



revi-it

et trygt samfund med it og data

Revisorerklæring

Det Digitale Folkebibliotek

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandlaftaler med kunder for perioden fra 23. december 2020 til 31. december 2021

Januar 2022

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Indholdsfortegnelse

Afsnit 1:	Det Digitale Folkebiblioteks beskrivelse af behandlingsaktivitet for leverancen af digitale bibliotekstjenester og services	1
Afsnit 2:	Det Digitale Folkebiblioteks udtalelse	7
Afsnit 3:	Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder om i perioden fra 23. december 2020 til 31. december 2021	9
Afsnit 4:	Kontrolmål, udførte kontroller, test og resultater heraf	12

Afsnit 1: Det Digitale Folkebiblioteks beskrivelse af behandlingsaktivitet for leverancen af digitale bibliotekstjenester og services

Formålet med behandling af personoplysninger

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at stille digitale bibliotekstjenester og services til rådighed for folkebiblioteker og biblioteksbrugere på tværs af kommuner. Foreningen Det Digitale Folkebibliotek har ansvaret for levering af indhold til og drift af folkebibliotekernes hjemmesideløsning (CMS), Biblioteket Appen, eReolens hjemmesider og apps samt levering af listeservices.

Behandlingen af personoplysninger i den forbindelse er i henhold til databehandleraftalen mellem bibliotekskommunerne og Det Digitale Folkebibliotek og tilhørende underdatabehandleraftaler med hhv. DBC, ITK, Redia og Microsoft Corporation.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om forskellige tjenester, der tilbyder transit af data eller behandling og opbevaring i systemer til brug for bibliotekerne. Behandlingen kan blandt andet dreje sig om autentificering af brugeren, brugeroprettelse, log in, reservering af materiale, udlån af digitale materialer, visning af statuslister, Material List, Follow Searches, betaling af mellemværender, kontakt via kontaktformularer samt beskedhistorik både på CMS'et, Biblioteket Appen og eReolen.

Personoplysninger

Typen af personoplysninger, der behandles er:

- Bruger-id'er såsom CPR-nummer, lånernummer, GUID, UNI-login, support-id og Patron-id
- Loginoplysninger
- Kontaktoplysninger
- Oplysninger om hvorvidt man vil modtage notifikationer via e-mail/mobil
- Oplysninger om hvorvidt man vil have opbevaret udlånshistorik og modtage personlige anbefalinger
- Låner- og reserveringsstatus
- Oplysninger om mellemværender
- Udlånte titler
- Betalings- og beskedhistorik
- Udlånshistorik
- Redaktionelt indhold, anmeldelser, blogs og temaer
- Kommentarer
- Søgestrengte som følges
- Materiale-ID'er, som brugeren har gemt.

Kategorier af registrerede personer omfattet af databehandlerens behandling af personoplysninger:

- Biblioteksansatte
- Biblioteksbrugere
- Biblioteksbrugere under 18 år

Praktiske tiltag

Sekretariatets ledelse har godkendt alle tiltag, herunder samtlige procedurer (adgangskontroller, udvikling og anskaffelser, sikkerhedshændelser, persondataanmodninger og risikostyring), kontroller, interne værktøjer og instrukser samt instrukser til underdatabehandlere.

Organisatorisk er alle medarbejdere i foreningen orienteret om procedurerne for behandling af persondata og informationssikkerhed herunder de forskellige værktøjer som ControlGDPR, risikovurderingsark og diverse tjeklister. Orienteringen er sket via orienteringsmøder og personaleseminarer for alle medarbejdere.

Medarbejdere hos Det Digitale Folkebibliotek skal føre logs over persondatahenvendelser, sikkerhedshændelser (manuelt) og brugerlogin i forskellige anvendte systemer (automatisk). Foreningens projektledere og driftsansvarlige er informeret om udvidelsen af Det Digitale Folkebiblioteks standard projektbeskrivelse og orienteret om diverse tjeklister og skemaet "*data protection by design and default*", der skal anvendes ved alle projekter vedr. udvikling af nye systemer.

