Drift og overvågning

Der udføres overvågning af, at digitale læremidler er tilgængelige. Servere og digitale læremidler overvåges ved hjælp af monitoreringssoftware.

Kontroltidspunkt og dokumentation
Overvågning og opfølgning udføres 24/7 eller i primær driftstid. Kontroller udføres af Lindhardt og Ringhofs og Egmont IT's driftsafdeling, og uden for normal arbejdstid udføres den af Egmont IT.

Databrud

Lindhardt og Ringhof har etableret en procedure, som overordnet fastsætter retningslinjer for, hvordan et databrud skal håndteres. Proceduren indeholder en beskrivelse af følgende områder:

- Action-plan, hvis der opstår et databrud
- Notifikation til berørte dataansvarlige
- Evt. notifikation til Datatilsynet.

Kontroltidspunkt og dokumentation
Databrudproceduren gennemgås årligt. Ved databrud udarbejdes incident-rapporter og dokumentation for foretaget handlinger.

Anvendelsen af underdatabehandlere
Lindhardt og Ringhof sikrer, at databehandleraftaler med underleverandører samt disses eventuelle underdatabehandlere indgås med, som minimum, omfattes af de samme krav som der fra de dataansvarlige er til Lindhardt og Ringhof.

Lindhardt og Ringhofs godkendte underdatabehandlere og underleverandører, der er relevante for ydelserne, er redegjort for i databehandleraftalerne med kunderne. Alle underbehandlingsaktiviteter er reguleret med en underdatabehandleraftale mellem Lindhardt og Ringhof og underdatabehandleren. Lindhardt og Ringhofs tilsyn med underdatabehandleres overensstemmelse med databehandleraftalen, er tilrettelagt på baggrund af risikovurderinger af den foretagne databehandling hos de enkelte underdatabehandlere.

Overførsel af personoplysninger til tredjelande

Alinea produkter:
Der må i forbindelse med Lindhardt og Ringhofs brug af Microsofts cloud løsning til driften af digitale læremidler ikke ske overførsel af personoplysninger til tredjelande. Af instruksen i databehandleraftalen fremgår, at der ikke må ske overførsler af personoplysninger til tredjelande uden en udtrykkelig instruks fra den dataansvarlige.

Lindhardt og Ringhof har i overensstemmelse hermed, ved brugen af Azures cloud services, valgt Holland som region for Microsofts databehandling og dermed instrueret Microsoft i, at databehandlingen alene må ske indenfor EU/EØS. Lindhardt og Ringhof har yderligere understreget denne instruks overfor Microsoft i særskilt korrespondance.

Derudover har Lindhardt og Ringhof i tilfælde af behov for support sikret et teknisk set-up (Customer Lockbox), der indebærer, at Microsoft i tilfælde af behov for adgang til Lindhardt og Ringhofs miljøer (også inden for EU/EØS) kræver Lindhardt og Ringhof forudgående godkendelse og tildeling af adgang. Lindhardt og Ringhof har således indført kontroller, der skal sikre, at det er Lindhardt og Ringhof, der foretager autorisation af, hvem, der får adgang til personoplysningerne, og at der ikke sker overførsler af personoplysninger til tredjelande, herunder i forbindelse med support-sager.

Clio produkter:
Der må i forbindelse med brug af AWS cloudløsning til driften af digitale læremidler ikke ske overførsel af personoplysninger til tredjelande. Af instruksen i databehandleraftalen fremgår, at der ikke må ske overførsler af personoplysninger til tredjelande uden en udtrykkelig instruks fra den dataansvarlige.

Lindhardt og Ringhof har i overensstemmelse hermed, ved brugen af AWS cloud services, valgt Irland som region for AWS´ databehandling og dermed instrueret Amazon i, at databehandlingen alene må ske indenfor EU/EØS. Lindhardt og Ringhof har yderligere understreget denne instruks overfor Amazon i særskilt korrespondance.

