www.pwc.dk

# *Gyldendal A/S*

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2020 til 31. december 2020 i henhold til standard databehandleraftale i relation til Gyldendal Uddannelses digitale læremidler

*Marts 2021*

# 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 digitale læremidler.

Medfølgende beskrivelse er udarbejdet til brug for Gyldendals kunder, der har anvendt Gyldendal Uddannelses 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:

- Miracle A/S
- Amazon Web Services Ireland Ltd.
- @ventures
- Redia A/S
- Substy A/S
- Systime A/S
- Guide2know ApS
- Tibalo ApS
- New Relic Inc.
- Adobe Inc.
- Jw Player
- Sleeknote ApS
- Sentia A/S
- Keen IO (USA)
- Knewton Inc. (USA)
- Microsoft Ireland Operations, Ltd. (O365 og Azure)
- TOPdesk Denmark A/S.

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

Gyldendal bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af informationssikkerhed og foranstaltninger i relation til Gyldendal Uddannelses digitale læremidler, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne i hele perioden fra 1. januar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan informationssikkerhed og foranstaltninger i relation til Gyldendal Uddannelses digitale læremidler var udformet, 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 Gyldendal Uddannelses 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 Gyldendal Uddannelses digitale læremidler til behandling af personoplysninger foretaget i perioden fra 1. januar 2020 til 31. december 2020

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne informationssikkerhed og de beskrevne foranstaltninger i relation til Gyldendal Uddannelses digital 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 Gyldendal Uddannelses 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 2020 til 31. december 2020. 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 2020 til 31. december 2020.

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.

København, den 24. marts 2021
**Gyldendal A/S**

Hanne Salomonsen
Direktør

# 2. Uafhængig revisors erklæring

**Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2020 til 31. december 2020 i henhold til standard databehandleraftale i relation til Gyldendal Uddannelses digitale læremidler**

Til: Gyldendal A/S og dataansvarlige i relation til Gyldendal Uddannelses digitale læremidler

**Omfang**

Vi har fået som opgave at afgive erklæring om Gyldendal A/S' (Gyldendal) beskrivelse i afsnit 3 af informationssikkerhed og foranstaltninger i relation til Gyldendal Uddannelses digitale læremidler i henhold til standard databehandleraftale med dataansvarlige i relation til Gyldendal Uddannelses digitale læremidler i hele perioden fra 1. januar 2020 til 31. december 2020 (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:

- Miracle A/S
- Amazon Web Services Ireland Ltd.
- @ventures
- Redia A/S
- Substy A/S
- Systime A/S
- Guide2know ApS
- Tibalo ApS
- New Relic Inc.
- Adobe Inc.
- Jw Player
- Sleeknote ApS
- Sentia A/S
- Keen IO (USA)
- Knewton Inc. (USA)
- Microsoft Ireland Operations, Ltd. (O365 og Azure)
- TOPdesk Denmark A/S.

Erklæringen anvender partielmetoden og omfatter ikke kontroller, som disse 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 FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

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 retvisende, 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 informationssikkerhed og foranstaltninger i relation til Gyldendal Uddannelses digitale læremidler samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet 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 Gyldendal Uddannelses 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 Gyldendal Uddannelses digitale læremidler, således som disse var udformet i hele perioden fra 1. januar 2020 til 31. december 2020, 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 hensigtsmæssigt udformet i hele perioden fra 1. januar 2020 til 31. december 2020, 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 2020 til 31. december 2020.

## 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 Gyldendal Uddannelses 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 24. marts 2021
**PricewaterhouseCoopers**
Statsautoriseret Revisionspartnerselskab

Jess Kjær Mogensen
statsautoriseret revisor

Bo Petersen
director

# 3. Beskrivelse af behandling

## Indledning

Formålet med Gyldendals behandling af personoplysninger på vegne af den dataansvarlige er følgende: Gyldendal leverer og drifter en række digitale læremidler for den dataansvarlige såsom fagportaler, i-bøger og webprøver. Adgang til de læremidler, der stilles til rådighed for lærere og andre ansatte samt elever, gives via Uni-Login, som dermed danner basis for registreringen af personhenførbare data.

Der er indgået databehandleraftale mellem den dataansvarlige og Gyldendal, hvilket er en forudsætning for anvendelse af Uni-Login-komplekset, ligesom karakteren af de digitale læremidler i sig selv nødvendiggør en databehandleraftale.

Aftaleforholdene er varierende. I mange tilfælde stilles læremidlerne til rådighed på baggrund af en hovedaftale indgået mellem Gyldendal og en kommune på vegne af kommunens skoler. I andre tilfælde er hovedaftalen indgået mellem den enkelte folkeskole og Gyldendal. I begge tilfælde betragtes kommunen som den egentlige dataansvarlige, og det er kommunen, som databehandleraftalen er indgået med. Er der tale om privatskoler og selvejende institutioner, indgås både hovedaftaler og databehandleraftaler med den enkelte institution, som selv er dataansvarlig.

I alle tilfælde behandler Gyldendal i medfør af disse aftaler personoplysninger for den dataansvarlige, fx i form af opgavebesvarelser, progressionsdata, noter, testresultater mv.

## Karakteren af behandlingen

Gyldendals behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om:

1. Opbevaring af de data, som den dataansvarliges brugere (ansatte og elever) inddaterer på de platforme, som brugerne har adgang til via den dataansvarliges licenser hos Gyldendal
2. Behandling af anonymiserede anvendelsesdata til brug for rapportering til den dataansvarlige om anvendelsen/udnyttelsen af den dataansvarliges licenser
3. I forbindelse med udførelse af support til brugere af Gyldendals systemer og dennes underdatabehandleres platforme behandles relevante oplysninger vedrørende brugeren såsom navn, kontaktoplysninger, evt. bruger-ID eller oplysninger, der identificerer den institution, brugeren henvender sig på vegne af.

Gyldendal henter og gemmer alene de persondata, som er nødvendige for at levere de ydelser og services (uddannelsesprodukter), som Gyldendal og den dataansvarlige har indgået aftale om. Opsamling og lagring af viden om den registrerede baseret på dennes brug og besvarelser sker kun, i det omfang det er en forudsætning for levering af ovennævnte ydelser og services. Alle øvrige behandlinger, herunder effektuering af den registreredes rettigheder, vil alene blive udført efter den dataansvarliges instruks.

## Applikations-/platformsbeskrivelse

Gyldendals produkter falder i følgende to hovedkategorier:

- Gyldendals egne ydelser
- Tredjepartsydelser, som Gyldendal markedsfører.

Gyldendal Uddannelses egne ydelsers generelle formål og funktion er de samme. Således udvikles, vedligeholdes og driftes ydelserne på de samme platforme og med faste underdatabehandlere.

Tredjepartsydelserne er produkter, som Gyldendal Uddannelse markedsfører, men de udvikles og driftes af den tredjepartsleverandør, der har udviklet ydelsen. Gyldendal Uddannelse integrerer dem i sit sikkerhedsregime, for så vidt angår brug og validering af Uni-Login. Tredjepartsleverandøren får således ikke, via Gyldendal, direkte adgang til STILs Uni-Login-services.