Foreningen har adresse/domicil hos Københavns Kommune, hvor der er fysisk adgangssikring til arbejdsstedet med personlige adgangstokens og adgangskoder. Der er personlige adgangskoder til pc'er og telefoner udleveret af Københavns Kommune og derigennem personlig adgangskode til de systemer, sekretariatet benytter. Nogle af mapperne i SharePoint er begrænset, således at kun relevante medarbejdere kan få adgang hertil.

Da Foreningen har adresse/domicil hos Københavns Kommune og benytter kommunens it-udstyr og it-systemer, er foreningens ansatte underlagt Københavns Kommunes it-tekniske sikkerhedsforanstaltninger.

Risikovurdering

Foreningens teams har alle foretaget risikovurderinger af systemer, projekter eller arbejdsgange hvor der behandles personoplysninger. Alle risici og handlingsplaner er efterfølgende blevet godkendt af sekretariatschefen.

Kontrolforanstaltninger

Behandlinger - instrukser

Det Digitale Folkebiblioteks behandlinger stemmer overens med standarddatabehandleraftalen. Standarddatabehandleraftalen følger den model, at hvis Det Digitale Folkebibliotek ændrer væsentligt på en behandling, foretager anden eller yderligere behandling af personoplysninger eller udskifter underdatabehandler, skal det forudgående meddeles til de dataansvarlige bibliotekskommuner, som herefter kan gøre indsigelse inden for en frist på 30 dage.

Der foreligger interne procedurer for modtagelse af instruks fra de dataansvarlige, og hvordan de skal håndteres i henhold til databehandleraftalen.

Sekretariatets benytter ControlGDPR som fortegnelsessystem over alle sekretariatets behandlinger af personoplysninger. Sekretariatets medarbejdere skal være opmærksomme på behandlinger i forbindelse med anskaffelse og udvikling af nye systemer, moduler el.lign. og give meddelelse herom til GDPR-teamet, så der kan ske registrering af behandlingen. Herudover gennemgås fortegnelsen minimum en gang årligt.

Fortegnelsen skal danne et overblik over behandlinger, der er iværksat, og skal dække: Kontaktoplysninger, formål med behandlingerne, beskrivelse, dels af kategorier af registrerede og personoplysninger, dels af kategorier af modtagere, som oplysningerne vil blive videregivet til, beskrivelse af sletningsfrister samt generel beskrivelse af tekniske, fysiske og organisatoriske sikkerhedsforanstaltninger.

Herudover registreres notifikationer i ControlGDPR, der sender påmindelse til GDPR-teamet om diverse deadlines, årlige og halvårslige opdateringer, kontroller, tidsfrister mv., som er relevante for Det Digitale Folkebiblioteks overholdelse af de persondataretlige regler, it-revisionsmæssige krav mv.

Det Digitale Folkebibliotek har iværksat en række organisatoriske, fysiske og tekniske sikkerhedsforanstaltninger, der skal sikre at behandling af personoplysninger og eventuelle instrukser efterleves. Sekretariatet har meddelt, at ingen behandling må ændres, påbegyndes eller ophøre uden GDPR-teamets godkendelse, idet dette kun kan ske med tilladelse fra de dataansvarlige bibliotekskommuner.

Det Digitale Folkebiblioteks sekretariatschef har godkendt samtlige procedurer, men GDPR-teamet skal sørge for at sikringsforanstaltninger oplyst i sekretariatets procedurer overholdes, kontrolleres og opdateres i overensstemmelse med de persondataretlige regler, it-revisionsmæssige krav og instrukser fra de dataansvarlige bibliotekskommuner.

Procedurekontrol

Der foretages halvårslige eller årlige kontrolgennemgange, hvor alle procedurer evalueres, hvilket sker på baggrund af diverse logs, risikovurderinger e.l.

Der er indført notifikationer i ControlGDPR til at minde GDPR teamet om slettedagene.

Alle projektledere og driftsansvarlige bliver særskilt indkaldt til at kontrollere om fortegnelse, projektbeskrivelser og risikovurderinger er opdaterede og korrekte.

Proceduregennemgang

Der skal ske en årlig gennemgang af alle procedurer med medarbejdere.

