Deloitte.

Gyldendal A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger i "Gyldendal Uddannelse"

Pr. 25. februar 2019

Indholdsfortegnelse

1. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger i "Gyldendal Uddannelse"

Til: Gyldendal A/S og Gyldendal A/S' kunder

Omfang

Vi har fået til opgave at afgive erklæring om Gyldendal A/S' (Gyldendal) beskrivelse i afsnit 3 af systemerne i "Gyldendal Uddannelse" til behandling af personoplysninger på vegne af dataansvarlige, der er omfattet af EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") 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 "databeskyttelsesloven") pr. 25. februar 2019 (beskrivelsen) og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Gyldendal har i et særskilt afsnit i afsnit 3 under overskriften "Underleverandører" beskrevet, hvilke underleverandører der anvendes som led i serviceleverancen fra "Gyldendal Uddannelse". Dette omfatter bl.a. serviceunderleverandørerne Amazon og Sentia til drift og hosting af hhv. cloud og infrastruktur. Serviceleverandørens systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandøren. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandøren.

Nogle af de kontrolmål, der er anført i Gyldendals beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Gyldendal. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

Gyldendals ansvar

Gyldendal er ansvarlig for udarbejdelsen af beskrivelsen og den tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene og for at udforme, implementere 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.

Deloitte 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 og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, *Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger*, og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt 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 Gyldendal Uddannelse og de underliggende applikationer 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 nået. 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 afsnit 2.

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

Begrænsninger i kontroller hos en dataansvarlig
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 Gyldendal Uddannelse, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion
Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse i afsnit 2. Det er vores opfattelse,

(a) at beskrivelsen af Gyldendal Uddannelse, således som den var udformet og implementeret pr. 25. februar 2019, i alle væsentlige henseender er retvisende

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 25. februar 2019.

Beskrivelse af test af kontroller
De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultatet 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 produkter, 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 databeskyttelsesforordningen er overholdt.

København, den 2. april 2019

Deloitte
Statsautoriseret Revisionspartnerselskab

Thomas Kühn
partner, statsautoriseret revisor

2. Ledelsens udtalelse

Gyldendal A/S (Gyldendal) behandler personoplysninger på vegne af vores kunder, der er dataansvarlige i henhold til EU's forordning om "Beskytte af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter " databeskyttelsesforordningen").

Medfølgende beskrivelse er udarbejdet til brug for Gyldendals kunder, der har anvendt systemerne i Gyldendal Uddannelse, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt. Gyldendal bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af systemerne i Gyldendal Uddannelse, der har behandlet personoplysninger for dataansvarlige, der er omfattet af databeskyttelsesforordningen, pr. 25. februar 2019. De kriterier, der er anvendt for at give denne udtalelse, var, at den medfølgende beskrivelse:
   (i) redegør for, hvordan systemerne i Gyldendal Uddannelse var udformet og implementeret, herunder redegør for:
      - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
      - De processer i både IT- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
      - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
      - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
      - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
      - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
      - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
      - Kontroller, som vi har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
      - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

   (ii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne Gyldendal Uddannelse 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 af Gyldendal Uddannelse, som den enkelte dataansvarlige måtte anse for vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 25. februar 2019. De kriterier, der blev 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

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse pr. 25. februar 2019.

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

København, den 2. april 2019

Gyldendal A/S

Hanne Salomonsen
Direktør, Gyldendal Uddannelse

3. Beskrivelse af behandling (systembeskrivelse)

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 betinger 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, f.eks. 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.