## Underleverandører

De underleverandører, der er relevante for Gyldendal Uddannelses digitale læremidler, og hvor der er indgået databehandleraftaler, varetager følgende behandlinger:

- **Miracle A/S** implementerer og leverer driftsydelser for de af Gyldendal Uddannelses løsninger, der afvikles i Amazon Web Services' cloud, med undtagelse af få produkter der leveres direkte af Gyldendals it-afdeling.
- **Amazon Web Services Ireland Ltd.** leverer hosting af Gyldendal Uddannelses digitale læremidler.
- **@ventures** udvikler og leverer webprøveplatformen til "Gyldendals Webprøver"
- **Redia A/S** udvikler og leverer fagportalen "Teknologiforståelse"
- **Substy A/S** udvikler og leverer "Vikarhylden"
- **Systime A/S** udvikler og leverer Gyldendal Uddannelses i-bogsplatform til ungdomsuddannelser og erhvervsskoler
- **Guide2know ApS** udvikler, leverer og supporterer læringsportaler til erhvervsuddannelser, herunder portalerne "highlight", PsychSim, MerkantilPlay og SusoPlay
- **Tibalo ApS** udvikler og leverer adaptive læringsløsninger til matematiktræning
- **New Relic Inc.** leverer værktøjer til monitorering af performance og oppetidsmåling
- **Adobe** leverer Typekit til levering, tilpasning og styring af fonte
- **Jw Player** leverer medieafspilninger i produkterne samt statistik
- **Sleeknote ApS** leverer kommunikationsredskaber til læreren i produkterne
- **Sentia A/S** leverer infrastruktur, herunder netværk og hosting af Gyldendal Uddannelses webshop samt loginløsning og -data.
- **Keen IO (USA)** benyttes til at bygge statistik over brugen af Gyldendal Uddannelses produkter, således at de kontinuerligt kan forbedres og videreudvikles til gavn for brugerne. Keen IO har alene adgang til pseudonymiserede oplysninger, og disse undergår automatisk behandling hos Keen IO.
- **Knewton Inc. (USA) (udgået august 2020)** leverer adaptive læringsløsninger, der er integreret i Gyldendal Uddannelses SmartMat-produkt. Det er således kun, hvis den dataansvarlige har købt SmartMat, at der sker overførsel af oplysninger til Knewton. Gyldendal har i samarbejde med Norsk Gyldendal udviklet produktet SmartMat, og algoritmen til systemets adaptive funktioner ligger hos Knewton Inc. i USA. Knewton har alene adgang til brugernes pseudonymiserede opgavebesvarelser, som undergår automatisk behandling, således at systemet kontinuerligt præsenterer brugerne for opgaver, der passer til deres niveau.
- **Microsoft Ireland Operations, Ltd.** leverer O365, som bl.a. benyttes i Gyldendal Uddannelses interne kommunikation – navnlig i forbindelse med support. Microsoft leverer også Azures produkter, som Gyldendal Uddannelse anvender til at få sikkerhed, integrationer, ensartet monitorering samt et driftsstabilt resultat til kunder og brugere, som skalerer.
- **TOPdesk Denmark A/S** leverer et service managementsystem, som Gyldendal IT bruger til håndtering af Gyldendal Uddannelses it-sager, som i visse tilfælde kan indeholde personoplysninger.

På tidspunktet for erklæringens udarbejdelse markedsfører Gyldendal Uddannelse følgende tredjepartprodukter:

- **Skriv og læs**, som er et læringsværktøj til den første læsning og skrivning.
- **Ordheltene**, som er et digitalt læringsspil for ordblinde elever og begyndende læsere.
- **DANSKSANGDIGITAL.DK**, som er en fagportal til musikundervisningen i 1.-6. klasse.

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

Gyldendal Uddannelses webshop:

Ved at logge ind i Gyldendal Uddannelses webshop er det muligt at agere som indkøber inden for de rammer, der er fastsat i hovedaftalen med kommunen/uddannelsesinstitutionen. Ved indkøb på vegne af kommunen/uddannelsesinstitutionen tilføjes produkterne til kommunens/uddannelsesinstitutionens sortiment, hvorefter elever og lærere tilknyttet de relevante klasser vil kunne tilgå produkterne.

## Personoplysninger

I henhold til standard databehandleraftalen behandles følgende almindelige personoplysninger om de registrerede:

- Navn, institutionstilknytning, rolle, klasse- og holdrelationer
- Opgavebesvarelser og -resultater af forskellig karakter
- Progressionsdata i forbindelse med opgaveløsningen i visse produkter
- Dialog mellem lærer og elev vedrørende de enkelte opgavebesvarelser og -resultater
- Noter
- Brugeradfærd
- Købshistorik for kommunens/uddannelsesinstitutionens indkøbere.

Kategorier af registrerede personer, der er omfattet af standard databehandleraftalen:

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

## Governance – it-sikkerhed

Gyldendal arbejder målrettet med at sikre fortrolighed, integritet og tilgængelighed i vores løsninger og arbejder kontinuerligt for at sikre et passende sikkerhedsniveau, således at kvaliteten i vores produkter lever op til både Gyldendals og de registreredes behov.

Nedenstående tiltag er implementeret med henblik på at sikre, at der er eksisterende governance til at sikre et passende sikkerhedsniveau. Listen udgør de i denne rapport vurderede tiltag, men er ikke begrænset hertil.

- Informationssikkerhedspolitik
- Retningslinjer for brug af it
- It-sikkerhedsorganisation
- Change management
- Beredskabsplan og -øvelser.

Gyldendals projektmodel indeholder it-sikkerhedstrin i modellens kvalificeringsfase, således at sikkerheden altid vurderes, forud for at en løsning bliver udviklet, og således at det sikres, at Gyldendal imødekommer de behov for sikkerhedstiltag, en given behandling afstedkommer.

## Praktiske tiltag – it-sikkerhed

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.

Nedenstående praktiske tiltag er implementeret og beskrives nærmere nedenfor i art. 25 og 32. Listen udgør de i denne rapport vurderede tiltag, men er ikke begrænset hertil.

- Kryptering af data
- Funktionsadskillelse og begrænsede adgange til data efter et rollebaseret behov
- Test- og udviklingsmiljøer indeholder ikke personhenførbare data, men udelukkende til formålet skabte testdata
- Backup
- Firewall
- Antivirussystemer
- Målrettede løsninger til sikring af tilgængelighed, herunder backup og beredskabsplaner
- Logfiler med alarmer ved fx mistænkelig adfærd, eller hvis der tildeles udvidede rettigheder
- Endpoint protection, herunder kryptering, segmentering og central styring af devices
- Løbende måling og afprøvning af udvalgte kontroller.

### Risikovurdering

Gyldendal har på baggrund af de personoplysninger, som behandles i medfør af standard databehandleraftalerne, vurderet konsekvenserne for de registrerede på baggrund af fortrolighed, integritet og tilgængelighed. Gyldendal Uddannelses systemportefølje er risikovurderet. Der er vurderet på henholdsvis administrative og tekniske mitigerende tiltag før og efter en hændelse for på den måde at sikre, at data behandles med en passende grad af sikkerhed i forhold til de konkrete personoplysninger og de behandlinger, som foretages på vegne af den dataansvarlige.

Gyldendals risikometode er baseret på principperne fra ISO 27005. De mitigerende tiltag er valgt på baggrund af hhv. SANS Institute Critical Security Controls, som sikrer et højt teknisk sikkerhedsniveau samt udvalgte og relevante kontroller fra ISO 27001 anneks A for på den måde at sikre data på flere parametre.

Det er Gyldendals vurdering, at der ikke er tale om høj risiko for de registrerede, bl.a. på grund af typerne af behandlede personoplysninger.

## *Kontrolforanstaltninger*

Følgende er en beskrivelse af, hvilke kontrolforanstaltninger Gyldendal har iværksat og gennemført til måling og kontrol af personoplysninger samt resultatmålinger herfra.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

En række artikler i databeskyttelsesforordningen er ikke fundet egnede i forhold til udarbejdelsen af kontrolmål i denne erklæring. Dette drejer sig om følgende artikler, da disse:

- ikke er målbare (artiklerne 1, 2, 3 og 4)
- ikke er relevante i forhold til Gyldendals rolle som databehandler (artiklerne 7, 8, 14, 15, 21, 22, 23, 26, 27, 31 og 36)
- vedrører specifikke typer behandlinger, som Gyldendal ikke foretager (artiklerne 9, 10, 11 og 20)
- vedrører opfyldelsen af formelle krav, som Gyldendal ikke er underlagt (artiklerne 37, 38, 39, 40, 41, 42, 43 og 51-99).

### Artikel 5. Principper for behandling af personoplysninger

Gyldendal har implementeret en række initiativer for at sikre, at indsamlingen, behandlingen og opbevaringen af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.

