www.pwc.dk

Gyldendal A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2021 til 31. december 2021 i henhold til Gyldendals standard databehandleraftale i relation til Gyldendals digitale læremidler

April 2022

pwc

Indholdsfortegnelse

1. Ledelsens udtalelse

Gyldendal A/S (Gyldendal) behandler personoplysninger på vegne af sine kunder i henhold til Gyldendals standard databehandleraftale i relation til Gyldendal Uddannelses, Systimes og Guide2Knows digitale læremidler (Gyldendals digitale læremidler).

Medfølgende beskrivelse er udarbejdet til brug for Gyldendals kunder, der har anvendt Gyldendals digitale læremidler, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den 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" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne") er overholdt.

Gyldendal anvender følgende underdatabehandlere til drift, vedligeholdelse og hosting af systemer i relation til Gyldendals digitale læremidler:

- Adobe Systems Benelux B.V
- Amazon Web Services Ireland Ltd.
- Atlassian, Inc.
- Conscia Danmark A/S
- Dansk Sang, Musiklærerforeningens forlag
- Efaktum, HJØRRING ApS
- Google Ireland Limited
- JWPlayer - Longtail Ad Solutions, Inc.
- MentorDanmark ApS
- Microsoft Ireland Operations, Ltd.
- Miracle A/S
- Netic A/S
- New Relic Inc.
- Redia A/S
- Sleeknote ApS
- TOPdesk Danmark A/S
- @Ventures
- Wasabi Technologies inc.
- Writereader ApS

Erklæringen anvender partielmetoden og omfatter ikke kontroller, som ovenstående underdatabehandlere varetager for Gyldendal.

Gyldendal bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne i hele perioden fra 1. januar 2021 til 31. december 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler var udformet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
- De processer i både it-systemer 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 underretning af de registrerede
- De processer, der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger 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 afgrænsningen af informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler har forudsat ville være implementeret af den 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 i informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler til behandling af personoplysninger foretaget i perioden fra 1. januar 2021 til 31. december 2021

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne informationssikkerhed og de beskrevne foranstaltninger i relation til Gyldendals digitale læremidler 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 informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler, som den enkelte dataansvarlige måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2021 til 31. december 2021. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

   (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2021 til 31. december 2021.

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 databeskyttelsesreglerne.

Gyldendal A/S
København, den 4. april 2022

Hanne Salomonsen
Direktør

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2021 til 31. december 2021 i henhold til Gyldendals standard databehandleraftale i relation til Gyldendal digitale læremidler

Til: Gyldendal A/S (Gyldendal) og dataansvarlige i relation til Gyldendals digitale læremidler

Omfang

Vi har fået som opgave at afgive erklæring om Gyldendals beskrivelse i afsnit 3 af deres informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler i henhold til Gyldendals standard databehandleraftale med dataansvarlige i hele perioden fra 1. januar 2021 til 31. december 2021 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Gyldendal har udformet og effektivt udført hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4. Erklæringen omfatter ikke en vurdering af Gyldendals generelle efterlevelse af kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne").

Gyldendal anvender følgende underdatabehandlere til drift, vedligeholdelse og hosting af systemer i relation til Gyldendals digitale læremidler:

- Adobe Systems Benelux B.V
- Amazon Web Services Ireland Ltd.
- Atlassian, Inc.
- Conscia Danmark A/S
- Dansk Sang, Musiklærerforeningens forlag
- Efaktum, HJØRRING ApS
- Google Ireland Limited
- JWPlayer - Longtail Ad Solutions, Inc.
- MentorDanmark ApS
- Microsoft Ireland Operations, Ltd.
- Miracle A/S
- Netic A/S
- New Relic Inc.
- Redia A/S
- Sleeknote ApS
- TOPdesk Danmark A/S
- @Ventures
- Wasabi Technologies inc.
- Writereader Aps

Erklæringen anvender partielmetoden og omfatter ikke kontroller, som ovenstående underdatabehandlere varetager for Gyldendal.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Gyldendals ansvar

Gyldendal er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 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 at udforme og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors 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.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gældende i Danmark, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af deres informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i ledelsens udtalelse.

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

Gyldendals beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler, som hver enkelt dataansvarlig måtte anse for vigtige efter sine 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 informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler, således som det var udformet og implementeret i hele perioden fra 1. januar 2021 til 31. december 2021, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2021 til 31. december 2021, 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 fungeret effektivt i hele perioden fra 1. januar 2021 til 31. december 2021.

Fremhævelse af forhold

Uden at det har givet anledning til modificering af vores konklusion, skal vi oplyse, at vi for Gyldendal - Ungdomsuddannelse og Gyldendal - Videregående uddannelse produkterne har konstateret, at der i relation til kontrolaktivitet B12, ikke kan fremskaffes tilstrækkelige dokumentation for, at der er gennemført test inden ændringer bliver lagt i produktion, ligesom Gyldendal har oplyst, at der ikke er etablerede systemunderstøttet funktionsadskillelse af miljøerne DEV, TEST, QA, PROD.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Gyldendals digitale læremidler, og 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 databeskyttelsesreglerne er overholdt.