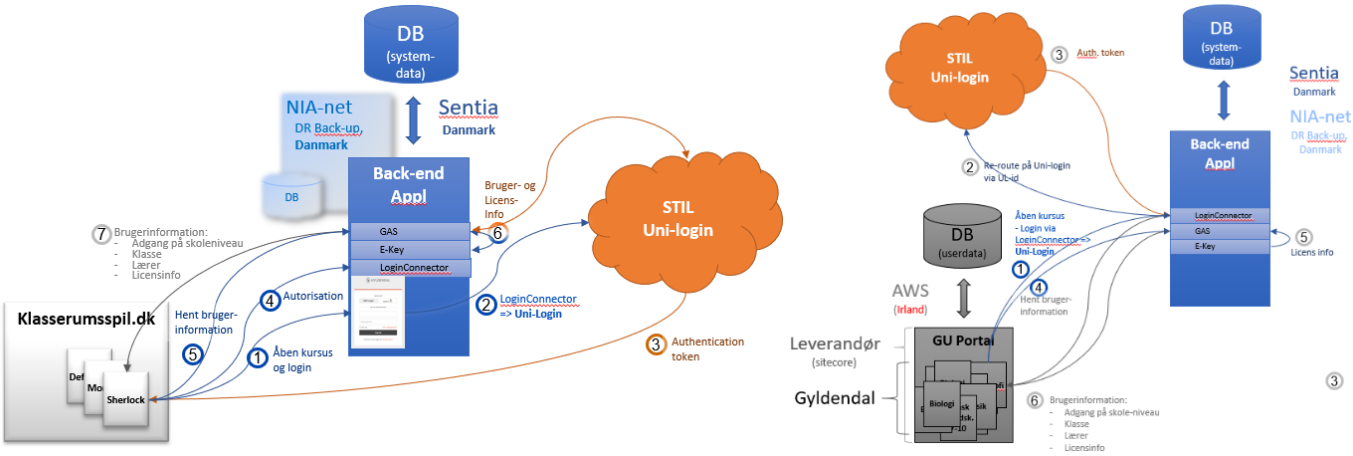
Gyldendal henter og gemmer alene de persondata, som er nødvendige for at levere de ydelser og services (uddannelsesprodukter), som Gyldendal og den dataansvarlige har indgået aftale om. Opsamling og lagring af viden om den registrerede baseret på dennes brug og besvarelser sker kun, i det omfang dette 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

Gyldendal Uddannelses produkter:

Gyldendals produkter falder i følgende to hovedkategorier, som skitseres nedenfor:

- Databehandlernes egne ydelser
- Tredjepartsydelser, som Gyldendal markedsfører.



Billederne ovenfor er en del af den læsevejledning, som Gyldendal Uddannelse sendte ud sammen med databehandleraftalerne. De illustrerer, hvordan data flyder imellem systemerne, når der logges ind i Gyldendal Uddannelses løsninger. Tegningen til venstre viser flowet, når der logges ind i tredjepartsprodukter. (I eksemplet her er brugt Klasserumsspil.dk). Tegningen til højre viser flowet, når der logges ind i Gyldendal Uddannelses egne produkter. For information om Uni-Login henvises til STIL: https://www.stil.dk/administration-og-infrastruktur/uni-login.

Underleverandører

Gyldendal Uddannelses egne ydelsers generelle formål og funktion er de samme. Således udvikles, vedligeholdes og driftes ydelserne på de samme platforme og med faste underleverandører (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 direkte adgang til STILS Uni-Login-services.

De *faste underleverandører* varetager følgende behandlinger:

Miracle A/S implementerer og leverer driftsydelser for de af Gyldendal Uddannelses løsninger, der afvikles i Amazon Web Services' cloud.

Amazon Web Services Ireland Ltd. leverer hosting af Gyldendal Uddannelses produkter.

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) 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. 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.

På tidspunktet for erklæringens udarbejdelse markedsfører Gyldendal Uddannelse følgende *tredjeparts-produkter*:

Skriv og læs, som er et læringsværktøj til den første læsning og skrivning.

Gyldendals webprøver, som er prøve- og træningsmaterialer, der bruges i grundskolen, på gymnasiet og på sprogskoler.

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, jf. ovenstående model.

Personoplysninger
I henhold til 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
- Dialoger 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 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 afsnit 25 og 32. Listen udgør de i denne rapport vurderede tiltag, men er ikke begrænset hertil.

- Kryptering af data
- Brug af egentlige navne er begrænset til situationer, hvor det er nødvendigt for at yde den relevante service – som udgangspunkt pseudonymiseres oplysninger
- 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
- Logfiler med alarmer ved f.eks. 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 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 SANS Institute Critical Security Controls, som sikrer et højt teknisk sikkerhedsniveau. Herudover er der tilført flere administrative 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.

Artikel	Kontrolmål/Årsag til, at artikel ikke er i scope (markeret med gråt)
1. Genstand og formål 2. Materielt anvendelsesområde 3. Territorialt anvendelsesområde 4. Definitioner	Indledende bestemmelser i forordningen, som der ikke kan måles på.