Da AWS ikke tilbyder samme tekniske mulighed som Microsofts Customer Lockbox, har Lindhardt og Ringhof etableret en tilsvarende facilitet ved hjælp af en proxy server og stærk kryptering. Løsningen indebærer – i lighed med Microsoft Customer Lockbox - at AWS i tilfælde af behov for adgang til Lindhardt og Ringhofs miljøer (også inden for EU/EØS) kræver Lindhardt og Ringhof forudgående godkendelse og tildeling af adgang. Lindhardt og Ringhof har således indført kontroller, der skal sikre, at det er Lindhardt og Ringhof, der foretager autorisation af, hvem der får adgang til personoplysningerne, og at der ikke sker overførsler af personoplysninger til tredjelande, herunder i forbindelse med supportsager.

Der er ikke installeret antivirus på de Linux servere i AWS miljøet der anvendes til afvikling af de produkter der blev overtaget i forbindelse med opkøbet af Clio ApS. Der har været foretaget undersøgelser af markedet, men ikke fundet egnede produkter. I lyset af migreringsplanerne for Clio produkterne i AWS miljøet, er det besluttet at stoppe yderligere undersøgelser.

Komplementerende kontroller

Lindhardt og Ringhof giver adgang og tildeler rettigheder i overensstemmelse med kundernes instrukser, i takt med at disse bliver indmeldt gennem STIL (og automatisk overføres). I særtilfælde kan adgang til Lindhardt og Ringhofs produkter tildeles af Lindhardt og Ringhofs support. Lindhardt og Ringhof er ikke ansvarlig for, at informationer om brugerne er korrekte, og det er således kundernes eget ansvar at sikre, at de tildelte adgange og rettigheder til læremidler sker i overensstemmelse med kundernes egne forventninger.

Derudover gælder det, at:

- De dataansvarlige selv er ansvarlige for, at de registrerede rettidigt markeres til sletning
- De dataansvarlige selv er ansvarlige for, at personoplysningerne er ajourførte, herunder at oplysningerne i STILs UNI-login til enhver tid er er korrekte.
- De dataansvarlige selv er ansvarlige for at medvirke til at der indgås en formel databehandleraftale hvor dette måtte være påkrævet.
- De dataansvarlige selv er ansvarlige for at sikre, at databehandleraftalens instrukser til Lindhardt og Ringhof er lovlige set i forhold til den til enhver tid gældende persondataretlige regulering og hensigtsmæssig set i forhold til databehandleraftalen
- De dataansvarlige selv er ansvarlige for håndtering af henvendelser fra den registrerede selv, myndigheder og evt. tredjemand, samt for anmodning til Lindhardt og Ringhof om rettidig assistance med denne håndtering
- De dataansvarlige selv er ansvarlige for, at der anvendes tilstrækkelig kryptering ved tilgang til Lindhardt og Ringhofs portaler.
- De dataansvarlige selv er ansvarlige for, at der anvendes stærke password ved tilgang til Lindhardt og Ringhofs portaler

Justering af kontrolmål/kontroller jf. FSR's erklæringsskabelon

Her listes hvilke kontroller der er taget ud af scope, hvilke der er tilføjet samt hvad der eventuelt er ændret.

Kontrol jf. FSR's erklæringsskabelon	Justering	Begrundelse
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.	Ude af scope	Kontrollen er udeladt, idet adgang til personoplysninger som alene opbevares og behandles digitalt i de nævnte faciliteter, kontrolleres af Lindhardt og Ringhofs samarbejdspartnere på hosting henholdsvis cloudområdet i deres egenskab af ejer af de pågældende faciliteter. Lindhardt og Ringhof evaluerer samarbejdspartnernes kontroludførelse via disses revisionserklæringer og herudover har ingen af Lindhardt og Ringhofs medarbejdere adgang til de pågældende faciliteter.
C.3 Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Ude af scope	Kontrollen er udeladt, idet der i overensstemmelse med Egmont koncernens retningslinjer ikke er krav om procedurelagte screeningsaktiviteter. Det påhviler lederne i de enkelte forretningsområder at foretage de screeningaktiviteter, f.eks. indhentelse af eksamensbeviser, straffeattester o. lign, som de finder nødvendige i den konkrete ansættelsessituation. Det bemærkes at Lindhardt og Ringhof ikke behandler følsomme eller fortrolige personoplysninger.

