et trygt samfund med it og data

Det Digitale Folkebibliotek

CVR Nr.: 41 34 41 21

Revisorerklæring

Erklæring fra uafhængig revisor – ISAE 3000
Erklæringsafgivelse med høj grad af sikkerhed i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov som databehandler for leverancen af digitale bibliotekstjenester og services pr. 22. december 2020

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

December 2020

Indholdsfortegnelse

Afsnit 1. Det Digitale Folkebiblioteks systembeskrivelse

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, Biblioteket Appen, Litteratursiden 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, Biblioteket Appen og Litteratursiden.

Personoplysninger

Typen af personoplysninger, der behandles er:

- Bruger-ID'er såsom CPR-nummer, lånernummer, GUID 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 i Biblioteket Appen
- Låner- og reserveringsstatus
- Oplysninger om mellemværender
- Udlånte titler
- Betalings- og beskedhistorik
- Udlånshistorik
- Redaktionelt indhold, anmeldelser, blogs og temaer
- Kommentarer
- Søgestrenge 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, risikovurderingsarket 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'ere 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 responses er efterfølgende blevet godkendt af sekretariatschefen.

Kontrolforanstaltninger

Behandlinger - instrukser

Det Digitale Folkebiblioteks behandlinger stemmer overens med databehandleraftalerne, som er indgået med bibliotekskommunerne. 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.

Sekretariatet 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 (se procedure for udvikling- og anskaffelse). 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 (fx tredjelande og hjemmel hertil), 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 halvårlige 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 oplistet 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 halvårlige eller årlige kontrolgennemgange, hvor alle procedurer evalueres, hvilket sker på baggrund af diverse logs, risikovurderinger eller lignende.

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 sker 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 procedurerne 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 medarbejderes mailsignatur er indsat link til Det Digitale Folkebiblioteks privatlivspolitik, og der afholdes endvidere halvårlige orienterings- og instruktionsmøder for medarbejdere i Det Digitale Folkebibliotek vedrørende korrekt behandling af personoplysninger. I forbindelse med orienteringsmøderne afholdes halvårlige slettedage, hvor medarbejdere skal sikre, at unødvendige og overflødige personoplysninger, der findes fysisk og digital 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 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 halvårlige kontroller.

Procedurer - Risikostyring

Det Digitale Folkebibliotek benytter et risikovurderingsark, hvor behandlingernes risici vurderes. Ved risk level 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 mail til de ansvarlige projektledere og driftsansvarlige. 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 projektbeskrivelsesskabelonen. 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 halvårlige kontroller. Hvert år oplister GDPR-teamet underdatabehandlere, og de matches med de tilhørende underdatabehandleraftaler med henblik på en vurdering af, om de gældende underdatabehandleraftaler stadig er tilstrækkelige.

Projektlederen kontrollerer datasikkerhedsniveauet for de enkelte opgaver i projektet.

Procedurer – Håndtering af persondataanmodninger

Registeret over modtagne persondatahenvendelser gennemgås 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.

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.

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 halvårlige 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.

Underdatabehandlere

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 og behandlingen af personoplysninger. 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.

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

Der er etableret formelle ansættelses- og fratrædelsesprocedurer for faste medarbejdere hos Det Digitale Folkebibliotek.

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 DDB CMS, 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 administrator rolle 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 webmaster-hostingplanen, 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-biblioteks-infra-strukturen, 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.

Afsnit 2: Det Digitale Folkebiblioteks udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Det Digitale Folkebiblioteks kunder, som, i rollen som dataansvarlige, har anvendt digitale bibliotekstjenester og services, 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 Digitale Folkebibliotek bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af digitale bibliotekstjenester og services, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 22. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan digitale bibliotekstjenester og services 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 pr. 22. december 2020.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den 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 implementeret pr. 22. december 2020. Kriterierne anvendt for at give denne udtalelse var, at:

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

(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

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, 22. december 2020

Det Digitale Folkebibliotek

Christel Elbrønd Krabbenhøft
Konstitueret sekretariatschef

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov pr. 22. december 2020

Til Det Digitale Folkebibliotek, bibliotekskommuner i rollen som dataansvarlige og disses revisorer

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 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.

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 og implementere kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), som er baseret på de grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighedsamt professionel adfærd.

REVI-IT A/S anvender international standard om kvalitetsstyring, ISQC 1[1] , og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om 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. 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 implementerede.

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 kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "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 dataansvarlig

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 pr. 22. december 2020, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 22. december 2020.

Beskrivelse af test af kontroller

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

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, 22. december 2020

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Partner, CISA

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

Den følgende oversigt er udformet for at skabe et overblik over de kontroller, som Det Digitale Folkebibliotek har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte artikler pr. 22. december 2020 er efterlevet.

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.