Artikel	Kontrolmål/Årsag til, at artikel ikke er i scope (markeret med gråt)
5. Principper for behandling af personoplysninger	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.
6. Lovlig behandling	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 den dataansvarlige.
7. Betingelser for samtykke	Den dataansvarlige sikrer det fornødne hjemmelsgrundlag for behandlingen. Som udgangspunkt er hjemlen ikke samtykke, men at behandlingen er nødvendig til udførelse af en opgave, som henhører under offentlig myndighedsudøvelse.
8. Betingelser for et barns samtykke i forbindelse med informationssamfundstjenester	
9. Behandling af særlige kategorier af personoplysninger	Der behandles ikke særlige kategorier af personoplysninger eller oplysninger om straffedomme eller lovovertrædelser i Gyldendals systemer.
10. Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser	
11. Behandling, der ikke kræver identifikation	Behandling forudsætter (pseudonym) identifikation.
12. Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder	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.
13. Oplysningspligt ved indsamling af personoplysninger hos den registrerede	Der efterleves procedurer og kontroller, som sikrer, at databehandleren har givet den dataansvarlige databehandlerens kontaktoplysninger, oplysning om formålet med behandling af personoplysningerne samt oplysning om evt. overførsel af personoplysninger til modtagere.
14. Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede	Forpligtelsen relaterer sig til den dataansvarlige. Gyldendal har udarbejdet "Gyldendal Uddannelses privatlivspolitik for elever og lærere, der benytter Gyldendal Uddannelses digitale læremidler", som kan læses på Gyldendal Uddannelses hovedside. Af denne fremgår det, at kommunen/uddannelsesinstitutionen er dataansvarlig, og at det således bl.a. er kommunen/uddannelsesinstitutionen, den registrerede skal kontakte for at gøre brug af sine rettigheder som registreret. Samme besked får de registrerede, der kontakter Gyldendal Uddannelse direkte.
15. Den registreredes indsigtsret	
16. Ret til berigtigelse	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.
19. Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	
17. Ret til sletning ("retten til at blive glemt")	

Artikel	Kontrolmål/Årsag til, at artikel ikke er i scope (markeret med gråt)
19. Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	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.
18. Ret til begrænsning af behandling 19. Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	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.
20. Ret til dataportabilitet	Dataportabilitet er ikke relevant.
21. Ret til indsigelse 22. Automatiske individuelle afgørelser, herunder profilering 23. Begrænsninger	Art. 21 er ikke relevant, da evt. indsigelse efter art. 21(1) skal rettes til den dataansvarlige, som herefter træffer beslutning. Personoplysninger behandles ikke med henblik på direkte markedsføring i Gyldendals digitale læremidler, hvorfor art. 21(2) og (3) heller ikke er relevant. Der foretages ikke automatiske, individuelle afgørelser i art. 22's forstand, hvorfor denne bestemmelse heller ikke er relevant for kontrollen. Art. 23 er rettet mod lovgiver, hvorfor der ikke kan måles på denne bestemmelse.
24. Den dataansvarliges ansvar	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.
25. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger	Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse gennem design og standardindstillinger i Gyldendals tekniske og organisatoriske sikringsforanstaltninger fungerer effektivt.
26. Fælles dataansvarlige 27. Repræsentanter for dataansvarlige og databehandlere, der ikke er etableret i Unionen	Forpligtelsen relaterer sig til den dataansvarlige
28. Databehandler 29. Behandling, der udføres for den dataansvarlige eller Gyldendal	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.
30. Fortegnelse over behandlingsaktiviteter	Der efterleves procedurer og kontroller, som sikrer, at Gyldendal fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.
31. Samarbejde med tilsynsmyndigheden	Ikke relevant. Gyldendal vil naturligvis samarbejde loyalt med Datatilsynet, såfremt tilsynet ønsker oplysninger mv., men der måles ikke på dette punkt.
32. Behandlingssikkerhed	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

Artikel	Kontrolmål/Årsag til, at artikel ikke er i scope (markeret med gråt)
	ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.
33. Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden	Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til at foretage rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden samt underretning til de registrerede, hvis personoplysninger er omfattet af bruddet.
34. Underretning om brud på persondatasikkerheden til den registrerede	
35. Konsekvensanalyse vedrørende databeskyttelse	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.
36. Forudgående høring	Ikke relevant
37. Databeskyttelsesrådgiver	Gyldendal er ikke forpligtet til at have en databeskyttelsesrådgiver.
38. Databeskyttelsesrådgiverens stilling	
39. Databeskyttelsesrådgiverens opgaver	
40. Adfærdskodekser	Der er ikke udarbejdet adfærdskodekser for branchen.
41. Kontrol af godkendte adfærdskodekser	
42. Certificering	
43. Certificeringsorganer	
44. Generelt princip for overførsel	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.
45. Overførsel baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet	
46. Overførsler omfattet af fornødne garantier	
47. Bindende virksomhedsregler	
48. Overførsel eller videregivelse uden hjemmel i EU-retten	
49. Undtagelser i særlige situationer	
50. Internationalt samarbejde om beskyttelse af personoplysninger	
51-99	Ikke relevant

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.