Sektion 4: Kontrolmål, udførte kontroller, test og resultater heraf

Vores arbejde er udført i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-I nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden fra 1. februar 2023 til 31. januar 2024.

Vi har udført vores tests af kontroller hos Lindhardt og Ringhof Forlag A/S via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Lindhardt og Ringhof Forlag A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af kontrollens udførelse.
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive operationelt effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Derudover foretages der stikprøvevis test af kontrollernes operationelle effektivitet i revisionsperioden.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Kortlægning af kontrolområder op mod GDPR-artikler, ISO 27701 og ISO 27001/2

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2:2013. Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2:2013
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Nyt område ift. ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Nyt område ift. ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevist inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med 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 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 forespurgt, om databehandleren har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi er blevet oplyst, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, hvorfor vi ikke har testet effektiviteten af relevante procedurer. Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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 inspiceret, at der foreligger formaliserede procedurer, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres. Vi har inspiceret, at procedurer er opdaterede.	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 den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Vi har stikprøvevis inspiceret, at risikovurderingen tager stilling til aftalte sikringsforanstaltninger.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har stikprøvevis inspiceret, at der for servere er slået antivirus til.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har stikprøvevis inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.	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 stikprøvevis inspiceret netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugernes adgang til personoplysninger. Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Vi har inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Vi har inspiceret, at brugernes adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har stikprøvevis inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevis inspiceret, at transmission over internettet sker med anerkendte krypteringsstandarder.	Ingen afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har stikprøvevis inspiceret, at der er etableret logning af brugere på systemer. Vi har inspiceret dokumentation for hvem der har adgang til logfiler.	Vi har inspiceret, at logning på en ud af fem databaser ikke er slået til. Vi har dog, efter rapportering af forholdet, inspiceret at forholdet er løst ved at logning er blevet slået til på databasen. Ingen yderligere afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form.	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. Vi har stikprøvevist inspiceret, at personoplysninger er pseudonymiseret eller anonymiseret i udviklings- og testdatabaser.	Vi har inspiceret, at proceduren for applikationsudvikling senest er opdateret i december 2021. Ingen yderligere 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. Vi har stikprøvevist inspiceret, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger, herunder penetrationstest.	Vi er blevet oplyst, at der ikke er udført sårbarhedsskanninger for Clio applikationen i revisionsperioden. Ingen yderligere afvigelser konstateret.
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 stikprøvevis inspiceret at ændringer til systemer, databaser og netværk er håndteret jævnfør proceduren herfor.	Vi har inspiceret, at proceduren for ændringer ikke fulgt fuldstændigt for 10 ud af 22 stikprøver. Vi er blevet oplyst, at der for Clio applikationen ikke er lavet ændringer i revisionsperioden, hvorfor vi ikke har kunnet teste kontrollens effektivitet for denne applikation. Ingen yderligere 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 inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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 stikprøvevis inspiceret, at adgang til personoplysninger sker gennem to-faktor autentifikation.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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, at der foreligger en informationssikkerhedspolitik. Vi har forespurgt, om ledelsen har behandlet og godkendt informationssikkerhedspolitikken inden for det seneste år. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere	Vi har inspiceret, at den generelle it-sikkerhedspolitik og udvalgte underliggende sub-sikkerhedspolitikker, senest er gennemgået og revideret af ledelsen i oktober 2018. Vi har dog inspiceret, at andre udvalgte underliggende sub-sikkerhedspolitikker er opdateret rettidigt. Ingen yderligere afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret informationssikkerhedspolitikken samt underliggende informationssikkerhedsprocedure. Vi har stikprøvevis inspiceret, at informationssikkerhedspolitikken er i overensstemmelse med databehandleraftaler.	Vi har inspiceret, at den generelle it-sikkerhedspolitik og udvalgte underliggende sub-sikkerhedspolitikker, senest er gennemgået og revideret af ledelsen i oktober 2018. Vi har dog inspiceret, at andre udvalgt underliggende sub-sikkerhedspolitikker er opdateret rettidigt. Vi har ikke konstateret afvigelser mellem indgåede databehandleraftaler og informationssikkerhedspolitikerne. Ingen yderligere afvigelser konstateret.
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.	Vi har stikprøvevist inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale. Vi har stikprøvevist inspiceret at nyansatte medarbejdere i erklæringsperioden er blevet introduceret til relevante politikker og procedurer.	Vi er blevet oplyst, at der ikke er en nedskrevet procedure for onboarding. Vi har dog inspiceret, at der er implementeret en systemmæssig checkliste, som understøtter onboarding processen. Ingen yderligere 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. Vi har stikprøvevist inspiceret, at rettigheder er inaktiveret eller ophørt er inddraget for fratrådte medarbejdere i erklæringsperioden.	Vi er blevet oplyst, at der ikke er en formel procedure, som sikrer, at aktiver bliver inddraget. Vi har inspiceret, at der i 10 ud af 10 stikprøver, ikke foreligger dokumentation for, at aktiver er blevet inddraget. Ingen yderligere afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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 stikprøvevist inspiceret, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt for fratrådte medarbejdere. Vi har stikprøvevis inspiceret at opsigelseskvitteringer i perioden indeholder orientering omkring tavshedspligt. Vi har forespurgt til opsigelseskvitteringer for fratrådte.	Vi har inspiceret, at der i 4 ud af 10 stikprøver, ikke foreligger dokumentation for at medarbejderen er gjort opmærksom på vedvarende fortrolighed efter fratrædelse. Ingen yderligere afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awarenesstræning.	Ingen afvigelser konstateret.
C.8	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	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 procedurerne er opdaterede.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Vi har stikprøvevist inspiceret, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Vi har stikprøvevist inspiceret, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner	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 forespurgt om der har været ophørte databehandlinger i erklæringsperioden.	Vi er blevet oplyst, at der ikke har været ophørte databehandlinger i perioden, hvorfor vi ikke har kunnet testet effektiviteten af kontrollen. Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har stikprøvevist inspiceret, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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 opdaterede.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har stikprøvevist inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	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 for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Vi har forespurgt om der har været ændringer af underdatabehandlere i perioden.	Vi er blevet oplyst, at der ikke har været ændringer i anvendelse af underdatabehandlere i perioden, hvorfor vi ikke har kunnet testet effektiviteten af kontrollen. Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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 stikprøvevist inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har inspiceret, at der i 1 ud af 6 underdatabehandlere, ikke er videreført relevante tekniske foranstaltninger, som anført i databehandleraftalen mellem de dataansvarlige og databehandleren. Ingen yderligere afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt 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, hvis der er noget væsentligt at rapportere.	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 har inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Vi har i én ud af seks underdatabehandlere inspiceret at der ikke er opdateret risikovurdering samt foretaget tilsyn i perioden. Vi har dog inspiceret, at der er foretaget en risikovurdering og tilsyn den 26. januar 2023. Ingen yderligere afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