De krav, som fremgår direkte af forordningen eller loven, kan ikke fraviges. Derimod kan der justeres på, hvordan sikkerheden implementeres, da sikkerhedskravene i forordningen på flere punkter er af mere generel og overordnet karakter, som bl.a. skal tage hensyn til formål, behandlingens karakter, kategorien af personoplysninger mv. Herudover kan der være konkrete krav i de enkelte kundekontrakter, der kan have en rækkevidde, der går ud over databeskyttelseslovens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos Det Digitale Folkebiblioteks kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

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
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

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15**,** 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15**,** 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7
J.1	**7,** 9, **13, 14**, 18	**7.2.4**, 7.3.4	*Nyt område ift. ISO 27001/2*
J.2	7, 14, 18	**7.3.4**	*Nyt område ift. ISO 27001/2*
J.3	11, 13, 14, 15, 17, 18, 21 28	**7.3.2, 8.2.5, 8.3.1, 8.5.4, 8.5.6**	*Nyt område ift. ISO 27001/2*
J.4	11, 13, 14, 15, 17, 18, 21 28	**7.3.2, 8.2.5, 8.3.1, 8.5.4, 8.5.6**	*Nyt område ift. ISO 27001/2*
K.1	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*
K.2	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*
K.3	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*

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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**ITK og DDF** Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurer er opdaterede.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	**ITK og DDF** Vi har inspiceret databe-handleraftaler, og stikprøvevis påset, at databehandleren kun udfører den instruks, som fremgår af databehandleraftalen	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	**ITK og DDF** Vi har inspiceret proceduren for efterlevelse af instruks, og påset, at databehandleren vil underrette, hvis en instruks strider mod gældende ret.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikrings-foranstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**ITK og DDF** Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Vi har inspiceret, at procedurer er opdaterede.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	**ITK og DDF** Vi har inspiceret risikoanalysen, og påset, at denne tager hensyn til væsentlige risici for de registrerede. Vi har inspiceret kontrollen af risikoanalysen, og påset, at denne bliver løbende opdateret.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	**ITK** Vi har stikprøvevis inspiceret implementering af beskyttelse mod malware, og vi har stikprøvevis påset, at dette er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	**ITK** Vi har stikprøvevis inspiceret firewalls, og stikprøvevis påset, at dette er konfigureret korrekt. Vi har stikprøvevis inspiceret kontrol af firewalls, og stikprøvevis påset, at dette er blevet udført i perioden.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	**ITK** Vi har stikprøvevis inspiceret opdeling af interne netværk, og stikprøvevis påset, at dette er segmenteret.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	**ITK og DDF** Vi har inspiceret proceduren for adgangstildeling, og påset, at adgang bliver tildelt efter et arbejdsbetinget behov. Vi har stikprøvevis inspiceret lister over adgange, og stikprøvevis påset, at disse har et arbejdsbetinget behov for adgang.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	**ITK** Vi har stikprøvevis inspiceret overvågning af systemer, og stikprøvevis påset, at disse er udstyret med alarmer.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	**ITK** Vi har stikprøvevis inspiceret anvendelse af kryptering i forbindelse med transmission, og stikprøvevis påset, at dette er implementeret korrekt.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
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.	**ITK** Vi har inspiceret proceduren for udvikling, og påset, at der er taget stilling til behandlingen af personoplysninger i forbindelse med udvikling. Vi har stikprøvevis inspiceret tickets, og stikprøvevis påset, at proceduren bliver fulgt.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	**ITK** Vi har inspiceret proceduren for ændringer, og påset, at ændringer til systemer, databaser og netværk følger en fastlagt procedure. Vi har stikprøvevis inspiceret tickets for ændringer, og stikprøvevis påset, at ændringer følger proceduren. Vi har stikprøvevis inspiceret sikkerhedsopdateringer, og stikprøvevis påset, at disse sker løbende.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	**ITK** Vi har inspiceret proceduren for adgangsstyring, og påset at tildeling og afbrydelse af brugeradgange er styret. Vi har stikprøvevis inspiceret oprettelse og lukning af brugeradgange, og stikprøvevis påset, at dette sker i overensstemmelse med proceduren. Vi har inspiceret kontrollen af adgange, og påset, at brugeradgange løbende bliver vurderet. **DDF** Vi har inspiceret proceduren for adgangsstyring, og påset at tildeling og afbrydelse af brugeradgange er styret. Vi har inspiceret kontrollen af adgange, og påset, at brugeradgange løbende bliver vurderet.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af tofaktor autentifikation.	**ITK** Vi har inspiceret adgangen til personoplysninger, og påset, at dette sker med 2faktor.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	**ITK** Vi har inspiceret lister over aktiver, og påset, at virksomheden har identificeret, hvilke medarbejdere, der har fået udleveret kort til kontoret.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	**ITK og DDF** Vi har inspiceret informations-sikkerhedspolitikken, og påset, at denne er tilgængelig for medarbejderne. Vi har inspiceret dokumentation for, at den løbende bliver opdateret.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informations-sikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	**ITK** Vi har inspiceret virksomhedens informationssikkerhedspolitik og databehandleraftaler med DDF, og påset, at der ikke er uoverensstemmelser. **DDF** Vi har inspiceret databehandler-aftaler og informationssikkerheds-politikken, og påset, at disse ikke er i modstrid.