Som en del af Gyldendals kernedrift er der udarbejdet en informationssikkerhedspolitik, der dækker hele organisationen, herunder Gyldendal Uddannelse. I denne beskrives initiativer og retningslinjer for sikker

behandling af personoplysninger samt generel sikker behandling af it. Som led i en løbende indsats for at styrke vores interne brug af it er der desuden udarbejdet en række interne guides og retningslinjer for håndtering af bl.a. it, persondata og medier. Alle procedurer og politikker fremsendes til relevante medarbejdere ved ændring og opdatering. I øvrigt er disse procedurer og politikker altid tilgængelige på vores intranet, således at alle medarbejdere kan fremfinde dem efter behov.

Jura & Compliance sikrer, at Gyldendals generelle informationssikkerhedspolitikken og persondatapolitik vedligeholdes, opdateres og fremlægges for ledelsen mindst hvert andet år. Gyldendal IT sikrer, at retningslinjer for sikker behandling af it opdateres løbende.

I 2019 har Gyldendal som led i implementeringen af sunde GDPR-procedurer afholdt løbende træning af alle medarbejdere. Dette sker via et træningsmodul, hvor den enkelte medarbejder uddannes i sikker håndtering af persondata, herunder de personfølsomme oplysninger, medarbejderne måtte komme i berøring med. Gyldendal foretager kontrol af, hvorvidt alle medarbejdere har gennemført modulet.

### Komplementerende kontroller hos de dataansvarlige, art. 5

Den dataansvarlige har følgende forpligtelser:

- At sikre, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering
- At sikre, at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen
- At sikre, at den dataansvarliges brugere er ajourførte.

### Art. 6. Lovlig behandling

Der er indgået databehandleraftaler med kommuner og de enkelte uddannelsesinstitutioner. Der rykkes jævnligt for databehandleraftaler hos de dataansvarlige, som endnu ikke har underskrevet en aftale med Gyldendal. I databehandleraftalens bilag 4.1 med tilhørende underbilag er ydelsen og typerne af den databehandling, der finder sted, beskrevet. I bilag 3 er den dataansvarliges instruks til Gyldendal beskrevet.

Gyldendal har indgået databehandleraftaler med underleverandører, og Gyldendal sikrer underleverandørernes overholdelse af deres forpligtelser i relation til persondatalovgivningen ved erklæringer og fysiske tilsyn, hvor dette vurderes relevant.

Gyldendals it-projektmodel indeholder sikkerhedstrin, der er integreret i modellens kvalifikationsfase, således at sikkerheden og lovligheden altid vurderes, før en løsning bliver udviklet, og således at det sikres, at Gyldendal imødekommer de behov for sikkerhedstiltag, en given behandling afstedkommer.

### Komplementerende kontroller hos de dataansvarlige, art. 6

Den dataansvarlige er ansvarlig for at sikre, at den fornødne hjemmel til behandlingen, jf. art. 6, er til stede.

### Art. 12. Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelse af den registreredes rettigheder

Den dataansvarlige sørger for oplysning om behandlingen til de registrerede. Gyldendal har på Gyldendal Uddannelses hovedside lagt en supplerende persondatapolitik til brugere af Gyldendals Uddannelses digitale læremidler, hvoraf det fremgår, at Gyldendal er databehandler og behandler oplysninger på den dataansvarliges vegne, og at den registrerede skal kontakte den dataansvarlige, hvis den registrerede ønsker at gøre brug af sine rettigheder.

Gyldendal understøtter den dataansvarliges forpligtelser til at fremfinde data, der er indsamlet om en registeret, på anmodning fra den dataansvarlige og har udarbejdet en generel procedure for håndtering af den registreredes rettigheder samt en mere specifik procedure for Gyldendal IT's opgaver i relation til at fremfinde data.

Henvendelse fra en registreret skal gå via den dataansvarlige, til hvem Gyldendal sender de efterspurgte oplysninger i en overskuelig form, hvorefter den dataansvarlige sørger for at videregive informationen til den registrerede. Såfremt Gyldendal modtager direkte henvendelser fra en registreret vedrørende effektuering af rettigheder, anmodes den registrerede om først at rette henvendelsen til den dataansvarlige.

### Komplementerende kontroller hos de dataansvarlige, art. 12

Den dataansvarlige er ansvarlig for at sikre fornøden oplysning til de registrerede om udøvelsen af deres rettigheder og kontrollere identiteten af de registrerede, der ønsker at udøve deres rettigheder.

### Art. 13 – Oplysningspligt ved indsamling af personoplysninger hos den registrerede

Den dataansvarlige sikrer opfyldelse af oplysningspligten over for den registrerede. Gyldendal har i standard databehandleraftalen givet den dataansvarlige alle de fornødne oplysninger, som kan viderebringes til den registrerede. Gyldendal har endvidere på Gyldendal Uddannelses hovedside lagt en supplerende persondatapolitik til brugere af Gyldendal Uddannelses digitale læremidler, hvoraf det bl.a. fremgår, at kommunen eller uddannelsesinstitutionen er den dataansvarlige, hvilke oplysninger der indsamles om brugerne, og hvorfor oplysningerne behandles. Det fremgår endvidere, at der i visse tilfælde sker en overførsel af oplysningerne til it-leverandører og -samarbejdspartnere, herunder partnere i tredjelande (USA).

### Komplementerende kontroller hos de dataansvarlige, art. 13

Den dataansvarlige er ansvarlig for behørig orientering af den registrerede iht. art. 13.

### Art. 16/19 – Ret til berigtigelse

STIL er ansvarlig for data vedrørende Uni-Login. Når man som Uni-Login-bruger får rettet sine data hos STIL, vil de være rettet hos Gyldendal inden for 24 timer, da alle data fra STIL overskrives en gang i døgnet.

1. De lærere, som fungerer som indkøbere, kan selv logge ind og rette deres egne informationer.
2. Der er defineret ansvarsområder hos Gyldendal Uddannelse ved berigtigelse af persondata samt ansvarlige for sagshåndtering heraf ved henvendelse. Berigtigelse vil oftest fordre kontakt til den dataansvarlige.
3. Der er udarbejdet procedurer til at sikre, at Gyldendal ved henvendelse får rettet henvendelse alle relevante steder.

### Komplementerende kontroller hos de dataansvarlige, art. 16/19

Den dataansvarlige er ansvarlig for at kontrollere identiteten på den, der anmoder om berigtigelse.

### Art. 17/19 – Ret til sletning ("retten til at blive glemt")

I samarbejde med dataansvarlig har databehandler defineret regler for sletning af den registrerede.

Medmindre andet specifikt er defineret, sletter Gyldendal efter følgende regler:

Elever/lærer (ikke indkøber):

Profil: Oplysninger stammer fra STIL og overskrives en gang i døgnet, hvorfor profilen ikke længere eksisterer, hvis denne er fjernet fra STIL.

Brugergenereret data: Slettes på forlangende fra den dataansvarlige, eller når record er > 10 år gammel. Bemærk, at nye principper for sletning er under udarbejdelse og implementering.

Lærer som indkøber:

Profil: Slettes på forlangende fra den dataansvarlige, eller når der ikke har været logget ind i 3 år; hvis der ikke er tilknyttet licenser på elektroniske produkter, eller brugeren ikke har tilmeldt sig e-mails fra Gyldendal Uddannelse.

Brugergenererede data: Slettes på forlangende fra den dataansvarlige, eller når record er > 10 år gammel. Bemærk, at nye principper for sletning er under udarbejdelse og implementering.

Kunder, som køber ind på vegne af en kommune, skole eller institution:

Profil: Slettes på forlangende fra den dataansvarlige, eller når der ikke har været logget ind i 3 år; hvis der ikke er tilknyttet licenser på elektroniske produkter, eller brugeren ikke har tilmeldt sig e-mails fra Gyldendal Uddannelse.

Gyldendal er fortsat i dialog med Undervisningsministeriet om en evt. fastlæggelse af generelle sletteregler for læremidler.