København, den 4. april 2022
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jess Kjær Mogensen
statsautoriseret revisor
mne21360

Bo Petersen
Director

3. Gyldendal A/S' beskrivelse af informationssikkerhed og foranstaltninger i relation til Gyldendals digitale læremidler

3.1 Introduktion

Denne fremstilling beskriver hvordan Gyldendal overholder databeskyttelsesforordningen ("GDPR"), samt supplerende national lovgivning i behandlingen af personoplysninger i forbindelse med leveringen af digitale læremidler.

Gyldendal har i løbet af 2021 fusioneret med sine datterselskaber Systime A/S og Guide2Know ApS i 2021. Aktiviteterne fra de tidligere selskaber er uændrede og indgår fortsat som en del af Gyldendals samlede produktportefølje. Denne erklæring omfatter dog først Guide2Knows aktiviteter fra 1. juni 2021.

Fremstillingen beskriver alle relevante forhold vedrørende behandlingssikkerhedens tekniske og organisatoriske foranstaltninger samt ansvaret mellem vores kunder som dataansvarlige og Gyldendal som databehandler.

3.2 Gyldendals digitale læremidler

Gyldendals behandlinger består i at udvikle og drifte en række digitale læremidler og platforme, som udbydes som 'software as a service' under forskellige brands – herunder navnlig Gyldendal, Systime og Guide2Know.

3.2.1 Grundlaget for behandlingen

Ved leveringen af de digitale læremidler behandler Gyldendal personoplysninger som databehandles på vegne af kunden, som i denne sammenhæng dermed er dataansvarlig. Behandlingen sker efter gældende regler og i overensstemmelse med den databehandleraftale, der indgås med kunden. Kunden er typisk en kommune, virksomhed eller en selvejende/privat institution. I databehandleraftalens bilag med tilhørende ydelsesbilag er ydelserne, typerne af behandlinger af personoplysninger samt den dataansvarliges instruks beskrevet. Den konkrete adgang til de digitale læremidler gives enten via Styrelsen for IT og Lærings ("STIL") login løsning, Unilogin eller Gyldendals egen loginløsning.

3.2.2 Behandling af personoplysninger

Gyldendals behandlinger på vegne af den dataansvarlige drejer sig primært om:

- Opbevaring af de data, som den dataansvarliges brugere (ansatte, elever, kursusdeltagere og øvrige brugere) indtaster på de platforme, som brugerne har adgang til via. den dataansvarliges licenser hos Gyldendal.
- Administration af kursusaktivitet med administration af brugere og tilknyttede læringsmoduler.
- Behandling af anonymiserede anvendelsesdata til brug for rapportering til den dataansvarlige om anvendelsen/udnyttelsen af den dataansvarliges licenser.
- Support af brugere ifm. tjenester Gyldendal udbyder. I denne forbindelse behandles der oplysninger i fornødent omfang, såsom navn, kontaktoplysninger og bruger-ID.

Indsamling af oplysninger om de registreredes brug af de digitale læremidler – herunder besvarelser – sker kun i det omfang, det er nødvendigt for at levere de digitale læremidler. Alle øvrige behandlinger – herunder effektuering af den registreredes rettigheder – udføres alene efter den dataansvarliges instruks.

3.2.3 Organisatoriske sikkerhedsforanstaltninger

Gyldendal A/S har flere ansatte, der beskæftiget sig fuld tid med IT- og cybersikkerhed. Der arbejdes målrettet med at sikre fortrolighed, integritet og tilgængelighed i vores løsninger, og vi arbejder kontinuerligt for at sikre et passende sikkerhedsniveau, således at kvaliteten i vores produkter lever op til både Gyldendals, kunders og de registreredes krav og behov.

Nedenstående tiltag er implementeret med henblik på at sikre et passende sikkerhedsniveau.

Listen indgår de i denne rapports vurderede tiltag, men er ikke begrænset hertil:

- Informationssikkerhedspolitik
- Retningslinjer for brug af IT
- Informationssikkerhedsudvalg – træffer principielle beslutning på overordnet niveau
- Change management
- Incident management
- Awarenesstræning
- Beredskabsplan og -øvelser

Gyldendals projektmodul indeholder IT-sikkerhedstrin i modellens kvalificeringsfase, således at sikkerheden altid vurderes forud for at en løsning bliver udviklet.

Når der foretages ændringer i programmer og databaser følges Gyldendals procedure på området, som har til formål at eliminere risikoen for fejl i processen fra udvikling til test og til produktion.