Der sendes årligt en redegørelse vedr. overholdelse af kontroller nævnt i Det Digitale Folkebiblioteks procedurer til sekretariatschefen. For at sikre at procedureerne overholdes og er mest muligt effektive, afholdes der som minimum årlige møder, hvor procedurer, kontroller, værktøjer, logs mv. gennemgås af GDPR-teamet. Herefter udfærdiges referat og redegørelse efter mødet, der skal godkendes af sekretariatschefen.

Det kontrolleres løbende, at der i alle medarbejders mailsignatur er indsat link til Det Digitale Folkebiblioteks privatlivspolitik, og der afholdes endvidere halvårslige awareness-møder for medarbejdere i Det Digitale Folkebibliotek vedrørende korrekt behandling af personoplysninger. I forbindelse med orienteringsmøderne afholdes halvårslige slettedage, hvor medarbejdere skal sikre, at unødvendige og overflødige personoplysninger, der findes fysisk og digitalt slettes, herunder i Outlook og andre systemer, der indeholder personoplysninger.

Procedurer - Adgangsstyring

Sekretariatets medarbejdere skal overholde kontrollerne i procedurer for adgangsstyring. Halvårligt kontrolleres det, at det kun er relevante brugere der har relevante roller og udvidede rettigheder.

Der er indført fysiske sikkerhedsforanstaltninger til sekretariatet i form af adgangskoder og –tokens. Københavns Kommune har logs over samtlige medarbejdere der har adgang til bygningen, ligesom at Det Digitale Folkebibliotek skal overholde Københavns Kommunes procedurer ved ansættelse og fratrædelse vedr. udlevering og aflevering af adgangstokens, computer og lignende.

Procedurerne evalueres på baggrund af de halvårige kontroller.

Procedurer - Risikostyring

Det Digitale Folkebibliotek benytter et risikovurderingsark, hvor behandlingernes risici vurderes. Ved risikoniveauerne medium og høj anføres en handlingsplan og deadline. Deadlines skal løbende følges op, og som minimum skal risikovurderingen kontrolleres hvert halve år. Kontrollerne er indført i ControlGDPR, hvorefter der sendes påmindelser ud. Herudover holder mindst én medarbejder kontrol med deadlines i risikoarket.

Procedurer - Udvikling og anskaffelser

Foreningen skal overholde kontrollerne i procedurer for udvikling og anskaffelser.

For at sikre medarbejdernes praktiske efterlevelse af proceduren er der udarbejdet en intern instruks om Data Protection by Design og Data Protection by Default til projektledere og driftsansvarlige, ligesom projektlederne skal udfylde en projektbeskrivelse, hvor persondatabehandling og -sikkerhed indgår som en selvstændig del af projektbeskrivelseskabelonen. Der defineres kriterier for accept af projektet og dets produkter, fx hvad angår funktionalitet, sikkerhedskrav mv. Der er ligeledes udarbejdet tjeklister til design-, kodning-, test- og implementeringsfasen som værktøj til at sikre overholdelse af proceduren. Der foretages halvårlig kontrol, hvor alle projektledere kontrollerer om fortegnelser, projektbeskrivelser og risikovurderinger er opdaterede og korrekte. Procedurerne evalueres på baggrund af de halvårige kontroller. Hvert år oplister GDPR-teamet underdatabehandlere, og de matches med de tilhørende underdatabehandlertaftaler med henblik på en vurdering af, om de gældende underdatabehandlertaftaler stadig er tilstrækkelige.

Projektlederen kontrollerer datasikkerhedsniveauet for de enkelte opgaver i projektet.

Procedurer – Håndtering af persondataanmodninger

Alle persondatahenvendelser til Det Digitale Folkebibliotek og underdatabehandlere logges i et samlet dokument. GDPR-teamet afholder interne møder efter behov, dog minimum hver måned, hvor loggen kontrolleres med henblik på at tjekke, at alle henvendelser er registreret korrekt og afsluttet til tiden. Der er udsendt instruks til underdatabehandlere vedrørende modtagelse af persondatahenvendelser.

Procedurer – Sikkerhedshændelser

Det Digitale Folkebibliotek logger sikkerhedshændelser i overensstemmelse med proceduren om sikkerhedshændelser.