Ved enkeltstående sletteopgaver kontakter den dataansvarlige Gyldendal, som opretter en specifik sletteopgave i Gyldendals serviceportal.

### Art. 17/19 – Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige er ansvarlig for at kontrollere identiteten på den, der anmoder om sletning.

### Art. 18/19 – Ret til begrænsning af behandling

Det er fastsat i standard databehandleraftalen, at Gyldendal på opfordring fra den dataansvarlige skal hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til den registreredes rettigheder, herunder bl.a. begrænsning af behandling af borgerens oplysninger.

### Art. 24 – Den dataansvarliges ansvar

Gyldendal har i standard databehandleraftalens bilag 1 og aftalens ydelsesbeskrivelser beskrevet, hvorledes Gyldendals tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger fungerer. De dataansvarlige har godkendt dette ved underskrivelse af standard databehandleraftalen.

Der henvises i øvrigt til gennemgangen under pkt. 32 for specifikke tiltag.

### Art. 25 – Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

Gyldendal Uddannelses systemer er rolleopdelt, der benyttes personlige brugerkonti/-navne, der stammer fra STIL hvor Gyldendal modtager skolegrunddata "Lille". Datasættets brug er begrænset til login samt i frontend hvor man efter login kan se sit eget navn i øverste højre hjørne; herudover gemmes data som indtastes i Gyldendals løsninger i kombination med unilogin og institutionstilknytning.

Gyldendal Uddannelse har sine egne administratorer, og brugere valideres enten via Uni-Login eller E-key. Ud fra en risikotilgang krypteres persondata i nødvendigt omfang. Når projekter igangsættes i Gyldendal, sker det efter en projektmodel, som i den indledende fase forudsætter vurdering af nødvendigheden af udarbejdelse af en konsekvensanalyse i projektet. Det sikres gennem projektmodellen, at der vurderes på risikoen for de registrerede, og dermed sikres det, at databeskyttelse er en integrerende del af designet.

Der er i Gyldendal Uddannelse etableret særskilte miljøer til test og udvikling. Data i disse miljøer indeholder ikke personhenførbare data, men udelukkende til formålet skabte testdata. Der er derudover implementeret change management-processer, således at ændringer til systemerne testes, registreres og vurderes af relevante medarbejdere forud for ændringer i produktionssystemerne.

### Art. 28/29 – Databehandler – Behandling, der udføres for den dataansvarlige eller databehandleren

Der er udsendt udkast til databehandleraftale til alle Gyldendal Uddannelses kunder, og der er indgået databehandleraftaler med hovedparten af kunderne. Der rykkes jævnligt for returnering af underskrevne aftaler eller dialog om aftalen hos de kunder, som endnu ikke har aftalen på plads.

Gyldendal Uddannelse benytter sig af en række forskellige underdatabehandlere, hvoraf nogle understøtter den egentlige drift, mens andre har udarbejdet supplerende digitale produkter, som indgår i Gyldendal Uddannelses portefølje. Der er indgået databehandleraftale med samtlige underdatabehandlere, der afspejler

de relevante krav i Gyldendals egen databehandleraftale med den dataansvarlige. Gyldendal Uddannelse benytter sig ligeledes af underdatabehandlere i USA. Der er sikret et gyldigt overførselsgrundlag i den forbindelse, se art. 44-50.

## Art. 30 – Fortegnelse over behandlingsaktiviteter

Gyldendal fører en fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige, jf. art. 30, stk. 2. Fortegnelsen gennemgås mindst én gang årligt af Jura & Compliance i samarbejde med Gyldendal Uddannelse og opdateres i den forbindelse, og når processer indeholdende håndtering af persondata ændres. (Ændringer af betydning for den dataansvarliges instruks vil, inden ændringen gennemføres, være behørigt varslet i overensstemmelse med det i standard databehandleraftalen fastsatte).

## Art. 32 – Behandlingssikkerhed

Gyldendal Uddannelse benytter sig primært af SQL-databaser og Windows-servere.

- Der er udarbejdet en samlet risikoanalyse i Neupart for Gyldendal, hvori Gyldendal Uddannelse indgår. Risikovurderingen er forelagt og godkendt af Gyldendal Uddannelses ledelse.
- Der bruges kodeord til OS og databaser og ved tilgang til applikationerne.
- Alle brugere af systemerne har unikke bruger-ID'er og identifikationer, hvad enten der er tale om slutbrugere eller medarbejdere hos Gyldendal.
- Der er HTTPS på alle Gyldendal Uddannelses portaler, og der sker kryptering af kodeord i systemerne.
- Der er installeret antivirus programmel på systemer der anvendes i forbindelse med Gyldendal Uddannelse. Disse opdateres løbende.
- Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, i forbindelse med Gyldendal Uddannelse, sker gennem sikret firewall.
- Der er brugeradministration af Gyldendals brugere i forbindelse med oprettelse, nedlæggelse og tildeling af udvidede rettigheder. Adgangsstyring mht. Gyldendals brugere sker via AD-grupper, så det er tydeligt, hvor der er tildelt adgang. Rettighederne bliver periodisk revideret hos IT og hos systemejerne. I samarbejde med HR bliver brugerne periodisk gennemgået mht. nedlæggelse og uautoriseret adgang.
- Der tages dagligt fuld backup af alle produktionsservere. Herudover tages der SQL-databasebackup efter følgende model: Fuld backup ugentligt, incremental backup dagligt og Transaction Log hvert 15. minut.
- Der foretages restore på systemerne minimum 10 gange årligt.
- Der er opsat logning i systemerne, fx ved ændring af data og kode samt brugeraktivitet på produkter, herunder aktivitets-, data- og versionshistorik. For logning gælder det, at Gyldendal løbende forholder sig til bedste praksis på området for logge samt anbefalede opbevaringsperioder.
- Der sker automatisk overvågning af loghændelser i Gyldendals SIEM-løsning, som alarmerer ved loghændelser, der vurderes at kunne udgøre en potentiel risiko, således at Gyldendals it-afdeling har mulighed for hurtigst muligt at reagere på evt. trusler.
- Der er udarbejdet en beredskabsplan, som testes årligt, og som efter hver test tilpasses og optimeres med henblik på at højne kvaliteten.
- Amazon i Irland hoster databaser i en cloudløsning, og Sentia i Danmark hoster den øvrige infrastruktur. Amazon er ISO 27001-certificeret, og Sentia udarbejder en revisionserklæring (ISAE 3402).
- Gyldendal indhenter revisionserklæringer fra Gyldendal Uddannelses underdatabehandlere (egenerklæringer fra underdatabehandlere) for at sikre, at der hos underdatabehandlere er en passende grad af sikkerhed. Gyldendal foretager fysiske besøg hos underdatabehandlere, hvor dette vurderes relevant.

- Der er udarbejdet retningslinjer for sikker brug af it, som sikrer awareness i organisationen. Retningslinjerne er henvendt til medarbejderne, således at disse er oplyst om, hvad der er tilladt og ikke tilladt på Gyldendals løsninger.
- Der er implementeret change management-processer, herunder test og validering af ændringer i systemerne.
- Gyldendal har implementeret kontroller til at sikre, at der indhentes erklæringer fra underdatabehandlerne om overholdelse af persondatalovgivningen. Kontrollerne sikrer, at alle erklæringer vurderes ud fra et sikkerhedsperspektiv. Der foretages fysiske tilsyn hos underdatabehandlerne, i det omfang dette skønnes relevant.

### Art. 33/34 – Underretning om brud på persondatasikkerheden til den registrerede

I beredskabsplanen findes en instruks for kommunikation til den dataansvarlige ved brud på den registreredes rettigheder. Instruksen sikrer, at Gyldendal ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidigt og fyldestgørende at foretage anmeldelse til tilsynsmyndigheden og til at underrette den/de registrerede, som er berørt af bruddet.

Incidents/sager vedrørende brud eller mistanke om brud på persondatasikkerheden vurderes og analyseres samt opbevares og kategoriseres. Der har i Gyldendal Uddannelse ikke været brud på persondatasikkerheden, siden persondataforordningen (GDPR) trådte i kraft.