Gyldendal har en informationssikkerhedspolitik, der dækker hele organisationen. I denne beskrives de overordnede initiativer og retningslinjer for sikker behandling af personoplysninger, samt generel sikker behandling af IT. Som led i den løbende indsats for at styrke hensigtsmæssig brug af IT er der udarbejdet politikker, vejledninger og retningslinjer for håndtering af bl.a. IT, persondata og medier. Disse dokumenter fremsendes til relevante medarbejdere ved væsentlige ændringer og opdateringer. Dokumenter er altid tilgængelige på vores intranet, således at alle medarbejdere kan fremfinde dem efter behov.

Jura & Compliance sikrer, at Gyldendals generelle informationssikkerhedspolitik og persondatapolitik vedligeholdes og opdateres løbende. Gyldendal IT sikrer at retningslinjer for sikker behandling af IT opdateres løbende.

Gyldendal afholder løbende træning af medarbejdere. Dette sker via. et elektronisk træningsmodul, hvor den enkelte medarbejder uddannes i sikker håndtering af persondata og cybersikkerhed. Der føres kontrol med, at alle medarbejdere gennemfører modulet.

Ligeledes er der etableret funktionsadskillelse og begrænsede adgange til data efter rollebaseret behov, hvilket medfører adgangsminimering til de dataansvarliges data. Der udføres mindst en gang om året periodisk gennemgang af de udvidede rettigheder til sikring af, at tildelte adgangsrettigheder fortsat udgør et arbejdsbetinget behov.

Ved ansættelse af nye medarbejdere vurderer Gyldendal behovet for efterprøvning fra ansættelse til ansættelse og kan omfatte:

- Referencer fra tidligere ansættelser
- Straffeattest
- Eksamensbeviser

Der indhentes, som udgangspunkt altid referencer fra tidligere ansættelser, mens straffeattest og eksamensbeviser kun bliver indhentet, såfremt der er et særligt behov. Gyldendal gemmer ikke dokumentation for hvilken type af efterprøvning af ansættelse, der er blevet foretaget.

Gyldendal pålægger, ved ansættelse af nye medarbejdere, sine medarbejdere tavshedspligt, som medarbejdere ligeledes skriftligt gøres opmærksomme på fortsat er gældende ved fratrædelse.

3.2.4 Risikovurdering

Gyldendal har vurderet konsekvenserne for de registrerede i forhold til fortrolighed, integritet og tilgængeliglig ved behandlingerne af personoplysninger i forbindelse med leveringen af digitale læremidler. Herudover er den fulde systemportefølje risikovurderet i forhold til administrativt- og teknisk mitigerende tiltag med henblik på at implementere en passende grad af sikkerhed.

Gyldendal arbejder kontinuerligt med IT- og Cybersikkerhed og Gyldendal holder sig orienteret om potentielle trusler. Gyldendals risikometode er baseret på principperne fra ISO 27005, og de mitigerende tiltag er udvalgte kontroller fra hhv. SANS (Institute Critical Security Controls) og ISO27001 anneks A.

Det er Gyldendals vurdering, at Gyldendals behandlinger af oplysninger i forbindelse med leveringen af digitale læremidler medfører en lav risiko for den registrerede, som følge af behandlingernes natur samt de implementerede sikkerhedstiltag.

3.2.5 GDPR og Gyldendals rolle og ansvar som databehandler

Gyldendals bistand til den dataansvarlige

Som nævnt er Gyldendal databehandler ved levering af digitale læremidler til kunden, som dermed er dataansvarlig. Gyldendal understøtter den dataansvarliges forpligtelser til håndtering af den registreredes rettigheder – herunder fx besvarelser af anmodninger om indsigt. Til det formål har Gyldendal udarbejdet generelle procedurer for håndtering af den registreredes rettigheder, samt mere specifikke procedurer for Gyldendal ITs konkrete håndtering. Såfremt Gyldendal modtager en direkte henvendelse fra en registreret, anmodes den registrerede om først at rette henvendelse til den dataansvarlige.

Herudover har Gyldendal udarbejdet supplerende privatlivspolitikker til brugere af Gyldendals produkter, hvori det fremgår, at Gyldendal agerer som databehandler og behandler oplysningerne på vegne af den dataansvarlige.

Gyldendals sletteprincipper

Gyldendals sletterutiner er defineret i databehandleraftalen og de tilhørende ydelsesbilag. Gyldendal sletter udelukkende oplysninger på baggrund af den dataansvarliges instruks samt efter principperne beskrevet nedenfor.

Gyldendal sletter – herunder anonymiserer – data efter følgende principper:

1. På forlangende af dataansvarlige
2. Når Gyldendal modtager nye dataset – her forstås opdateret liste over registrerede tilknyttet en dataansvarlig – fra den dataansvarlige
3. Tidligst 90 dage og senest 18 måneder efter, at en registreret forlader en dataansvarlig

3.2.6 Gyldendals underdatabehandlere

I forbindelse med driften af de digitale læremidler benyttes en række underdatabehandlere. Gyldendal har indgået databehandleraftaler med disse, ligesom at der føres tilsyn med, at underdatabehandlerne overholder deres forpligtelser efter persondatalovgivningen og databehandleraftalen. Tilsyn føres ved undersøgelser af erklæringer og fysiske tilsyn, hvor dette er muligt og relevant.