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.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Vi har stikprøvevis inspiceret, at der er dokumentation for, at dataoverførsler er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Vi har, i 1 ud af 6 underdatabehandleraftaler, inspiceret at der fremgår under-underdatabehandlere, som er beliggende i tredjelande, herunder, at der kan ske overførelser til disse. Underdatabehandleren bliver benyttet til teknisk support. Ingen yderligere afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har forespurgt til nødvendig garanti for overførelser til tredjeland.	Vi har ikke modtaget dokumentation for gyldigt overførselsgrundlag til tredjelande for overførelsen under G.2, da vi er blevet oplyst om, at Lindhardt og Ringhof ikke er bekendt med, at der er foretaget overførsler til tredjeland. Ingen yderligere afvigelser konstateret.

Kontrolmål H – De registreredes rettigheder

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.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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 opdaterede.	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, de foreliggende procedurer for bistand til den dataansvarlige. Vi har forespurgt, om databehandleren har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder.	Vi er blevet oplyst, at databehandleren ikke har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen. Ingen afvigelser konstateret

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret loggen over brud i perioden. Vi har forespurgt, om der har været persondatassikkerhedsbrud i perioden.	Vi er blevet oplyst, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen. Ingen afvigelser konstateret

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	*Lindhardt og Ringhof Forlag A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
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.	Ingen afvigelser konstateret.