Alle politikker er i øvrigt integreret i et årshjul, hvor Jura & Compliance sikrer, at de vedligeholdes, opdateres og fremlægges for ledelsen mindst hvert andet år.

I 2018 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 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 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 information 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 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 højst 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.

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

<u>Elever/lærer (ikke indkøber):</u>

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
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.

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.

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

Komplementerende kontroller hos de dataansvarlige, art. 17/19
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 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 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 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, og der benyttes personlige brugerkonti/-navne. 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 databehandleraftalen fastsatte).

Art. 32 – Behandlingssikkerhed
Gyldendal Uddannelse benytter sig af SQL-databaser og Windows-servere

1. Der er udarbejdet en samlet risikoanalyse i Neupart for Gyldendal, hvori Gyldendal Uddannelse indgår. Risikovurderingen er forelagt og godkendt af Gyldendal Uddannelses ledelse.
2. Der bruges kodeord til OS og databaser og ved tilgang til applikationerne.
3. Alle brugere af systemerne har unikke bruger-ID'er og identifikationer, hvad enten der er tale om slutbrugere eller medarbejdere hos Gyldendal.
4. Der er HTTPS på alle Gyldendal Uddannelses portaler, og der sker kryptering af kodeord i systemerne.
5. 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.
6. 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.
7. Der foretages restore på systemerne minimum 10 gange årligt.
8. Der er opsat logning i systemerne, f.eks. 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.
9. 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.
10. Der er udarbejdet en beredskabsplan, som testes årligt, og som efter hver test tilpasses og optimeres med henblik på at højne kvaliteten.
11. 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).
12. Gyldendal indhenter revisionserklæringer fra Gyldendal Uddannelses underleverandører (egenerklæringer fra tredjepartsleverandører) for at sikre, at der hos underleverandørerne er en passende

grad af sikkerhed. Gyldendal foretager fysiske besøg hos tredjepartsleverandører, hvor dette vurderes relevant.

13. 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.
14. Der er implementeret Change Management-processer, herunder test og validering af ændringer i systemerne.
15. 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 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**, 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.

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***	***Revisors udførte test***	***Resultat af revisors 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. 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. Vi har inspiceret dokumentation for, at der er udarbejdet opdaterede, specifikke systeminstrukser for behandling af personoplysninger, der omfatter principper for behandling af personoplysninger. Vi har inspiceret dokumentation for, at der er gennemført træning af alle medarbejdere vedrørende principperne for behandling af persondata.	Ingen afvigelser konstateret
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. Vi har inspiceret, at der er udarbejdet informationssikkerhedspolitikker, hvori principperne for håndtering af persondata håndteres.	Ingen afvigelser konstateret
4.1.3	Der er udarbejdet konkrete retningslinjer for brug af IT.	Vi har inspiceret, at der er udarbejdet konkrete retningslinjer for brug af IT, herunder håndtering af anmodninger vedrørende den registreredes rettigheder.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
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. Vi har påset, at der er udarbejdet specifikke persondatapolitikker, der dækker Gyldendal Uddannelse og underliggende forlag. Vi har inspiceret, at disse gennemgås årligt.	Ingen afvigelser konstateret
4.1.5	Alle medarbejdere har deltaget i et træningsmodul målrettet GDPR. 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. Vi har inspiceret dokumentation for, at der er implementeret en proces, hvor medarbejdere og deres respektive ledere informeres, såfremt dette ikke gennemføres rettidigt.	Ingen afvigelser konstateret
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 inspiceret, at der er udarbejdet et årshjul for årlig godkendelse og opdatering af interne politikker og retningslinjer.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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-sikkerheds-ansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået processen for gennemgang og opdatering af relevante politikker og retningslinjer. Vi har inspiceret, at der er udarbejdet et års-hjul for årlig godkendelse og opdatering af in-terne politikker og retningslinjer, og at disse præsenteres for direktionen.	Ingen afvigelser konstateret
4.2.2	Der er indgået databehandleraftaler med dataansvarlige instanser, hvor ydelser og typer af databehandling er be-skrevet. Det fremgår af databehandleraftalerne, hvilken instruks der er indgået med underdatabehandlere.	Vi har foretaget interview med IT-sikkerheds-ansvarlige og relevante medarbejdere og har på baggrund af forespørgsler gennemgået ydelser og typer af databehandling, som Gyl-dendal forestår. Vi har stikprøvevis inspiceret databehandleraf-taler (én for skoler og gymnasiuer, én for kommuner og én ikke-standardaftale) og kon-stateret, at instruks for behandling, herunder typer af persondata, fremgår heraf.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
4.3.1	Gyldendal understøtter den dataansvarliges forpligtelser til at fremfinde data, der er indsamlet om den registrerede. 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. Vi har sammen med IT-sikkerhedsansvarlige påset, at relevante persondata kan fremfindes af den dataansvarlige, og at Gyldendal kan bistå med at fremfinde data, hvis dette er nødvendigt.	Ingen afvigelser konstateret
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. 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 afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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 (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) og konstateret, at kontaktoplysninger, oplysning om formål med behandling af personoplysninger og oplysning om evt. overførsel af personoplysninger fremgår.	Ingen afvigelser konstateret