For at give et overblik over sikkerhedshændelser, er der oprettet en log, hvor disse skal registreres. Årligt afholder GDPR-teamet et internt møde, hvor den forgangne periodes sikkerhedshændelser gennemgås. På den baggrund vurderes det, hvorvidt en sikkerhedsforanstaltning eller proceduren kan eller bør forbedres. GDPR-teamet kontrollerer på halvårige møder, at der sker en ensartet håndtering af sikkerhedsbrud ved at

kvalificere og prioritere konsekvenserne af sikkerhedsbrud efter samme skala, og at der indsamles og opbevares information om sikkerhedsbrud, der kan tjene som bevismateriale.

Underleverandører

Det Digitale Folkebibliotek har som databehandler for bibliotekskommunerne outsourcet flere tekniske sikkerhedsforanstaltninger til underleverandører, der fungerer som underdatabehandlere, og sekretariatets medarbejdere har ikke adgang til de fleste databaser o.l.

Det Digitale Folkebibliotek har lister med virksomhedsoplysninger over samtlige underdatabehandlere der kontrolleres løbende på GDPR-teamets møder. Skal en underleverandør udskiftes, skal bibliotekskommunerne skriftligt orienteres, ligesom Det Digitale Folkebibliotek skal sikre, at underdatabehandlerne som minimum er underlagt de samme forpligtelser, som Det Digitale Folkebibliotek selv er underlagt efter databehandleraftalen med bibliotekskommunerne og tilhørende bilag.

Det Digitale Folkebibliotek fører tilsyn med underdatabehandlernes overholdelse af databehandleraftalen. Tilsynet tager derfor udgangspunkt i sikkerhedsniveauet og de sikkerhedsforanstaltninger, der er aftalt. Tilsyn føres, dels ved at sekretariatets projektledere og/eller driftsansvarlige holder periodiske statusmøder om driften, udviklingen, leverancen etc. med leverandørens kontaktperson, (intervallet for statusmøderne kommer an på aftalens længde og/eller sekretariatets risikovurdering af leverancen og de omhandlede behandlinger af persondata), dels ved at indhente it-revisionserklæringer (ISAE 3000). Resultat af revisionserklæringer vil blive sendt til de dataansvarlige bibliotekskommuner som dokumentation for, at databehandleraftalernes krav om udfærdigelse af it-revisionserklæring er opfyldt og for Det Digitale Folkebiblioteks tilsyn.

Det bemærkes, at det i kontrolmål F.6 testes, hvorvidt Det Digitale Folkebibliotek har ført tilsyn med relevante underdatabehandlere i perioden.

Tredjelande

Databehandler må kun opbevare personoplysninger på lokaliteter og lande i overensstemmelse med databehandleraftalen. Standarddatabehandleraftalen følger den model, at hvis vi ændrer væsentligt på en behandling eller giver os til at foretage en anden behandling, skal vi meddele dette til bibliotekskommunerne, som herefter kan gøres indsigelse inden for en frist på 30 dage.

Medarbejdere

Det Digitale Folkebiblioteks faste medarbejdere er underlagt egne ansættelses- og fratrædelsesprocedurer.

Ved ansættelse i Det Digitale Folkebibliotek skal alle medarbejdere have en orientering i foreningens informationssikkerhedspolitik, introduceres til foreningens procedurer vedr. databehandling, kontroller, behandlingsregistrering i ControlGDPR, risikovurderingsark samt anden relevant information såsom medarbejderinstruks, tjeklister, skemaer, projektskabeloner mv.

Komplementerende kontroller

Retsgrundlaget for behandling af personoplysninger

De dataansvarlige bibliotekskommuner m.fl. har ansvaret for at sikre, at der er et lovligt grundlag for at behandle de personoplysninger, der behandles af Det Digitale Folkebibliotek som databehandler for bibliotekskommunerne m.fl.

Ansvar for data, dataindhold og privatlivspolitik

Det Digitale Folkebibliotek stiller i overensstemmelse med det i foreningens vedtægter angivne formål og de indgåede tilslutningsaftaler en række biblioteksløsninger til rådighed for de dataansvarlige bibliotekskommuner m.fl., som disse i forskellig grad selv råder over. Bibliotekskommunerne m.fl. er selv ansvarlige for de data og det indhold, de eventuelt selv måtte indføre i løsningerne, og de er tillige ansvarlige for selv at udforme og vedligeholde privatlivspolitikken på deres hjemmesider i CMS'et, dog at Det Digitale Folkebibliotek i et vist omfang rådgiver de enkelte bibliotekskommuner m.fl. vedrørende spørgsmål om privatlivspolitik, herunder om den dataansvarliges opfyldelse af oplysningsforpligtelsen over for den registrerede.