Sektion 5: Supplerende oplysninger fra Lindhardt og Ringhof Forlag A/S

B.9 - Logning

Revisionens testresultat drejer sig om manglende auditlog på en database indeholdende resultater af prøver som elever har gennemført. I databasen registreres et spørgsmåls-ID, besvarelsesresultatet og timestamp på en given opgave samt pseudonymiseret bruger-ID.

Vi gør opmærksom på at revisionens testresultat ikke omfatter direkte personhenførbare oplysninger.

Logning er efterfølgende blevet etableret.

B.10 og B.12 – Procedurer for ændringer til systemer, netværk m.v.

Revisionens testresultater omhandler dels manglende opdatering af den skrevne procedure for udvikling, ændringer m.v., dels konstatering af at proceduren ikke i alle tilfælde er blevet fulgt. Vi er overgået til en review praksis, hvor to personer ofte sidder sammen og gennemgår ændringer, men at vores system til registrering af ændringer ikke dokumenterer dette. Proceduren for denne praksis ændres, så det dokumenteres fremadrettet.

Vi gør opmærksom på, at der kun er adgang til personhenførbare oplysninger i pseudonymiseret form i forbindelse med løsningen af denne type opgaver.

Der er iværksat en opdatering af den skrevne procedure og foranstaltninger til at sikre overholdelse af procedurerne som beskrevet herover. Proceduren træder i kraft den 31. juli 2024.

B.11 – Sårbarhedsscanning Clio applikationen

Revisionen har konstateret, at der ikke er gennemført sårbarhedsscanning af Clio applikationen som hostes i AWS cloud.

Applikationsporteføljen, der blev overtaget med Clio ApS ultimo 2022, har i 2023 været under migrering fra en løsning hostet på AWS platformen til en løsning hostet på Microsoft Azure cloud. Vi har på denne baggrund ikke prioriteret at gennemføre sårbarhedsscanninger af et ophørende miljø.

Migreringen vil være tilendebragt i løbet af sommeren 2024, hvorefter de tidligere Clio applikationer vil være lukket ned og miljøerne vil blive dekommissioneret.

C.1 og C.2 – Egmont koncernens it-sikkerhedspolitikker

Revisionen har konstateret, at koncernens overordnede, generelle, it-sikkerhedspolitik ikke er gennemgået og revideret for nyligt, hvorimod det ikke er tilfældet for de underliggende, detaljerede, it-sikkerhedspolitikker.

Revisionen har ved en udvidelse af revisionen, ikke konstateret afvigelser imellem koncernens it-sikkerhedspolitikker og de indgåede databehandleraftaler.

Egmont koncernens samlede it-sikkerhedspolitik er baseret på ISO27002 og består derfor af dels en generel "paraply-politik", dels en række underliggende – mere detaljerede - politikker.

De detaljerede it-sikkerhedspolitikker omfatter følgende:

1. Acceptable Use Policy
2. Definitions
3. Data Classification Policy
4. Dispensations Policy
5. Cloud and Outsourcing Policy
6. Identity and Access Management Policy
7. Privileged Access Policy
8. Vulnerability and Patch Management Policy
9. Malware Protection Policy
10. Security Monitoring Policy
11. [Not in use]
12. Local Network Security Policy
13. Storage Security Policy
14. Server Security Policy
15. [Not in use]
16. Backup Security Policy
17. [Not in use]
18. Endpoint Security Policy
19. Application and System Development
20. Cloud Network Security Policy

Lindhardt og Ringhof A/S' compliance med GDPR og de indgåede databehandleraftaler rummes indenfor koncernens detaljerede it-sikkerhedspolitikker, og det påhviler koncernsikkerhedsfunktionen at sikre konsistens imellem koncernens generelle it-sikkerhedspolitik og de detaljerede politikker.