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	**ITK og DDF** Vi har inspiceret ansættelses-proceduren, og påset, at der i forbindelse med ansættelse vil blive indhentet relevant materiale til efterprøvning af medarbejderen.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende data-behandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	**ITK og DDF** Vi har inspiceret proceduren for ansættelse, og påset, at med-arbejdere skal underskrive en fortrolighedsaftale ved ansættelse. Vi har stikprøvevis inspiceret ansættelseskontrakt, og stikprøvevis påset, at medarbejderen har underskrevet en fortrolighedserklæring. Vi har stikprøvevis inspiceret introduktionsmateriale, og stikprøvevis påset, at medarbejdere bliver introduceret til behandling af person-oplysninger.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	**ITK** Vi har inspiceret proceduren for adgangsstyring, og påset, at adgange, herunder aktiver, bliver inddraget i forbindelse med fratrædelse. Vi har stikprøvevis inspiceret inddragelse af adgangsrettigheder, og påset, at dette følger proceduren. **DDF** Vi har inspiceret proceduren for adgangsstyring, og påset, at adgange, herunder aktiver, bliver inddraget i forbindelse med fratrædelse.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
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.	**ITK** Vi har inspiceret proceduren for fratrædelse, og påset at fratrådte medarbejdere bliver orienteret om fortrolighedsklausulen i forbindelse med fratrædelse. **DDF** Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortroligheds-aftalen og generel tavshedspligt.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	**ITK og DDF** Vi har stikprøvevis inspiceret seneste awarenesstræning af medarbejdere, og stikprøvevis påset, at træningen har været i relation til it-sikkerhed.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver og bliver inddraget i relevante områder.	**ITK** Vi har inspiceret, at databehandleren har vurderet behovet for en DPO, og påset, at DPO'en bliver inddraget. **DDF** Vi har inspiceret dokumentation for, at DPO'en er blevet tilmeldt Datatilsynet. Vi har inspiceret dokumentation for, at DPO'en har de nødvendige kvalifikationer.	**DDF** Ingen afvigelser konstateret. **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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**ITK og DDF** Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overens-stemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	**ITK og DDF** Vi har inspiceret databehandleraftaler, og påset, at der er aftalt specifikke krav til opbevaringsperioder og sletterutiner.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: - Tilbageleveret til den dataansvarlige og/eller - Slettet, hvor det ikke er i modstrid med anden lovgivning.	**ITK og DDF** Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**ITK og DDF** Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at procedurerne er opdaterede.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	**ITK og DDF** Vi har inspiceret databehandleraftaler, og påset, at behandling kun finder sted på aftalte lokationer.	**DDF** Ingen afvigelser konstateret. **ITK** 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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**DDF** Vi har inspiceret proceduren for anvendelse af underdata-behandlere, og påset, at der er taget stilling til krav til data-behandleraftaler og instruks Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	**DDF** Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at databehandleren kun anvender godkendte eller specifikke underdatabehandlere.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	**DDF** Vi har inspiceret proceduren for ændringer af underdata-behandlere, og vi har påset, at der er taget stilling til rettidig underretning af dataansvarlige.	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 databehandleraftaler og underdatabehandleraftaler, og stikprøvevis påset, at databehandleren er blevet underlagt samme eller tilsvarende forpligtelser, og at underdata-behandleren er blevet pålagt det samme.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: ⎩ Navn ⎩ CVR-nr. ⎩ Adresse ⎩ Beskrivelse af behandlingen.	**DDF** Vi har inspiceret databehandler-aftaler, og påset, at underdata-behandlere fremgår af aftalen.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	**DDF** Vi har inspiceret proceduren for tilsyn med underdatabehandlere, og vi har påset, at der løbende bliver ført tilsyn med underdata-behandlere, herunder underdatabehandlere, som indgår i denne erklæring efter partiel og helhedsmetoden.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	**ITK og DDF** Vi har inspiceret databehandler-aftaler, og påset, at overførsler til tredjelande er beskrevet. Vi har forespurgt til, om virksomheden overfører personoplysninger til tredjelande, og vi har inspiceret oversigten over lokation for data.	**ITK** Ikke relevant, da vi er blevet informeret om, at person-oplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret. **DDF** Ikke relevant, da vi er blevet informeret om, at person-oplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	**ITK og DDF** Vi har forespurgt til, om virksomheden overfører personoplysninger til tredjelande, og vi har inspiceret oversigten over lokation for data.	**ITK** Ikke relevant, da vi er blevet informeret om, at person-oplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret. **DDF** Ikke relevant, da vi er blevet informeret om, at person-oplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	**ITK og DDF** Vi har forespurgt til, om virksomheden overfører person-oplysninger til tredjelande, og vi har inspiceret oversigten over lokation for data.	**ITK** Ikke relevant, da vi er blevet informeret om, at person-oplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret. **DDF** Ikke relevant, da vi er blevet informeret om, at person-oplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Kontrolmål H – De registreredes rettigheder