4.5 Ret til berigtigelse (art. 16 og art. 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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har inspiceret, at der er udarbejdet procedurer internt i Gyldendal vedrørende berigtigelse af data om nødvendigt. Vi har konstateret, at STIL er ansvarlig for ændringer i data vedrørende Uni-Login, og at lærere, som fungerer som indkøbere, selv kan rette i egne informationer.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har konstateret, at der ikke er etableret nogen regler for sletning fra databehandler, herunder STIL. Vi har inspiceret, at der er udarbejdet interne procedurer for sletning af data, som Gyldendal har ansvaret for.	Ingen afvigelser konstateret
4.6.2	Ved sletteopgaver kan dataansvarlig kontakte Gyldendal, som håndterer dette via en opgave i deres 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. Vi har udtaget én stikprøve på en sag vedrørende sletning af persondata, hvor vi har konstateret, at denne er udført i overensstemmelse med retningslinjer, og at dataansvarlig har været informeret.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har stikprøvevis inspiceret databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale), hvori håndtering af den registreredes ret til begrænsning af personoplysninger er beskrevet.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har stikprøvevis inspiceret, at databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) beskriver de tekniske og organisatoriske sikringsforanstaltninger, som er godkendt af dataansvarlig.	Ingen afvigelser konstateret
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. Vi har stikprøvevis inspiceret, at databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) beskriver de tekniske og organisatoriske sikringsforanstaltninger. Vi har fået oplyst, at kryptering og pseudonymisering ved login defineres af STIL.	Ingen afvigelser konstateret
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. Vi har stikprøvevis inspiceret, at databehandleraftaler (én for skoler og gymnasier, én for	Ingen afvigelser konstateret

		kommuner og én ikke-standardaftale) beskriver de tekniske og organisatoriske sikringsforanstaltninger. Vi har fået oplyst, at kodeord ved login defineres af STIL.	
4.8.4	Det er i indgåede databehandleraftaler defineret passende krav til backup for Gyldendal Uddannelses ydelser.	Vi har foretaget interview med IT-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler. Vi har stikprøvevis inspiceret, at databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) beskriver de tekniske og organisatoriske sikringsforanstaltninger. Vi har fået oplyst, at datainput varetages af STIL. For test af Gyldendals backup henvises til art. 32.	Ingen afvigelser konstateret
4.8.5	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. Vi har stikprøvevis inspiceret, at databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) beskriver leverandørens ansvar for at sikre fortrolighed og korrekt transmission af data.	Ingen afvigelser konstateret
4.8.6	Det er i indgåede databehandleraftaler defineret passende krav til fysisk sikring af driftslokation for Gyldendal Uddannelses ydelser.	Vi har konstateret, at Gyldendal benytter en ekstern leverandør til hosting af infrastruktur. Vi har inspiceret, at der er indhentet revisionserklæringer (ISAE 3402) fra leverandøren	Ingen afvigelser konstateret