Koncernens generelle it-sikkerhedspolitik vil blive gennemgået og opdateret inden afgivelse næste revisionserklæring. Der er ligeledes etableret foranstaltninger som sikrer, at it-sikkerhedspolitikken revideres årligt.

C.4, C.5 og C.6 - Procedurer for on- og offboarding af medarbejdere

Revisionen har konstateret visse mangler i procedurerne vedrørende både on- og offboarding af medarbejdere. Der er dog ikke konstateret brud på persondatasikkerheden i den forbindelse.

Vi er enige i de konstaterede mangler og har iværksat systemiske tiltag til generel opstramning af procedurerne for både on- og offboarding. Dette vil være gennemført inden 31. juli 2024.

F.4 – Videreførsel af foranstaltninger til underdatabehandler

Revisionen har konstateret, at videreførsel af foranstaltninger fra databehandleraftaler med kunder til databehandleraftale med én specifik underdatabehandler, ikke er gennemført systematisk.

Der er tale om en aftale med et EU-baseret konsulenthus som varetager udviklingsopgaver for Lindhardt og Ringhof Forlag A/S. Udviklingshuset løser konkrete udviklingsopgaver under Lindhardt og Ringhofs instruks og har alene adgang til udviklingsmiljøer hvor der ikke opbevares personoplysninger. I særlige tilfælde, fx i forbindelse med fejlfinding, kan der tildeles specifik og tidsbegrænset adgang som kan medføre adgang til personhenførbare oplysninger.

Der foretages en tilpasning af aftalegrundlaget med den pågældende underleverandør.

F.6 – Kontrol gennemført udenfor erklæringsperioden

Revisionen har konstateret, at opdatering af risikovurdering og gennemførelse af tilsyn – vedrørende én specifik underdatabehandler – er gennemført 5 dage før erklæringsperiodens startdato. Lindhardt og Ringhof bemærker i den forbindelse, at der siden 2020 er udført tilsyn og revision af risikovurdering for den pågældende underdatabehandler i 2020, 2021, 2022 og 2023. Der er foretaget opdatering af risikovurdering d. 26/3-2024 og et tilsyn d. 9/4-2024.

Lindhardt og Ringhofs ledelse har indskærpet at kontroller skal gennemføres i overensstemmelse med årshjulet herfor.

G.2 og G.3 – Forhold imellem underdatabehandler og under-underdatabehandler

Revisionen har konstateret, at der i én specifik underdatabehandleraftale er oplistet under-underdatabehandlere beliggende i tredjelande.

Der er tale om en dansk leverandør af et kundesupport- og sagssystem. Systemet anvendes til supporthenvendelser via e-mail og telefon fra lærere og administrativt personale på skolerne. Leverandøren har underdatabehandlere i bla. UK, USA og Australien.

L&R anerkender at regimet for persondatabehandling er foranderligt. Hidtil har det ikke været kutyme at opliste underdatabehandlerens underdatabehandlere, ligesom der ikke har eksisteret en officiel forpligtelse til at angive samtlige led databehandlerkæden. Vi er opmærksomme på, at de seneste sager og udmeldinger fra Datatilsynet lægger op til en øgning i omfanget og detaljeringsgraden ved angivelsen af underdatabehandlere i databehandleraftalen, og at der er ved at ske en praksisændring. Selvom omfanget endnu er uafklaret, er der utvivlsomt et skærpet fokus på kortlægningen databehandlerkæden. Vi anerkender behovet for at møde de krav og ændringer, der følger med udviklingen og søger således at få implementeret de krav, der følger af den nye praksis.

Vi har fra august 2024 ophørt samarbejdet med den pågældende underdatabehandler og dette er varslet til vores kunder.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Kim Bjørn Tiedemann
Underskriver 1
Serienummer: a3692f38-1a15-4653-867b-61843aebab1a
IP: 194.192.xxx.xxx
2024-04-19 06:58:46 UTC

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 77.241.xxx.xxx
2024-04-19 07:21:07 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serienummer: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2024-04-19 12:32:31 UTC

Penneo dokumentnøgle: EMEUS-1TW12-1NSHV-3TPG0-CYHBK-HOCVN