Ved leveringen af digitale læremidler benytter Gyldendal følgende underdatabehandlere:

- **Adobe inc.** leverer Typekit til levering, tilpasning og styring af fonte
- **Amazon Web Services Ireland Ltd.** leverer hosting
- **Atlassian, Inc.** leverer systemet bag "sig din mening", hvor brugere kan kontakte Gyldendal direkte i relation til indholdet i iBøger®
- **Conscia Danmark A/S** implementerer og leverer driftsydelser for produkter under Gyldendal Ungdomsuddannelse og Videregående, der afvikles i Amazon Web Services' cloud
- **Dansk Sang, Musiklærerforeningens forlag** leverer som tredjepartsleverandør produktet DANSKSANGDIGITAL.DK, som Gyldendal sælger og markedsfører
- **Efaktum ApS** leverer talesyntese til iBøger®
- **Google Ireland, ltd.** Leverer infrastruktur til Gyldendals fagportaler, i-bøger samt arbejdsredskaber – fx e-mail
- **JW Player inc.** leverer mediaafspilning i produkterne samt statistik
- **Mentordanmark A/S** leverer, udvikler og vedligeholder "Vikarhylden"
- **Miracle A/S** implementerer og leverer driftsydelser for de af Gyldendal Grundskoles løsninger, der afvikles i Amazon Web Services' cloud
- **Microsoft Ireland Operations, Ltd.** Leverer O365, som bl.a. benyttes i Gyldendals interne kommunikation – navnlig i forbindelse med support. Microsoft leverer også Azures produkter, som Gyldendal anvender til at få sikkerhed, integrationer, ensartet monitorering samt et driftsstabilt resultat og brugere, som skalerer
- **Netic A/S** leverer platformsgateway for systemgenererede mails, der afsendes fra platformen – fx velkomstmails, herudover leverer Netic logmanagement til systemer hostet i AWS
- **New Relic Inc.** leverer værktøjer til monitorering af performance og oppetidsmåling
- **Redia A/S** udvikler og leverer fagportalen "Teknologiforståelse"
- **Sleeknote ApS** leverer kommunikationsredskaber til læreren i produkterne
- **TOPdesk Denmark A/S** Leverer et service managementsystem, som Gyldendal IT bruger til håndtering af Gyldendals it-sager, som i visse tilfælde kan indeholde personoplysninger.
- **@Ventures** udvikler og leverer webprøveplatformen til "Gyldendals Webprøver"
- **Wasabi Technologies, Inc** leverer en offsite backup ydelse
- **Writereader A/S** leverer som tredjepartsleverandør produktet Skriv og Læs, som Gyldendal sælger og markedsfører.

3.2.7 Gyldendals overførsel af oplysninger til tredjelande eller internationale organisationer:

Gyldendal overfører ikke oplysninger til tredjelande eller internationale organisationer uden forudgående specifik godkendelse fra den dataansvarlige.

Nogle af de underdatabehandlere, som Gyldendal anvender, er lokaliseret i USA, Australien eller er lokaliseret i EU som en del af en koncern hjemmehørende i USA. Gyldendal benytter disse leverandører på baggrund af EU-Kommissionens standardkontrakter ("SCC"), ligesom at Gyldendal løbende vurderer sikkerheden ved brugen af disse underleverandører. Data lagres kun i EU.

Der er tale om følgende amerikanske leverandører (se beskrivelser om anvendelse ovenfor):

- Microsoft Ireland Operations, Ltd.
- Google Ireland, Ltd.
- Amazon Web Services Ireland Ltd.
- Wasabi Technologies, Inc
- New Relic, inc.
- Adobe
- JW Player

Der er tale om følgende australske leverandører (se beskrivelser om anvendelse ovenfor):

- Atlassian, Inc.

3.3 Gyldendals typer af digitale læremidler

Gyldendals digitale læremidler kan inddeles i tre overordnede produktlinjer:

(1) Gyldendal Grundskole

(2) Gyldendal Ungdomsuddannelse

(3) Gyldendal Videre- og efteruddannelse.

Disse digitale produktlinjers behandling af personoplysninger beskrives nærmere i det følgende. Det skal bemærkes, at den konkrete behandling altid afhænger af, hvilke produkter den dataansvarlige har tegnet licenser på.

Den dataansvarlige skal derfor altid orientere sig i den seneste version af databehandleraftalens ydelsesbilag. Denne beskrivelse er udarbejdet med henblik på at give den dataansvarlige et overblik over hvilke behandlinger, der typisk foretages på baggrund af de produktkategorier, som den dataansvarlige har tegnet licenser på.

3.3.1 Gyldendal – Grundskole:

Applikations-/platformsbeskrivelse

Gyldendals produkter til grundskolen (herefter "Grundskoleprodukterne") består primært af fagportaler til alle grundskolens fag – fx dansk.gyldendal.dk. Derudover består produktporteføljen hovedsageligt af en lang række af i-bøger der udgives i tilknytning til bogsystemer, webprøver og træningsprodukter.