Ved mistanke om brud på persondatasikkerheden analyserer Gyldendal altid hændelsen og vurderer, om der er tale om et brud på persondatasikkerheden, og hvilken risiko hændelsen måtte udgøre for de registrerede, der er omfattet af hændelsen.

### Art. 35 – Konsekvensanalyse vedrørende databeskyttelse

Når projekter igangsættes, eller der sker væsentlige ændringer i behandlingen af personoplysninger i Gyldendal, benyttes en projektmodel, som i den indledende fase forudsætter vurdering af nødvendigheden af udarbejdelse af en konsekvensanalyse i projektet.

### Art. 44-50 – Overførsel af personoplysninger til tredjelande eller internationale organisationer

1. Der overføres data til USA, hvor der er indgået databehandleraftaler med leverandørerne på EU-Kommissionens standardkontrakt.
2. De dataansvarlige har i standard databehandleraftalen specifikt accepteret overførsel til USA.

Der er tale om følgende amerikanske leverandører:

- **Keen IO**, som udarbejder statistikker over brugen af Gyldendal Uddannelses løsninger med henblik på at forbedre og videreudvikle disse løsninger. Keen IO har alene adgang til pseudonymiserede oplysninger, og disse undergår automatisk behandling hos Keen IO.
- **Knewton (udgået august 2020)**, som i Gyldendal Uddannelses SmartMat-produkt fungerer som underdatabehandler. Det er således kun, hvis den dataansvarlige har købt SmartMat, at der sker overførsel af oplysninger til Knewton. Knewton har udviklet produktet SmartMat, og algoritmen til systemets adaptive funktioner ligger hos virksomheden i USA. Knewton har alene adgang til brugernes pseudonymiserede opgavebesvarelser, som undergår automatisk behandling, således at systemet kontinuerligt præsenterer brugerne for opgaver, der passer til deres niveau.
- **New Relic Inc.** leverer værktøjer til monitorering af performance og oppetidsmåling.
- **Adobe** leverer Typekit, til tilpasning og styring af fonte.
- **Jw Player** leverer medieafspilninger i produkterne samt statistik.

# 4. Kontrolmål, kontrolaktivitet, test og resultat heraf

## 4.1 Principper for behandling af personoplysninger (art. 5)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at principperne for indsamling, behandling og opbevaring af personoplysninger hos databehandleren er beskrevet, godkendt og kommunikeret til medarbejderne, og at der sker løbende revurdering og tilpasning heraf.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.1.1 | Principperne for behandling af personoplysninger er adresseret i persondatapolitikker, herunder, men ikke begrænset til, principper for indsamling, behandling og opbevaring af personoplysninger.<br>Gyldendal har orienteret alle medarbejdere om retningslinjerne for persondata. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået processen for at sikre overholdelse af principperne for behandling af personoplysninger.<br>Vi har inspiceret dokumentation for, at der er udarbejdet opdaterede, specifikke systeminstrukser for behandling af personoplysninger, der omfatter principper for behandling af personoplysninger.<br>Vi har inspiceret dokumentation for, at der er gennemført træning af medarbejdere vedrørende principperne for behandling af persondata. | Ingen væsentlige bemærkninger. |
| 4.1.2 | Der er udarbejdet en informationssikkerhedspolitik, hvori der håndteres principper for behandling af persondata. | Vi har foretaget interview med it-sikkerhedsansvarlige samt relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået processen for at sikre overholdelse af principperne for behandling af personoplysninger.<br>Vi har inspiceret, at der er udarbejdet informationssikkerhedspolitikker, hvori principperne for håndtering af persondata håndteres. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at principperne for indsamling, behandling og opbevaring af personoplysninger hos databehandleren er beskrevet, godkendt og kommunikeret til medarbejderne, og at der sker løbende revurdering og tilpasning heraf.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.1.3 | Der er udarbejdet konkrete retningslinjer for brug af it. | Vi har foretaget interview med it-sikkerhedsansvarlige samt relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået processen for brug af IT.<br>Vi har inspiceret, at der er udarbejdet konkrete retningslinjer for brug af it, herunder håndtering af anmodninger vedrørende den registreredes rettigheder. | Ingen væsentlige bemærkninger. |
| 4.1.4 | Der foretages periodisk revurdering – mindst en gang årligt – af retningslinjer og politikker for håndtering af persondata. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået processen for gennemgang og opdatering af relevante politikker og retningslinjer.<br>Vi har påset, at der er udarbejdet specifikke persondatapolitikker, der dækker Gyldendal Uddannelse og underliggende forlag.<br>Vi har inspiceret, at disse gennemgås årligt. | Ingen væsentlige bemærkninger. |
| 4.1.5 | Alle medarbejdere har deltaget i et træningsmodul målrettet GDPR.<br>Gyldendal foretager kontrol af, hvorvidt alle medarbejdere har gennemført modulet. | Vi har foretaget interview med it-sikkerhedsansvarlig om processen for monitorering af medarbejdere, som har/ikke har gennemført GDPR-træning.<br>Vi har inspiceret dokumentation for, at der er implementeret en proces, hvor medarbejdere og deres respektive ledere informeres, såfremt dette ikke gennemføres rettidigt. | Ingen væsentlige bemærkninger. |
| 4.1.6 | Gyldendal har udarbejdet et årshjul, hvori gennemgang og opdatering af politikker og retningslinjer er planlagt til at foregå som minimum hvert andet år. | Vi har foretaget interview med it-sikkerhedsansvarlige samt relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået årshjul.<br>Vi har inspiceret, at der er udarbejdet et årshjul for årlig godkendelse og opdatering af interne politikker og retningslinjer. | Ingen væsentlige bemærkninger. |

## 4.2 Lovlig behandling (art. 6)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at der alene sker behandling af personoplysninger i overensstemmelse med de indgåede databehandleraftaler, og at lovligheden heraf er gennemgået med dataansvarlige.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.2.1 | Politikker og retningslinjer vedrørende lovlig behandling af personoplysninger indgår i Gyldendals årshjul, hvor disse – som minimum hvert andet år – revurderes og godkendes af direktionen. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået processen for gennemgang og opdatering af relevante politikker og retningslinjer.<br>Vi har inspiceret, at der er udarbejdet et årshjul for årlig godkendelse og opdatering af interne politikker og retningslinjer, og at disse præsenteres for direktionen. | Ingen væsentlige bemærkninger. |
| 4.2.2 | Der er indgået databehandleraftaler med dataansvarlige instanser, hvor ydelser og typer af databehandling er beskrevet.<br>Det fremgår af indgåede databehandleraftaler, hvilken instruks der er indgået med underdatabehandler. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler gennemgået ydelser og typer af databehandling, som Gyldendal forestår.<br>Vi har stikprøvevis inspiceret databehandleraftaler og konstateret, at instruks for behandling, herunder typer af persondata, fremgår heraf. | Ingen væsentlige bemærkninger. |

## 4.3 Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelse af den registreredes rettigheder (art. 12)

**Kontrolmål:**

*Der er i systemet indbygget en funktionalitet, som understøtter, at den dataansvarlige kan udlevere oplysninger om behandlingen af personoplysninger i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.3.1 | Gyldendal understøtter den dataansvarliges forpligtelser til at fremfinde data, der er indsamlet om den registrerede.<br>Dette sker udelukkende på anmodning fra den dataansvarlige. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler afklaret typer af data, der kan fremfindes, for at bistå den dataansvarlige.<br>Vi har sammen med it-sikkerhedsansvarlige inspiceret, at relevante persondata kan fremfindes af den dataansvarlige, og at Gyldendal kan bistå med at fremfinde data, hvis dette er nødvendigt. | Ingen væsentlige bemærkninger. |
| 4.3.2 | Gyldendal har udarbejdet en procedure for at bistå den dataansvarlige i forbindelse med den registreredes rettigheder samt it's opgaver i relation til at fremfinde data. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler afklaret typer af data, der kan fremfindes, for at bistå den dataansvarlige.<br>Vi har inspiceret, at der er udarbejdet procedurer internt i Gyldendal vedrørende bistand til den registreredes mht. dennes ret til indsigt, berigtigelse og sletning af data. | Ingen væsentlige bemærkninger. |