De dataansvarlige bibliotekskommuners m.fl. ansvar og rådighed over DDB CMS

Biblioteker, der benytter sig af redaktør hostingplanen, har en lokal administratorrolle og kan konfigurere de funktioner, som Det Digitale Folkebibliotek stiller til rådighed for dem, ligesom de kan oprette og formidle indhold.

Biblioteker, der benytter sig af webmasterhostingplanen, har en administratorrolle og kan ændre den grundlæggende opsætning af CMS'et og tilføje ny funktionalitet.

Biblioteker, der benytter sig af DDB CMS programmør hostingplanen, råder selv over deres egen server, og skal derfor også selv ansvarlig for at fastsætte retningslinjer og procedurer for medarbejderes eller eksterne parters adgang til serveren.

Ordningen med bibliotekernes mulighed for at ændre eller tilføje ny funktionalitet i DDB CMS betyder, at det pågældende bibliotek må sikre sig de nødvendige interne eller eksterne kompetencer og ressourcer til at foretage de ønskede ændringer på forsvarlig vis. De må endvidere efterfølgende opretholde en stabil drift og sikre, at den løbende opdatering af hjemmesiden med nye versioner af DDB CMS er mulig. Dette ansvar påhviler efter ibrugtagning af hostingplanen biblioteket selv.

Ekstrafunktionalitet til Biblioteket-appen

Det er muligt for de enkelte bibliotekskommuner at tilkøbe ekstrafunktionalitet til Biblioteket-appen direkte hos leverandøren, og for disse tilkøbsprodukter er Det Digitale Folkebibliotek ikke databehandler for bibliotekskommunerne.

Ansvar for integrationer til andre biblioteksløsninger

Det Digitale Folkebiblioteks løsninger er integreret til andre biblioteksløsninger i it-biblioteksinfrastrukturen, fx Adgangsplatformen og det fælles bibliotekssystem (FBS/Cicero). Det Digitale Folkebibliotek er ikke ansvarlig for sikkerheden vedrørende disse løsninger eller for rigtigheden af de data, der overføres eller anvendes hertil.

Forlagenes digitale udlån i udlånsordningen eReolen administreres af den af forlagene udpegede administrator Publizon a/s, der er selvstændig databehandler for bibliotekskommunerne som dataansvarlige vedrørende behandling af personoplysninger i forbindelse med forlagenes digitale udlån og de enkelte kommuners betaling herfor. Det Digitale Folkebibliotek er ikke vedrørende disse behandlinger af personoplysninger, men kun for behandlinger af personoplysninger i udlånsordningens eReolens brugergrænseflader.

Afsnit 2: Det Digitale Folkebiblioteks udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Det Digitale Folkebiblioteks kunder, som har indgået en databehandleraftale med Det Digitale Folkebibliotek, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Denne erklæring er udarbejdet efter helhedsmetoden vedrørende ydelser fra serviceunderleverandøren (underdatabehandleren) ITK og efter partielmetoden for serviceleverandørerne (underdatabehandlerne) Microsoft Corporation, Redia og DBC A/S. Det Digitale Folkebiblioteks systembeskrivelse omfatter derfor kontrolmål og tilknyttede kontroller hos ITK, men ikke kontrolmål og tilknyttede kontroller hos Microsoft Corporation, Redia og DBC A/S.

Det kan oplyses at Redia og DBC A/S får udarbejdet egne ISAE 3000 erklæringer om overholdelse af GDPR.

Det bemærkes, at det i kontrolmål F.6 testes, hvorvidt Det Digitale Folkebibliotek har ført tilsyn med relevante underdatabehandlere i perioden.