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**ITK og DDF** Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdaterede.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	**ITK og DDF** Vi har inspiceret, at virksomheden fører log over persondata-anmodninger. Vi har stikprøvevis inspiceret udførelse af bistand til dataansvarlige, og stikprøvevis påset, at gennemførelse af rettigheder er muligt.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**ITK og DDF** Vi har inspiceret proceduren, og påset, at denne indeholder krav om underrettelse af de dataansvarlige. Vi har inspiceret proceduren, og påset, at denne er opdateret.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	**ITK og DDF** Vi har stikprøvevis inspiceret awarenesstræning af medarbejdere, og stikprøvevis påset, at medarbejdere bliver trænet i identifikation af eventuelle brud.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	**ITK og DDF** Vi har inspiceret loggen over persondatabrud.	**ITK** Vi har observeret, at der ikke har været brud på persondata-sikkerheden indenfor de seneste 6 måneder, hvorfor vi ikke har kunnet teste implementering af proceduren. Ingen afvigelser konstateret. **DDF** Vi har observeret, at der ikke har været brud på persondata-sikkerheden indenfor de seneste 6 måneder, hvorfor vi ikke har kunnet teste implementering af proceduren. Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: - Karakteren af bruddet på persondatasikkerheden - Sandsynlige konsekvenser af bruddet på persondatasikkerheden - Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	**ITK og DDF** Vi har inspiceret proceduren for sikkerhedsbrud, og påset, at der er taget stilling til bistand til de dataansvarlige.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.

Kontrolmål J – Betingelser for samtykke og oplysningspligt

Der efterleves procedurer og kontroller, som sikrer, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger, og hvori det sikres, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt anden information, der er nødvendig for opfyldelse af oplysningspligten.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
J.1	Der foreligger skriftlige procedurer for indhentelse af skriftligt samtykke til behandling af personoplysninger. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**DDF og ITK** Vi har forespurgt til, om databehandleren indhenter samtykke på vegne af den dataansvarlige.	**DDF** Vi er blevet oplyst, at databehandleren ikke indhenter samtykke på vegne af den dataansvarlige, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret. **ITK** Vi er blevet oplyst, at databehandleren ikke indhenter samtykke på vegne af den dataansvarlige, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret.
J.2	Der er implementeret tekniske foranstaltninger, der sikrer, at det kan dokumenteres, hvilke oplysninger der er givet i forbindelse med indgåelse af samtykket.	**DDF og ITK** Vi har forespurgt til, om databehandleren indhenter samtykke på vegne af den dataansvarlige.	**DDF** Vi er blevet oplyst, at databehandleren ikke indhenter samtykke på vegne af den dataansvarlige, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret. **ITK** Vi er blevet oplyst, at databehandleren ikke indhenter samtykke på vegne af den dataansvarlige, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret.
J.3	Der foreligger skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at den registrerede modtager oplysninger om formål med behandling af personoplysninger samt oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	**DDF** Vi har stikprøvevis inspiceret oplysningstekster, og stikprøvevis påset, at denne er i overensstemmelse med GDPR.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
J.4	Der foretages løbende – og mindst én gang årligt – kontrol af, at alle registrerede har modtaget beskrivelsen af den registreredes ret til indsigt i, berigtigelse eller sletning af personoplysninger.	**DDF** Vi har inspiceret kontrollen af privatlivspolitikker, og påset, at disse løbende bliver vurderet og opdateret.	Ingen afvigelser konstateret.

Kontrolmål K – Fortegnelse over behandlingsaktiviteter

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
K.1	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	**ITK og DDF** Vi har inspiceret dokumentation for, at der foreligger en fortegnelse over kategorier af behandlings-aktiviteter for den enkelte dataansvarlige med angivelse af den nødvendige information.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
K.2	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	**ITK og DDF** Vi har inspiceret dokumentation for, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er opdateret og korrekt.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.
K.3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	**ITK og DDF** Vi har inspiceret dokumentation for, at ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	**DDF** Ingen afvigelser konstateret. **ITK** Ingen afvigelser konstateret.