## 4.4 Oplysningspligt ved indsamling af personoplysninger hos den registrerede (art. 13)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at databehandleren har givet den dataansvarlige databehandlerens kontaktoplysninger, oplysning om formålet med behandling af personoplysningerne og oplysning om evt. overførsel af personoplysninger til modtagere.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.4.1 | Af den indgåede kontrakt, herunder databehandleraftaler, fremgår kontaktoplysninger, oplysning om formål med behandling af personoplysninger og oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer. | Vi har stikprøvevis inspiceret databehandleraftaler og konstateret, at kontaktoplysninger, oplysning om formål med behandling af personoplysninger og oplysning om evt. overførsel af personoplysninger fremgår. | Ingen væsentlige bemærkninger. |

## 4.5 Ret til berigtigelse (art. 16 og 19)

**Kontrolmål:**

*Der er i systemet indbygget en funktionalitet, som sikrer, at den registreredes ret til berigtigelse af egne registrerede personoplysninger kan understøttes, herunder berigtigelse hos modtagere af personoplysningerne.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.5.1 | Der er defineret ansvarsområder ved berigtigelse af persondata samt en ansvarlig for håndtering heraf ved henvendelse fra dataansvarlige. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler afklaret ansvarsområder for berigtigelse af data.<br>Vi er informeret om, at STIL er ansvarlig for ændringer i data vedrørende Uni-Login, og at lærere, som fungerer som indkøbere, selv kan rette i egne informationer.<br>Vi har inspiceret, at der er udarbejdet procedurer internt i Gyldendal vedrørende berigtigelse af data om nødvendigt. | Ingen væsentlige bemærkninger. |

## 4.6 Ret til sletning ("retten til at blive glemt") (art. 17 og 19)

**Kontrolmål:**

*Der er i systemet indbygget en funktionalitet, som sikrer, at den registreredes ret til sletning af egne registrerede personoplysninger kan understøttes, herunder sletning hos modtagere af personoplysningerne.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.6.1 | I samarbejde med dataansvarlig har databehandler defineret regler for sletning af den registrerede. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler afklaret ansvarsområder og politikker for sletning af data.<br>Vi er informeret om, at der ikke er etableret nogen regler for sletning fra databehandler, herunder STIL.<br>Vi har inspiceret, at der er udarbejdet interne procedurer for sletning af data, som Gyldendal har ansvaret for. | Ingen væsentlige bemærkninger. |
| 4.6.2 | Ved sletteopgaver kan dataansvarlig kontakte Gyldendal, som håndterer dette via en opgave i sin serviceportal. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler afklaret ansvarsområder og politikker for sletning af data.<br>Vi har stikprøvevis inspiceret sletning af persondata, hvor vi har konstateret, at denne er udført i overensstemmelse med retningslinjer, og at dataansvarlig har været informeret. | Ingen væsentlige bemærkninger. |

## 4.7 Ret til begrænsning (art. 18 og 19)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til begrænsning af behandling af egne registrerede personoplysninger kan understøttes, herunder begrænsning hos modtagere af personoplysningerne.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.7.1 | Der foreligger en godkendt databehandleraftale, som beskriver håndtering af den registreredes ret til begrænsning af personoplysninger. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået processen for begrænsning af behandling for individer.<br>Vi har stikprøvevis inspiceret databehandleraftaler, hvori håndtering af den registreredes ret til begrænsning af personoplysninger er beskrevet. | Ingen væsentlige bemærkninger. |

## 4.8 Den dataansvarliges ansvar – implementering af passende databeskyttelse (art. 24)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at Gyldendals tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige via en databehandleraftale.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.8.1 | Det er i indgåede databehandleraftaler beskrevet, at der skal være passende logisk og organisatorisk sikkerhed for Gyldendal Uddannelses ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler.<br>Vi har stikprøvevis inspiceret, at databehandleraftaler beskriver de tekniske og organisatoriske sikringsforanstaltninger, som er godkendt af dataansvarlig. | Ingen væsentlige bemærkninger. |
| 4.8.2 | Det er i indgåede databehandleraftaler defineret passende krav til pseudonymisering og/eller kryptering for Gyldendal Uddannelses ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler.<br>Vi har stikprøvevis inspiceret, at databehandleraftaler beskriver de tekniske og organisatoriske sikringsforanstaltninger.<br>Vi har fået oplyst, at kryptering og pseudonymisering ved login defineres af STIL. | Ingen væsentlige bemærkninger. |
| 4.8.3 | Det er i indgåede databehandleraftaler defineret passende krav til kodeord for Gyldendal Uddannelses ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler.<br>Vi har stikprøvevis inspiceret, at databehandleraftaler beskriver de tekniske og organisatoriske sikringsforanstaltninger.<br>Vi har fået oplyst, at kodeord ved login defineres af STIL for UNI-login. | Ingen væsentlige bemærkninger. |
| 4.8.4 | Det er i indgåede databehandleraftaler defineret passende krav til beskyttelse af data, der transmitteres til Gyldendal Uddannelses ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler.<br>Vi har stikprøvevis inspiceret, at databehandleraftaler beskriver leverandørens ansvar for at sikre fortrolighed og korrekt transmission af data. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at Gyldendals tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige via en databehandleraftale.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.8.5 | Det er i indgåede databehandleraftaler defineret passende krav til fysisk sikring af driftslokation for Gyldendal Uddannelses ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige samt relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået den fysiske sikring for driftlokation.<br>Vi har konstateret, at Gyldendal benytter en ekstern leverandør til hosting af infrastruktur.<br>Vi har inspiceret, at der er indhentet revisionserklæringer (ISAE 3402) fra leverandøren Sentia samt et GDPR-tillæg fra Amazon vedrørende deres kontroller. | Ingen væsentlige bemærkninger. |
| 4.8.6 | Det er i indgåede databehandleraftaler defineret passende krav til logning for Gyldendal Uddannelses ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler.<br>Vi har stikprøvevis inspiceret, at databehandleraftaler beskriver de tekniske og organisatoriske sikringsforanstaltninger.<br>For test af Gyldendals egen logning henvises til art. 32. | Ingen væsentlige bemærkninger. |
| 4.8.7 | Det er i indgåede databehandleraftaler defineret passende krav til sletterutiner for Gyldendal Uddannelses ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler.<br>Vi har stikprøvevis inspiceret, at databehandleraftaler beskriver de tekniske og organisatoriske sikringsforanstaltninger.<br>Vi har inspiceret, at der er udarbejdet en redegørelse samt argumentation for hjemmel vedrørende data i Gyldendal Uddannelse. Vi har desuden påset dokumentation for, at STIL ikke har defineret sletterutiner for data. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at Gyldendals tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige via en databehandleraftale.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.8.8 | Gyldendal har retningslinjer for adgang til systemer, herunder persondata. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for brugeradministration.<br>Vi har inspiceret procedurebeskrivelser for tildeling af adgange til systemer og persondata. | Ingen væsentlige bemærkninger. |
| 4.8.9 | Gyldendal har retningslinjer for lukning af adgange til systemer, herunder persondata. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for brugeradministration.<br>Vi har inspiceret procedurebeskrivelser for lukning af adgange til systemer og persondata. | Ingen væsentlige bemærkninger. |
| 4.8.10 | Gyldendal har retningslinjer for periodisk revurdering af tildelte adgange, herunder retningslinjer for tildeling af udvidede rettigheder samt systemadministratorer. Det sikres, at sådanne rettigheder kun tildeles ud fra et restriktivt arbejdsbetinget behov. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for brugeradministration.<br>Vi har inspiceret procedurebeskrivelser og rolleopdeling, der danner grundlag for periodisk revurdering af rettigheder, og konstateret, at dette som minimum foretages årligt.<br>Vi har inspiceret dokumentation for senest periodisk revurdering. | Ingen væsentlige bemærkninger. |