Det Digitale Folkebibliotek bekræfter, at:

- a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af, hvordan Det Digitale Folkebibliotek har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 23. december 2020 til 31. december 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
 - (i) Redegør for, hvordan Det Digitale Folkebiblioteks processer og kontroller relateret til databeskyttelse 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 med henvisning til digitale bibliotekstjenester og services' afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som,

hvis det er nødvendigt for at nå de kontrolmål der er anført i beskrivelsen, er identificeret i beskrivelsen

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger
- (ii) Indeholder relevante oplysninger om ændringer ved databehandlerens digitale bibliotekstjenester og services til behandling af personoplysninger foretaget i hele perioden fra 23. december 2020 til 31. december 2021
- (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne digitale bibliotekstjenester og services 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 digitale bibliotekstjenester og services, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.
- b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 23. december 2020 til 31. december 2021. Kriterierne anvendt for at give denne udtalelse var, at:
- (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
 - (ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og
 - (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 23. december 2020 til 31. december 2021
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerisk og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

København, den 28. februar 2022

Det Digitale Folkebibliotek



Glenn Leervad-Bjørnhart
Sekretariatschef

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder om i perioden fra 23. december 2020 til 31. december 2021

Til Det Digitale Folkebibliotek og Det Digitale Folkebiblioteks kunder i rollen som dataansvarlige.

Omfang

Vi har fået som opgave at afgive erklæring med høj grad af sikkerhed om Det Digitale Folkebiblioteks beskrivelse i "Afsnit 1" af digitale bibliotekstjenester og services i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig i hele perioden fra 23. december 2020 til 31. december 2021 og b+c) om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Denne erklæring er udarbejdet efter helhedsmetoden vedrørende ydelser fra serviceunderleverandøren (underdatabehandleren) ITK og efter partielmetoden for serviceleverandørerne (underdatabehandlerne) Microsoft Corporation, Redia og DBC A/S. Det Digitale Folkebiblioteks kontrolbeskrivelse omfatter derfor kontrolmål og tilknyttede kontroller hos ITK, men ikke kontrolmål og tilknyttede kontroller hos Microsoft Corporation, Redia og DBC A/S. Vores testhandlinger omfatter relevante kontroller hos ITK, jf. testhandlinger og resultater af test i afsnit 4.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Det Digitale Folkebiblioteks ansvar

Det Digitale Folkebibliotek er ansvarlig for udarbejdelsen af beskrivelsen og 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 samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

REVI-IT A/S anvender international standard om kvalitetsstyring, ISQC 1¹, og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

Revisors ansvar

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

¹ ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er 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 digitale bibliotekstjenester og services samt for kontrollerens 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 "Afsnit 1".

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

Det Digitale Folkebiblioteks beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved digitale bibliotekstjenester og services, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

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

- (a) at beskrivelsen af digitale bibliotekstjenester og services, således som denne var udformet og implementeret i perioden fra 23. december 2020 til 31. december 2021, 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 perioden fra 23. december 2020 til 31. december 2021, og
- (c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i perioden fra 23. december 2020 til 31. december 2021.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Det Digitale Folkebiblioteks digitale bibliotekstjenester og services, 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 28. februar 2022

REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Basel Rimon Obari
Partner, CISA, CISM



Michael Marseen
Statsautoriseret revisor

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

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

Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-I nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden fra 23. december 2020 til 31. december 2021.

Denne erklæring er udarbejdet efter helhedsmetoden vedrørende ydelser fra serviceunderleverandøren (underdatabehandleren) ITK og efter partielmetoden for serviceleverandørerne (underdatabehandlerne) Microsoft Corporation, Redia og DBC A/S. Det Digitale Folkebiblioteks kontrolbeskrivelse omfatter derfor kontrolmål og tilknyttede kontroller hos ITK, men ikke kontrolmål og tilknyttede kontroller hos Microsoft Corporation, Redia og DBC A/S. Vores testhandlinger omfatter relevante kontroller hos ITK.

Kontroller udført hos de dataansvarlige er ikke omfattet af vores erklæring.

Vi har udført vores tests af kontroller hos Det Digitale Folkebibliotek via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Det Digitale Folkebibliotek. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

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

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2.

Artikler og punkter markeret med fed angiver primære områder.