Grundskoleprodukterne falder i følgende to hovedkategorier:

- Gyldendals egne ydelser
- Tredjepartsydelser, som Gyldendal markedsfører.

Grundskoleprodukternes ydelsers formål er at udvikle, vedligeholde og drifte ydelserne på platforme og med faste underdatabehandlere.

Tredjepartsydelser er produkter, som Grundskoleprodukterne markedsfører, men som udvikles og driftes af en tredjepartsleverandør. Tredjepartsydelserne integreres i Grundskoleprodukternes sikkerhedsregime, for så vidt angår brug og validering af Unilogin. Tredjepartsleverandøren får således ikke en direkte adgang til STIL via Gyldendal. Gyldendal anser tredjepartsleverandører som underdatabehandlere og foretager tilsyn med disse på tilsvarende niveau som øvrige underdatabehandlere.

På tidspunktet for erklæringens udarbejdelse markedsfører Gyldendal disse tredjepartsleverandører:

- **Skriv og læs,** som er et læringsværktøj til den første læsning og skrivning
- **DANSKSANGDIGITAL.DK**, som er en fagportal til musikundervisning i 1.-6. klasse

Tekniske sikkerhedsforanstaltninger

Gyldendal vurderer løbende, hvilke praktiske sikkerhedstiltag der skal indgå i vores løsninger. Vi forholder os til aktuelle trusler og mulige mitigerende tiltag for at afværge sådanne trusler, ligesom vi løbende vurderer nye typer af sikkerhedsmålrettet IT for på den måde at sikre, at vi kontinuerligt tilpasser vores arbejde med sikring af data.

For Grundskoleprodukterne er der etableret funktionsadskillelse og begrænsede adgange til data efter rollebaseret behov, hvilket medfører adgangsminimering til de dataansvarliges data.

Der er implementeret en change- og release log for Grundskoleprodukterne for at tracke ændringer foretaget i vores systemer, samt for at kunne lokalisere og forklare evt. sikkerhedsbrister.

Der er ligeledes implementeret et SIEM-system på relevante logfiler, så Gyldendal bliver advaret ved mistænkelig adfærd – fx ved tildeling af udvidede rettigheder. Derudover har vi sikret Grundskoleprodukterne ved kryptering, firewall, antivirussystemer, endpoint protection og overvågning.

Ved tilgang fra en ikke-Gyldendal lokation er det påkrævet at være logget på via Gyldendals VPN for at kunne tilgå Gyldendals netværk. Gyldendal har desuden i foråret 2021 implementeret multi-faktor-autentificering (MFA) for dets medarbejdere ved tilgang via VPN til Gyldendals systemer.

Herudover arbejdes der med kunstige data udviklet af STIL i vores test- og udviklingsmiljøer, hvorfor der aldrig indgår personhenførbare data i vores udvikling og test.

Endvidere har Gyldendal implementeret formaliserede og ledelsesgodkendte backupprocedurer, hvilket bevirker, at vi i tilfælde af en sikkerhedsbrist kan reetablere vores servere.

Derudover har Gyldendal implementeret kontroller til sikring af indhentelse af erklæringer fra underdatabehandlere om overholdelse af persondatalovgivningen. Kontrollerne sikrer, at alle erklæringer vurderes ud fra et sikkerhedsperspektiv.

Det skal bemærkes, at ovenstående gennemgang udgør i denne rapport, vurderede tiltag, men ikke begrænset hertil.

Tredjepartsleverandører benytter sig af Grundskoleprodukternes loginløsning, og afhængigt af produktets karakter behandles personoplysninger i produkterne som angivet nedenfor under punktet "Personoplysninger" (jf. i øvrigt databehandleraftalens bilag 4a-4d).

Personoplysninger

I henhold til standarddatabehandleraftalen behandles følgende almindelige, ikke-følsomme personoplysninger om de registrerede:

- Navn, institutionstilknytning, rolle, klasse- og holdrelation
- Opgavebesvarelser og -resultater af forskellig karakter
- Progessionsdata i forbindelse med opgaveløsningen i visse produkter
- Dialog mellem lærer og elev vedrørende de enkelte opgavebesvarelser og -resultater
- Noter
- Brugeradfærd

Kategorier af registrerede personer, der er omfattet af standarddatabehandleraftalen:

- Elever
- Lærere
- Andre ansatte, som den dataansvarlige måtte give adgang til Grundskoleprodukternes systemer og løsninger.

3.3.2 Gyldendal – Ungdomsuddannelse

Applikations-/platformsbeskrivelse

På ungdomsuddannelsesområdet figurerer to brands som afsendere af Ungdomsuddannelsesprodukterne (tilsammen "Ungdomsuddannelsesprodukterne"). Systime står som afsender på produkterne til de gymnasiale ungdomsuddannelser, og Gyldendal står for erhvervsuddannelserne. På hele ungdomsuddannelsesområdet udgives og driftes alt overvejende iBøger® og iBiblioteket®.