## 4.9 Databeskyttelse gennem design og standardindstillinger (art. 25)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse gennem design og standardindstillinger i Gyldendals tekniske og organisatoriske sikringsforanstaltninger fungerer effektivt.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.9.1 | Gyldendal har designet sine systemer og applikationer med en logisk rolleopdeling ud fra et arbejdsbetinget behov. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for brugeradministration og tildeling af roller.<br>Vi har inspiceret dokumentation for, at der i Gyldendals Active Directory benyttes klare roller til tildeling af rettigheder.<br>Vi har inspiceret, at disse roller er sporbare i Gyldendal Uddannelses applikationer. | Ingen væsentlige bemærkninger. |
| 4.9.2 | Gyldendal benytter identificerbare og personhenførbare systemadministratorkonti. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for brugeradministration og tildeling af roller.<br>Vi har inspiceret dokumentation for, at der i Gyldendals Active Directory benyttes klare roller til tildeling af rettigheder.<br>Vi har inspiceret, at disse roller er sporbare i Gyldendal Uddannelses applikationer. | Ingen væsentlige bemærkninger. |
| 4.9.3 | Der følges godkendte test- og valideringsprocedurer for hver ændring til systemerne i scope, således at planlagte tests i forbindelse med en ændring er tilstrækkelige, gennemført og godkendt forinden implementering.<br>Der tages stilling til ændringens potentielle indvirkning på implementerede GDPR-processer. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for test og validering af ændringer.<br>Vi har stikprøvevis inspiceret ændringer og påset, at disse har været godkendt og testet.<br>Vi har inspiceret proceduren for udarbejdelse af konsekvensanalyser i forbindelse med ændringer og konstateret, at der for alle ændringer indtil nu ikke har været identificeret et behov for en sådan analyse. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse gennem design og standardindstillinger i Gyldendals tekniske og organisatoriske sikringsforanstaltninger fungerer effektivt.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.9.4 | Persondata krypteres i Gyldendals systemer ud fra en risikobaseret tilgang. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler inspiceret proceduren for kryptering af data, herunder persondata.<br>Vi har inspiceret dokumentation for, at kommunikation fra Gyldendals systemer er tilstrækkeligt krypteret. | Ingen væsentlige bemærkninger. |
| 4.9.5 | Der foretages en konsekvensanalyse, hvis dette er nødvendigt.<br>I Gyldendals projektmodel skal det indledningsvis vurderes, om det er nødvendigt med en konsekvensanalyse. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for udarbejdelse af konsekvensanalyser.<br>Vi er informeret om, at Gyldendal har vurderet, at der ikke har været behov for at udføre konsekvensanalyser. | Ingen væsentlige bemærkninger. |
| 4.9.6 | Separate miljøer er etableret for at sikre, at udviklings-, test- og produktionsaktiviteter er adskilt. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har inspiceret, at der benyttes separate test-, udviklings- og produktionsmiljøer ved udviklingsaktiviteter.<br>Vi har inspiceret dokumentation for opdeling af miljøer. | Ingen væsentlige bemærkninger. |

## 4.10 Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (art. 28 og 29)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), og at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.10.1 | Den dataansvarlige har godkendt de af databehandler afgivne garantier for, at procedurer, tekniske foranstaltninger og kontroller opfylder kravene i forordningen. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har inspiceret, at databehandleraftaler indeholder alle relevante områder.<br>Der henvises til art. 24. | Ingen væsentlige bemærkninger. |
| 4.10.2 | Den dataansvarlige har godkendt de af databehandleren benyttede underdatabehandlere. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har inspiceret, at databehandleraftaler indeholder alle relevante områder.<br>Vi har inspiceret databehandleraftaler, for at verificere at underdatabehandlere fremgår. | Vi har observeret, at underdatabehandleren Azure ikke fremgår af standard databehandleraftaler med dataansvarlige. Samtidig fremgår Azure ikke af fortegnelsen, og som resultat deraf er der ikke dokumentation for tilsyn med Microsoft.<br>Vi har observeret, at kunderne er informeret om, at Microsoft er tilføjet som underdatabehandler i januar 2021.<br>Ingen yderligere væsentlige bemærkninger. |

## 4.11 Fortegnelse over behandlingsaktiviteter (art. 30)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at Gyldendal fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.11.1 | Der er i databehandleraftalens ydelsesbeskrivelser udarbejdet fortegnelser over kategorier af behandlingsaktiviteter med udgangspunkt i Datatilsynets vejledning herom. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået proceduren for udarbejdelse af databehandleraftaler.<br>Vi har stikprøvevist inspiceret dokumentation for, at Gyldendal angiver behandlingsaktiviteter i databehandleraftalen.<br>Vi har endvidere inspiceret dokumentation for, at databehandleraftalen indeholder en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger. | Ingen væsentlige bemærkninger. |
| 4.11.2 | Gyldendal har udarbejdet en fortegnelse over egne behandlingsaktiviteter med udgangspunkt i Datatilsynets vejledning herom.<br>Denne opdateres mindst en gang årligt, og når processer for håndtering af persondata ændres. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået behandlingsaktiviteter hos Gyldendal.<br>Vi har inspiceret dokumentation for, at der internt hos Gyldendal er udarbejdet en oversigt over behandlingsaktiviteter, og at dette er kommunikeret til organisationen.<br>Vi har påset dokumentation for, at der er udarbejdet en instruks om gennemgang og opdatering af oversigten. | Vi har observeret, at underdatabehandleren Azure ikke fremgår af standard databehandleraftaler med dataansvarlige. Samtidig fremgår Azure ikke af fortegnelsen, og som resultat deraf er der ikke dokumentation for tilsyn med Microsoft.<br>Vi har observeret, at kunderne er informeret om, at Microsoft er tilføjet som underdatabehandler i januar 2021.<br>Ingen yderligere væsentlige bemærkninger. |