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

G.2	15, 30, 44, 45 , 46, 47, 48, 49	6.10.2.1, 7.5.1 , 7.5.2, 7.5.3, 7.5.4, 8.4.2 , 8.5.2, 8.5.3	13.2.1
G.3	15, 30, 44, 45 , 46, 47, 48, 49	6.10.2.1, 7.5.1 , 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, 13, 14 , 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>Nyt område ift. ISO 27001/2</i>
H.2	12, 13, 14 , 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>Nyt område ift. ISO 27001/2</i>
I.1	33, 34	6.13.1.1	16.1.1-5
I.2	33, 34 , 39	6.4.2.2, 6.13.1.5, 6.13.1.6	16.1.5-6
I.3	33, 34	6.13.1.4	16.1.5
I.4	33, 34	6.13.1.4 , 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
A.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
A.2	<p>Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.</p>	<p>DDF og ITK</p> <p>Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
A.3	<p>Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Vi har forespurgt, om databehandleren har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.</p>	<p>DDF og ITK</p> <p>Vi er blevet informeret om, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, hvorfor vi ikke har testet effektiviteten af relevante procedurer.</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
B.2	<p>Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
B.3	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.</p>	<p>ITK</p> <p>Vi har forespurgt til anvendelse af beskyttelse mod malware.</p>	<p>Ingen afvigelser konstateret.</p>
B.4	<p>Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.</p>	<p>ITK</p> <p>Vi har inspiceret, at ekstern adgang sker gennem VPN.</p>	<p>Ingen afvigelser konstateret.</p>
B.5	<p>Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.</p>	<p>ITK</p> <p>Vi har stikprøvevis inspiceret netværksdokumentation for at sikre behørig segmentering.</p>	<p>Ingen afvigelser konstateret.</p>

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.</p> <p>Vi har stikprøvevis inspiceret, at brugeres adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	<p>ITK</p> <p>Vi har stikprøvevis inspiceret systemer og påset at disse løbende overvåges.</p>	<p>Ingen afvigelser konstateret.</p>
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	<p>ITK</p> <p>Vi har stikprøvevis inspiceret transmission af personoplysninger over internettet, og stikprøvevis påset, at dette sker via krypteret forbindelse.</p>	<p>Ingen afvigelser konstateret.</p>
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	<p>ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende.</p> <p>Vi har forespurgt til anvendelse af personoplysninger i forbindelse med udviklingsprocessen.</p>	<p>Ingen afvigelser konstateret.</p>
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	<p>ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.</p> <p>Vi har stikprøvevis inspiceret ændringer i perioden, og stikprøvevis påset, at proceduren er fulgt.</p>	<p>Ingen afvigelser konstateret.</p>

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.13	<p>Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger.</p> <p>Brugernes adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.</p>	<p>DDF</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Vi har stikprøvevis inspiceret, at medarbejdernes adgange til systemer og databaser er godkendt, og at der er et arbejdsbetinget behov.</p> <p>Vi har stikprøvevis inspiceret, at fratrådte medarbejders adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.</p> <p>Vi har inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.</p> <p>ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Vi har stikprøvevis inspiceret, at medarbejdernes adgange til systemer og databaser er godkendt, og at der er et arbejdsbetinget behov.</p> <p>Vi har inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
B.14	<p>Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.</p>	<p>ITK</p> <p>Vi har inspiceret adgangen til personoplysninger, og påset, at dette sker med 2-faktor autentifikation.</p>	<p>Ingen afvigelser konstateret.</p>