Tekniske sikkerhedsforanstaltninger

Gyldendal vurderer løbende, hvilke praktiske sikkerhedstiltag der skal indgå i vores løsninger. Vi forholder os til aktuelle trusler og mulige mitigerende tiltag for at afværge sådanne trusler, ligesom vi løbende vurderer nye typer af sikkerhedsmålrettet IT for på den måde at sikre, at vi kontinuerligt tilpasser vores arbejde med sikring af data.

For Ungdomsuddannelsesprodukterne er der etableret funktionsadskillelse og begrænsede adgange til data efter rollebaseret behov, hvilket medfører adgangsminimering til de dataansvarliges data.

Der er implementeret en change- og release log for Ungdomsuddannelsesprodukterne for at tracke ændringer foretaget i vores systemer, samt for kunne lokalisere og forklare evt. sikkerhedsbrister.

Der er ligeledes implementeret et SIEM-system på udvalgte logfiler, så Gyldendal bliver advaret ved mistænkelig adfærd – fx ved tildeling af udvidede rettigheder. Derudover har vi sikret Ungdomsuddannelsesprodukterne ved kryptering, firewall, antivirussystemer, endpoint protection og overvågning af fysiske servere og ved tilgang fra en ikke-Gyldendal lokation er det påkrævet at være logget på via Gyldendals VPN for at kunne tilgå Gyldendals netværk. Gyldendal har desuden i foråret 2021 implementeret multi-faktor-autentificering (MFA) for dets medarbejdere ved tilgang via VPN til Gyldendals systemer.

Endvidere har Gyldendal implementeret formaliserede og ledelsesgodkendte backupprocedurer, hvilket bevirker, at vi i tilfælde af en sikkerhedsbrist kan reetablere vores servere.

Herudover har Gyldendal implementeret kontroller til sikring af indhentelse af erklæringer fra underdatabehandlere om overholdelse af persondatalovgivningen. Kontrollerne sikrer, at alle erklæringer vurderes ud fra et sikkerhedsperspektiv.

Det skal bemærkes, at ovenstående gennemgang udgør i denne rapport, vurderede tiltag, men ikke begrænset hertil.

Personoplysninger

I henhold til standarddatabehandleraftalen behandles følgende almindelige personoplysninger om de registrerede:

- Navn, e-mail, institutionstilknytning, uddannelsesretning, rolle og i visse produkter endvidere klasse- og holdrelationer
- Opgavebesvarelser og -resultater af forskellig karakter
- Progessionsdata i forbindelse med opgaveløsningen i visse produkter
- Dialog mellem lærer og elev vedrørende de enkelte opgavebesvarelser og -resultater
- Noter
- Anvendelsesdata

Kategorier af registrerede personer, der er omfattet af standarddatabehandleraftalen:

- Elever
- Lærere
- Andre ansatte, som den dataansvarlige måtte give adgang til Gyldendal Ungdomsuddannelses systemer og løsninger.

3.3.3 Gyldendal – Videregående- og efteruddannelse

Applikations-/platformsbeskrivelse

På dette område arbejder Gyldendal med flg. brands og produkter:

- På voksenuddannelsesområdet udgiver Gyldendal primært iBøger®.
- På videregående uddannelser udgiver Munksgaard og Hans Reitzels Forlag primært iBøger® - dog suppleret af enkelte videoportaler som fx Highlight og MerkantilPlay
- Guide2know udgiver e-learning (herefter ”Gyldendal E-learning”) primært som LMS og E-learning-moduler.

iBøgerne og videoportalerne er web-baserede, dvs. administratorer og brugere logger på via. en hjemmeside, for at opnå adgang.

LMS’et indeholder to portaler – Administrationsportalen og (en eller flere) læringsportaler.

LMS’et kan leveres sammen med en række ydelser fx integration af organisations- og brugerdata til kundens egne systemer (ADFS-integration) samt levering til borgerens digitale postkasse (E-Boks).

Tekniske sikkerhedsforanstaltninger

Gyldendal vurderer løbende, hvilke praktiske sikkerhedstiltag der skal indgå i vores løsninger. Vi forholder os til aktuelle trusler og mulige mitigerende tiltag for at afværge sådanne trusler, ligesom vi løbende vurderer nye typer af sikkerhedsmålrettet IT for på den måde at sikre, at vi kontinuerligt tilpasser vores arbejde med sikring af data.

For Videregående- og efteruddannelse er der etableret funktionsadskillelse og begrænsede adgange til data efter rollebaseret behov, hvilket medfører adgangsminimering til de dataansvarliges data.

Der er implementeret en change- og release log for Videregående- og efteruddannelse for at tracke ændringer foretages i vores systemer samt for kunne lokalisere og forklare evt. sikkerhedsbrister.