## 4.12 Behandlingssikkerhed (art. 32)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.12.1 | Der er udarbejdet en risikoanalyse for Gyldendal, som omfatter Gyldendal Uddannelse. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for udarbejdelse af risikoanalyser.<br>Vi har inspiceret dokumentation for, at der er udarbejdet en risikoanalyse for Gyldendal Uddannelse, og at denne er godkendt af ledelsen. | Ingen væsentlige bemærkninger. |
| 4.12.2 | Alle brugere i Gyldendal Uddannelse autentificeres af systemet, og kravene til kodeord er passende konfigureret på OS-, database- og applikationsniveau.<br>Alle brugere med adgang til Gyldendal Uddannelse er tildelt unikke bruger-ID'er. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået anvendte kodeordsmetoder.<br>Vi har inspiceret dokumentation for, at der er implementeret kodeordskrav for applikationerne under Gyldendal Uddannelse og de underliggende databaser hos Gyldendal. | Under vores revision af remote access er vi informeret om, at der ikke er multifaktorautentifikation på VPN.<br>Ingen yderligere væsentlige bemærkninger. |
| 4.12.3 | Gyldendal foretager kryptering af kommunikation i forbindelse med sine ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået den anvendte krypteringsmetode.<br>Vi har endvidere inspiceret dokumentation for, at der benyttes aktive certifikater til overførsel af information. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.12.4 | Der efterleves en implementeret procedure for brugeradministration af Gyldendals brugere, som omfatter oprettelse, nedlæggelse, udvidede rettigheder, periodisk revurdering af tildelte rettigheder og standardbrugere. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået processen for brugeradministration.<br>Vi har stikprøvevis inspiceret, at der forefindes formelle procedurer for brugeradministration, og at disse efterleves.<br>Vi har endvidere inspiceret, at der sker formel godkendelser fra de respektive lederes side i forbindelse med den senest udførte revurdering af brugere og rettigheder. | Ingen væsentlige bemærkninger. |
| 4.12.5 | Der tages backup i overensstemmelse med etablerede retningslinjer, som bl.a. specificerer timing og scope mht. backup. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået proceduren for backup.<br>Vi har endvidere inspiceret dokumentation for, at der er konfigureret en daglig backup af Gyldendal Uddannelses applikationer og databaser. | Ingen væsentlige bemærkninger. |
| 4.12.6 | Det er muligt at foretage restore, når dette er nødvendigt. Gyldendal foretager regelmæssigt en restore-test. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået proceduren for test af restore.<br>Vi har påset, at der kan foretages restore af miljøer på ca. 10 minutter, hvorfor der sjældent foretages formelle restore-tests. Vi har fået oplyst, at der regelmæssigt foretages genskabelse af miljøer.<br>Vi har observeret en livedemonstration af restore, hvor vi har konstateret, at dette kan gøres øjeblikkeligt. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.12.7 | Der er opsat logning på Gyldendals egne brugeres adgang til persondata. Ved anormaliteter adviseres Gyldendals it-afdeling. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået proceduren for logning.<br>Vi har inspiceret, at der benyttes Logpoint til opsamling af logge, og at der sker overvågning af data og brugeraktivitet. | Ingen væsentlige bemærkninger. |
| 4.12.8 | Der er opsat automatisk overvågning af loghændelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået proceduren for logning.<br>Vi har inspiceret, at der benyttes Logpoint til opsamling af logge, og at der er opsat e-mailadvisering til Gyldendals it-afdeling. | Ingen væsentlige bemærkninger. |
| 4.12.9 | Der er udarbejdet beredskabs- og incident response-planer. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået proceduren for beredskab samt incident response.<br>Vi har inspiceret dokumentation for, at der er udarbejdet en beredskabsplan, hvor proceduren for håndtering af incidents samt roller fremgår.<br>Vi har yderligere påset, at beredskabsplanen opbevares i fysiske eksemplarer hos den relevante ledelse. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.12.10 | Der er opsat sikker behandling af fysisk sikkerhed, herunder indhentning af revisionserklæringer fra hosting-leverandør om hosting-ydelser. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler konstateret, at der er udarbejdet en procedure for indhentning og godkendelse af revisionserklæringer og rapporter fra eksterne leverandører.<br>Vi har inspiceret, at Gyldendal har udført egne tilsyn ved underleverandører.<br>Vi har inspiceret, at Gyldendal har indhentet og gennemgået revisionsrapporten fra Sentia samt tillægget fra Amazon. | Ingen væsentlige bemærkninger. |
| 4.12.11 | Der er udarbejdet retningslinjer for brug af it, herunder awareness om sikker brug af it, for Gyldendals medarbejdere. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler gennemgået retningslinjer for it og uddannelse af medarbejdere.<br>Vi har inspiceret, at der føles op på at medarbejdere deltager i awareness træning. | Ingen væsentlige bemærkninger. |
| 4.12.12 | Test- og valideringsprocedurer følges for hver ændring til systemerne i scope, således at planlagte tests i forbindelse med en ændring er tilstrækkelige, gennemført og godkendt forinden implementering. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for test og validering af ændringer.<br>Vi har stikprøvevis påset, at denne har været godkendt og testet. | Ingen væsentlige bemærkninger. |
| 4.12.13 | 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.<br>Inspiceret, at antivirussoftware er opdateret. | Ingen væsentlige bemærkninger. |

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.12.14 | 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.<br>Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor. | Ingen væsentlige bemærkninger. |

## 4.13 Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (art. 33 og 34)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden samt underretning til de registrerede, hvis personoplysninger er omfattet af bruddet.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.13.1 | Der foreligger instruks, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet.<br>Incident-rapportering vedrørende brud på persondatasikkerheden opbevares og kategoriseres. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået proceduren for håndtering af brud på persondatasikkerheden.<br>Vi har stikprøvevis inspiceret håndtering af brud på persondatasikkerheden og kan konstatere, at den generelle procedure er blevet fulgt.<br>Vi har konstateret, at der ikke har været nogen kritiske brud på persondatasikkerheden, hvad angår Gyldendal Uddannelse. | Ingen væsentlige bemærkninger. |

## 4.14 Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (art. 35)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges konsekvensanalyse vedrørende databeskyttelse, inden der foretages behandling af personoplysninger, og at der foretages en fornyet konsekvensanalyse ved ændring i den risiko, som behandlingsaktiviteterne udgør.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.14.1 | I projektmodellen skal det vurderes i en af de indledende faser, om det er nødvendigt med en konsekvensanalyse, for så vidt angår behandling af persondata, over for den registrerede. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for udarbejdelse af konsekvensanalyser.<br>Vi har inspiceret dokumentation for, at der er udarbejdet en skabelon til konsekvensanalyser, og at dette indgår som et trin i Gyldendals projektmodel.<br>Vi har konstateret, at der ikke har været et projekt i Gyldendal Uddannelsesregi i erklæringsperioden, hvor det har været vurderet nødvendigt med en konsekvensanalyse. | Ingen væsentlige bemærkninger. |

## 4.15 Overførsel af personoplysninger til tredjelande eller internationale organisationer (art. 44-50)

**Kontrolmål:**

*Der efterleves procedurer og kontroller, som sikrer, at der alene sker overførsel af personoplysninger til et tredjeland eller en international organisation, hvis Kommissionen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau.*

| Nr. | Databehandlerens kontrolaktivitet | PwC's udførte test | Resultat af test |
|---|---|---|---|
| 4.15.1 | Såfremt der overføres data til tredjelande eller internationale organisationer, skal der være indgået databehandleraftaler med leverandørerne. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for overførsel af data til tredjelande og internationale organisationer.<br>Vi har konstateret, at Gyldendal benytter en ekstern leverandør til hosting af infrastruktur.<br>Vi har inspiceret, at Gyldendal har udført egne tilsyn ved underleverandører.<br>Vi har inspiceret, at der er indhentet revisionserklæringer (ISAE 3402) fra leverandøren Sentia og et GDPR-tillæg fra Amazon vedrørende deres kontroller. | Vi har observeret, at underdatabehandleren Azure ikke fremgår af standard databehandleraftaler med dataansvarlige. Samtidig fremgår Azure ikke af fortegnelsen, og som resultat deraf er der ikke dokumentation for tilsyn med Microsoft.<br>Vi har observeret, at kunderne er informeret om, at Microsoft er tilføjet som underdatabehandler i januar 2021.<br>Ingen yderligere væsentlige bemærkninger. |
| 4.15.2 | Dataansvarlig har accepteret overførsel af data til tredjelande eller internationale organisationer i sine databehandleraftaler med Gyldendal. | Vi har foretaget interview med it-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for overførsel af data til tredjelande og internationale organisationer.<br>Vi har konstateret, at Gyldendal benytter en ekstern leverandør til hosting af infrastruktur.<br>Vi har stikprøvevis inspiceret databehandleraftaler og konstateret, at en instruks om overførsel til tredjelande og internationale organisationer fremgår heraf.<br>Vi har påset, at der udsendes et bilag til databehandleraftalen, hvori der redegøres for overførsel af data til Danmark, Irland og USA. | Ingen væsentlige bemærkninger. |

PENNEO

*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."*

**Hanne Gunnel Salomonsen**
**Direktør**
På vegne af: Gyldendal A/S
*Serienummer: PID:9208-2002-2-239889182383*
*IP: 86.58.xxx.xxx*
*2021-03-24 12:14:05Z*
NEM ID

**Jess Kjær Mogensen**
**Statsautoriseret revisor**
På vegne af: PricewaterhouseCoopers Statsautoriseret…
*Serienummer: CVR:33771231-RID:49470796*
*IP: 83.136.xxx.xxx*
*2021-03-24 13:26:12Z*
NEM ID

**Bo Petersen**
**Director**
På vegne af: PricewaterhouseCoopers Statsautoriseret…
*Serienummer: CVR:33771231-RID:33762968*
*IP: 83.136.xxx.xxx*
*2021-03-24 13:28:17Z*
NEM ID