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
C.1	<p>Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
C.2	<p>Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.</p>	<p>DDF</p> <p>Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Vi har inspiceret dokumentation for, at politikken ligger tilgængelig for relevante medarbejdere.</p> <p>ITK</p> <p>Vi har inspiceret informationssikkerhedspolitikken, og påset, at denne er i overensstemmelse med indgåede databehandleraftaler.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	<p>DDF</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.</p> <p>Vi har stikprøvevis inspiceret, at der er dokumentation for efterprøvningen af nyansatte medarbejdere i erklæringsperioden.</p> <p>ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.</p> <p>Vi har forespurgt til ansættelser i erklæringsperioden.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	<p>DDF</p> <p>Vi har stikprøvevis inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale.</p> <p>Vi har stikprøvevis inspiceret at nyansatte medarbejdere i erklæringsperioden er blevet introduceret til relevante politikker og procedurer.</p> <p>ITK</p> <p>Vi har stikprøvevis inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale.</p> <p>Vi har stikprøvevis inspiceret at nyansatte medarbejdere i erklæringsperioden har deltaget i introforløb.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	<p>DDF</p> <p>Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages.</p> <p>Vi har stikprøvevis inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget for fratrådte medarbejdere i erklæringsperioden.</p> <p>ITK</p> <p>Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages.</p> <p>Vi har forespurgt til fratrædelser i erklæringsperioden.</p>	<p>DDF</p> <p>Ingen afvigelser konstateret.</p> <p>ITK</p> <p>Vi er blevet informeret om, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har testet effektiviteten af relevante procedurer.</p> <p>Ingen afvigelser konstateret.</p>
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	<p>DDF</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere opretholder fortrolighedsaftalen og generel tavshedspligt.</p> <p>Vi har stikprøvevis inspiceret, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt for fratrådte medarbejdere i erklæringsperioden.</p> <p>ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.</p> <p>Vi har forespurgt til fratrædelser i erklæringsperioden.</p>	<p>DDF</p> <p>Ingen afvigelser konstateret.</p> <p>ITK</p> <p>Vi er blevet informeret om, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har testet effektiviteten af relevante procedurer.</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	DDF og ITK Vi har inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	DDF og ITK Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	DDF og ITK Vi har inspiceret dokumentation for, at DPO'en er blevet inddraget i relevante opgaver i erklæringsperioden.	DDF og ITK Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	DDF og ITK Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.	DDF og ITK Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
D.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
D.2	<p>Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.</p>	<p>DDF og ITK</p> <p>Vi har stikprøvevis inspiceret databehandleraftaler, og påset, at der er taget stilling til slette og opbevaringsrutiner.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
D.3	<p>Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:</p> <ul style="list-style-type: none"> Tilbageleveret til den dataansvarlige og/eller Slettet, hvor det ikke er i modstrid med anden lovgivning. 	<p>DDF og ITK</p> <p>Vi har forespurgt til ophørte databehandlinger i erklæringsperioden.</p>	<p>DDF og ITK</p> <p>Vi er blevet informeret om, at der ikke har været ophørte databehandlinger i perioden, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer.</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
E.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
E.2	<p>Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.</p>	<p>DDF og ITK</p> <p>Vi har stikprøvevis inspiceret, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
F.1	<p>Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>DDF</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	<p>Ingen afvigelser konstateret.</p>

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	DDF Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har stikprøvevis inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	DDF Vi har stikprøvevis inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	DDF Vi har stikprøvevis inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	DDF Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisi-onserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	DDF Vi har inspiceret dokumentation for, at databehandleren har ført tilsyn med relevante underdatabehandlere i perioden.	Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	DDF og ITK Vi har inspiceret den løbende kontrol af databehandleraftaler, og påset, at aftaler er blevet gennemgået i perioden.	DDF og ITK Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	<p>DDF</p> <p>Vi har stikprøvevis inspiceret databehandleraftaler og underdatabehandleraftaler, og påset, at der er taget stilling til tredjelandsoverførsler.</p> <p>Vi har stikprøvevis inspiceret lokation for opbevaring af personoplysninger.</p> <p>Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer.</p> <p>ITK</p> <p>Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.</p> <p>Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	<p>DDF og ITK</p> <p>Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer i erklæringsperioden.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål H – De registreredes rettigheder

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
H.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
H.2	<p>Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.</p>	<p>DDF</p> <p>Vi har inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.</p> <p>ITK</p> <p>Vi har forespurgt, om databehandleren har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	Det Digitale Folkebiblioteks kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>DDF og ITK</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Vi har inspiceret, at proceduren er opdateret.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	<p>DDF og ITK</p> <p>Vi har inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	<p>DDF og ITK</p> <p>Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p> <p>Vi har inspiceret loggen over hændelser i perioden, og forespurgt, om der har været persondatassikkerhedsbrud i perioden.</p>	<p>DDF og ITK</p> <p>Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer.</p> <p>Ingen afvigelser konstateret</p>
I.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>DDF og ITK</p> <p>Vi har inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p>	<p>DDF og ITK</p> <p>Ingen afvigelser konstateret.</p>