		Sentia samt et GDPR-tillægget fra Amazon vedrørende deres kontroller.	
4.8.7	Det er i indgåede databehandleraftaler defineret passende krav til logning for Gyldendal Uddannelses ydelser. Datainput varetages af STIL, hvorfor Gyldendal ikke selv logger nogen aktivitet, for så vidt angår brugeraktiviteter i Gyldendal Uddannelse-portalerne.	Vi har foretaget interview med IT-sikkerhedsansvarlige og relevante medarbejdere og har gennemgået proceduren for godkendelse af databehandleraftaler. Vi har stikprøvevis inspiceret, at databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) beskriver de tekniske og organisatoriske sikringsforanstaltninger. For test af Gyldendals egen logning henvises til art. 32.	
4.8.8	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. Vi har stikprøvevis inspiceret, at databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) beskriver de tekniske og organisatoriske sikringsforanstaltninger. 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 afvigelser konstateret
4.8.9	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.	Ingen afvigelser konstateret

		Vi har inspiceret procedurebeskrivelser for tildeling af adgange til systemer og persondata.	
4.8.10	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. Vi har inspiceret procedurebeskrivelser for lukning af adgange til systemer og persondata.	Ingen afvigelser konstateret
4.8.1´1	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. Vi har inspiceret procedurebeskrivelser og rolleopdeling, der danner grundlag for periodisk revurdering af rettigheder, og konstateret, at dette som minimum foretages årligt.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
4.9.1	Gyldendal har designet deres 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. Vi har inspiceret dokumentation for, at der i Gyldendals Active Directory benyttes klare roller til tildeling af rettigheder. Vi har konkluderet, at disse roller er sporbare i Gyldendal Uddannelses applikationer.	Ingen afvigelser konstateret
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. Vi har inspiceret dokumentation for, at der i Gyldendals Active Directory benyttes klare roller til tildeling af rettigheder. Vi har konkluderet, at disse roller er sporbare i Gyldendal Uddannelses applikationer.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
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. 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. Vi har stikprøvevis udtaget én stikprøve pr. miljø og påset, at denne har været godkendt og testet. 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 sådan analyse.	Ingen afvigelser konstateret
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 og maskering af data, herunder persondata. Vi har inspiceret dokumentation for, at kommunikation fra Gyldendals systemer er tilstrækkeligt krypteret.	Ingen afvigelser konstateret
4.9.5	Der foretages en konsekvensanalyse, hvis dette er nødvendigt. 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. Det er konstateret, at Gyldendal ikke har behov for at udføre konsekvensanalyser i de fleste scenarier, da de ikke varetager kildedata.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
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 konstateret, at der benyttes separate test-, udviklings- og produktionsmiljøer ved udviklingsaktiviteter.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
4.10.1	Den dataansvarlige har godkendt de af databehandler afgivne garantier for, at procedurer, tekniske foranstaltninger og kontroller opfylder kravene i forordningen.	Der henvises til art. 24	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har stikprøvevist inspiceret dokumentation for, at Gyldendal angiver behandlingsaktiviteter i databehandleraftalen. Vi har endvidere inspiceret dokumentation for, at databehandleraftalen indeholder en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.	Ingen afvigelser konstateret
4.11.2	Gyldendal har udarbejdet en fortegnelse over egne behandlingsaktiviteter med udgangspunkt i Datatilsynets vejledning herom. 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. Vi har inspiceret dokumentation for, at der internt hos Gyldendal er udarbejdet en oversigt over behandlingsaktiviteter, og at dette er kommunikeret til organisationen. Vi har påset dokumentation for, at der er udarbejdet en instruks om gennemgang og opdatering af oversigten.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har inspiceret dokumentation for, at der er udarbejdet en risikoanalyse for Gyldendal Uddannelse, og at denne er godkendt af ledelsen.	Ingen afvigelser konstateret
4.12.2	Alle brugere i Gyldendal Uddannelse autentificeres af systemet, og kravene til kodeord er passende konfigureret på OS-, database- og applikationsniveau. 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. Vi har inspiceret dokumentation for, at der er implementeret kodeordskrav for applikationerne under Gyldendal Uddannelse og de underliggende databaser hos Gyldendal.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
4.12.3	Gyldendal foretager kryptering af kommunikation i forbindelse med deres ydelser.	Vi har foretaget interview med IT-sikkerhedsansvarlige og relevante medarbejdere og har på baggrund af forespørgsler fået gennemgået den anvendte krypteringsmetode. Vi har endvidere inspiceret dokumentation for, at der benyttes aktive certifikater til overførsel af information.	Ingen afvigelser konstateret
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. Vi har stikprøvevis (én oprettelse, én nedlæggelse, én tildeling af udvidede rettigheder og én komplet revurdering af adgange) inspiceret, at der forefindes formelle procedurer for brugeradministration, og at disse efterleves. 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 afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
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. Vi har endvidere inspiceret dokumentation for, at der er konfigureret en daglig backup af Gyldendal Uddannelses applikationer og databaser.	Ingen afvigelser konstateret
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. 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. Vi har observeret en livedemonstration af restore, hvor vi har konstateret, at dette kan gøres øjeblikkeligt.	Ingen afvigelser konstateret
4.12.7	Der er opsat logning på ændringer af persondata samt brugeraktivitet. 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.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
		Vi har inspiceret, at der benyttes Logpoint til opsamling af logge, og at der sker overvågning af data og brugeraktivitet.	
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. Vi har inspiceret, at der benyttes Logpoint til opsamling af logge, og at der er opsat e-mail-advisering til Gyldendals IT-afdeling.	Ingen afvigelser konstateret
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. Vi har inspiceret dokumentation for, at der er udarbejdet en beredskabsplan, hvor proceduren for håndtering af incidents samt roller fremgår. Vi har ydereligere påset, at beredskabsplanen opbevares i fysiske eksemplarer hos den relevante ledelse. Vi har inspiceret, at Gyldendal har fået foretaget en Crisis Management-analyse via en ekstern leverandør, hvor der er foretaget beredskabs- og incident response-test.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
4.12.10	Der er opsat sikker behandling af fysisk sikkerhed, herunder indhentning af revisionserklæringer fra hostingleverandør om hostingydelser.	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. Vi har inspiceret, at Gyldendal har indhentet og gennemgået revisionsrapporten fra Sentia samt tillægget fra Amazon.	Ingen afvigelser konstateret
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. Vi har inspiceret dokumentation for, at der er igangsat uddannelse af alle medarbejdere vedrørende sikker brug af IT samt GDPR. Vi har fået oplyst, at der planlægges en kvartalsvis uddannelsesopdatering til alle medarbejdere vedrørende håndtering af persondata samt sikker IT-praksis.	Ingen afvigelser konstateret
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.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors test***
		Vi har stikprøvevis udtaget én stikprøve pr. miljø og påset, at denne har været godkendt og testet.	