Der er ligeledes implementeret et SIEM-system på udvalgte logfiler, så Gyldendal bliver advaret ved mistænkelig adfærd – fx ved tildeling af udvidede rettigheder. Derudover har vi sikret Videregående- og efteruddannelse ved kryptering, firewall, antivirussystemer, endpoint protection og overvågning af fysiske servere og ved tilgang fra en ikke-Gyldendal lokation er det påkrævet at være logget på via Gyldendals VPN for at kunne tilgå Gyldendals netværk. Gyldendal har desuden i foråret 2021 implementeret multi-faktor-autentificering (MFA) for dets medarbejdere ved tilgang via VPN til Gyldendals systemer.

Endvidere har Gyldendal implementeret formaliserede og ledelsesgodkendte backupprocedurer, hvilket bevirker, at vi i tilfælde af en sikkerhedsbrist kan reetablere vores servere.

Herudover har Gyldendal implementeret kontroller til sikring af indhentelse af erklæringer fra underdatabehandlere om overholdelse af persondatalovgivningen. Kontrollerne sikrer, at alle erklæringer vurderes ud fra et sikkerhedsperspektiv.

Det skal bemærkes, at ovenstående gennemgang udgør i denne rapport, vurderede tiltag, men ikke begrænset hertil.

Personoplysninger

I henhold til standarddatabehandleraftalen behandles følgende almindelige personoplysninger om de registrerede:

- Navn, institutionstilknytning, rolle, klasse- og holdrelation
- Opgavebesvarelser og -resultater af forskellig karakter
- Progessionsdata i forbindelse med opgaveløsningen i visse produkter
- Dialog mellem lærer og elev vedrørende de enkelte opgavebesvarelser og -resultater
- Noter
- Brugeradfærd

Herudover kan der – afhængigt af brugen – behandles følgende, yderligere oplysninger i LMS:

- Kontaktoplysninger, E-mail og organisatorisk tilhørsforhold (fx HR-afdeling, Virksomhed X)
- Indsamling kan i visse tilfælde omfatte uddannelsesmæssigt baggrund / stilling (Sygeplejerske, SOSU. Mv.).
- Personoplysningerne i de borgerrettede moduler indeholder også cpr-numre, der anvendes til integration med den digitale postkasse på borger.dk

Der behandles følgende kategorier af registrerede:

- Elever
- Lærere
- Ansatte (fx medarbejdere og ledere i kommuner)
- Borgere (fx ledige med kontakt til jobcentre)
- Andre ansatte, som den dataansvarlige måtte give adgang til Gyldendal Ungdomsuddannelses systemer og løsninger

3.4 Kontrolmål og – aktiviteter

Kontrolmål og -aktiviteter fremgår af afsnit 4

3.5 Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige er selv ansvarlig for at anvende Gyldendal på en måde, der er i overensstemmelse med lovgivningens krav. Dette omfatter blandt andet, at kunden som dataansvarlig er ansvarlig for:

- At den fornødne hjemmel til behandlingen, jf. art. 6, er til stede
- At sikre fornøden oplysning til de registrerede om udøvelsen af deres rettigheder og kontrollere identiteten af de registrerede, der ønsker at udøve deres rettigheder
- At behørigt orientering af den registrerede iht. art. 13
- At kontrollere identiteten på den, der anmoder om berigtigelse
- At kontrollere identiteten på den, der anmoder om sletning
- At sikre at instruksen er lovlig set i forhold til den til enhver tid gældende databeskyttelsesretlige regulering
- At sikre at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen
- At sikre at den dataansvarliges brugere er ajourførte
- At sikre at udøvelsen af den registreredes rettigheder sker rettidigt, herunder besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag
- At eventuelle integrationer til andre systemer overholder lovgivningen.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurerne er opdateret.	Ingen væsentlige bemærkninger.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	Inspiceret, at ledelsen sikrer, at behandlingen af personoplysninger alene foregår i henhold til instruks. Inspiceret ved stikprøver af behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen væsentlige bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet, i tilfælde hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Ingen væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurerne er opdateret. Inspiceret ved stikprøver af databehandleraftaler, at der er etableret de aftalte sikkerhedsforanstaltninger.	Ingen væsentlige bemærkninger.
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 sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandleren foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandleren har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Ingen væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Inspiceret, at antivirussoftware er opdateret.	Vi har noteret i vores stikprøvetest, at der ikke er installeret antivirus på Linux servere i relation til de Systime produkter under Gyldendal Ungdomsuddannelse og Gyldendal Videregående uddannelse, der anvender AWS baserede Cloudløsning. Gyldendal har oplyst, at dette forhold ikke påvirker Gyldendal Grundskole eller Gyldendal Efteruddannelse produkterne. Ingen yderligere væsentlige bemærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor.	Ingen væsentlige bemærkninger.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.6	Adgang til personoplysninger er isoleret til brugere med et arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret ved stikprøver på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen væsentlige bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • PRTG - Landskabsovervågning • Logning	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret ved stikprøver af alarmer, at der er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Ingen væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Ingen væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test

B.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold:
	• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
	• Sikkerhedshændelser omfattende:
	  ○ Ændringer i logopsætninger, herunder deaktivering af logning
	  ○ Ændringer i systemrettigheder til brugere
	  ○ Fejlede forsøg på log-on til systemer, databaser og netværk
	
	Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.
		Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang af og opfølgning på logge.
		Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.
		Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og sletning.
		Inspiceret ved stikprøver af logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser.
		Inspiceret ved stikprøver af logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.
			Ingen væsentlige bemærkninger.

B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	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. Inspiceret ved stikprøver på udviklings- og testdatabaser, at personoplysningerne heri er pseudonymiseret eller anonymiseret. Inspiceret ved stikprøver på udviklings- og testdatabaser, hvor personoplysningerne ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Ingen væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt til de dataansvarlige i behørigt omfang.	Ingen væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Vi har konstateret i vores stikprøve test af ændringer, at der for 4 ud af 20 ændringer ikke har været muligt at modtage tilstrækkelig dokumentation for, at de blevet formelt godkendt inden de blev lagt i produktion. Gyldendal har oplyst, at disse 4 ændringer ikke indeholder ændringer, der påvirker persondata. Vi har desuden konstateret, at der i relation til de Systime produkter under Gyldendal Ungdomsuddannelse og Gyldendal Videregående uddannelse ikke kan fremskaffes tilstrækkelige dokumentation for, at der er gennemført test inden ændringer bliver lagt i produktion, samt blevet oplyst, at der ikke er etablerede systemunderstøttet funktionsadskillelse af miljøerne DEV, TEST, QA, PROD. Gyldendal har oplyst, at dette forhold ikke påvirker Gyldendal Grundskole eller Gyldendal Efteruddannelse produkterne. Ingen yderligere væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, herunder om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved stikprøver på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved stikprøver på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for en regelmæssig – mindst årlig – vurdering og godkendelse af tildelte brugeradgange.	Ingen væsentlige bemærkninger.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede, sker som minimum ved anvendelse af tofaktorautentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.	Vi har konstateret, at Gyldendal fra foråret 2021 har implementeret multifaktorautentifikation på VPN for alle brugere. Ingen yderligere væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Ingen væsentlige bemærkninger.

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen væsentlige bemærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved stikprøver af databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.	Ingen væsentlige bemærkninger.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved stikprøver på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved stikprøver af nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at der er foretaget efterprøvningen i forbindelse med ansættelsen.	Ingen væsentlige bemærkninger.

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.4	Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver medarbejderne introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejdernes behandling af personoplysninger.	Inspiceret ved stikprøver af nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved stikprøver af nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information.	Ingen væsentlige bemærkninger.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelsen, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Inspiceret ved stikprøver af fratrådte medarbejdere i erklæringsperioden, at rettighederne er inaktiveret eller ophørt, samt at aktiverne er inddraget.	Vi har konstateret i vores stikprøvetest af fratrådte medarbejdere, at der er enkelte fratrådte medarbejdere, hvor de tilhørende brugere ikke er blevet nedlagt rettidigt. Ingen af disse brugere har dog været anvendt efter medarbejdere er fratrådt. Ingen yderligere væsentlige bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved stikprøver af fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen væsentlige bemærkninger.

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen væsentlige bemærkninger.

Kontrolmål D:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen væsentlige bemærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved stikprøver af databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved stikprøver af databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysningerne er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen væsentlige bemærkninger.
D.3	Ved ophør af behandlingen 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.	Inspiceret, at der foreligger formaliserede procedurer for behandlingen af den dataansvarliges data ved ophør af behandlingen af personoplysninger. Inspiceret ved stikprøver af ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen væsentlige bemærkninger.

Kontrolmål E:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved stikprøver af databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen væsentlige bemærkninger.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved stikprøver af databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, 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 væsentlige bemærkninger.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen væsentlige bemærkninger.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved stikprøver af underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen væsentlige bemærkninger.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelsen af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelsen af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændringer i anvendelsen af underdatabehandlerne i erklæringsperioden.	Ingen væsentlige bemærkninger.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved stikprøver af underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen væsentlige bemærkninger.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen væsentlige bemærkninger.
F.6	På baggrund af en ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, foretager databehandleren en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen væsentlige bemærkninger.

Kontrolmål H:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

Nr.	Databehandlerens kontrolaktivitet	PwC's 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen væsentlige bemærkninger.
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.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen væsentlige bemærkninger.

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at procedurerne er opdateret.	Ingen væsentlige bemærkninger.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafikken overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, hvis der er mistanke om behov for opfølgning.	Ingen væsentlige bemærkninger.

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden. Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen væsentlige bemærkninger.

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Disse procedurer skal indeholde anvisninger på beskrivelser af: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede anvisninger på: • 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. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen væsentlige bemærkninger.