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***	***Revisors udførte test***	***Resultat af revisors test***
4.13.1	Der foreligger instruks, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet. 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. Vi har for én stikprøve inspiceret håndtering af brud på persondatasikkerheden og kan konstatere, at den generelle procedure er blevet fulgt. Vi har konstateret, at der ikke har været nogen kritiske brud på persondatasikkerheden, hvad angår Gyldendal Uddannelse.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har inspiceret dokumentation for, at der er udarbejdet en skabelon til konsekvensanalyser, og at dette indgår som et trin i Gyldendals projektmodel. Vi har konstateret, at der siden den 25. maj 2018 ikke har været et projekt i Gyldendal Uddannelses regi, hvor det har været vurderet nødvendigt med en konsekvensanalyse. Vi har desuden inspiceret dokumentation for, at Gyldendal har konsulteret en ekstern instans vedrørende omfanget og brugen af konsekvensanalyser.	Ingen afvigelser konstateret

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***	***Revisors udførte test***	***Resultat af revisors 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. Vi har konstateret, at Gyldendal benytter en ekstern leverandør til hosting af infrastruktur. Vi har inspiceret, at der er indhentet revisionserklæringer (ISAE 3402) fra leverandøren Sentia og et GDPR-tillæg fra Amazon vedrørende deres kontroller.	Ingen afvigelser konstateret
4.15.2	Dataansvarlig har accepteret overførsel af data til tredjelande eller internationale organisationer i deres 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. Vi har konstateret, at Gyldendal benytter en ekstern leverandør til hosting af infrastruktur. Vi har stikprøvevis inspiceret databehandleraftaler (én for skoler og gymnasier, én for kommuner og én ikke-standardaftale) og konstateret, at en instruks om overførsel til tredjelande og internationale organisationer fremgår heraf.	Ingen afvigelser konstateret

		Vi har påset, at der udsendes et bilag til data-behandleraftalen, hvori der redegøres for overførsel af data til Danmark, Irland og USA.	