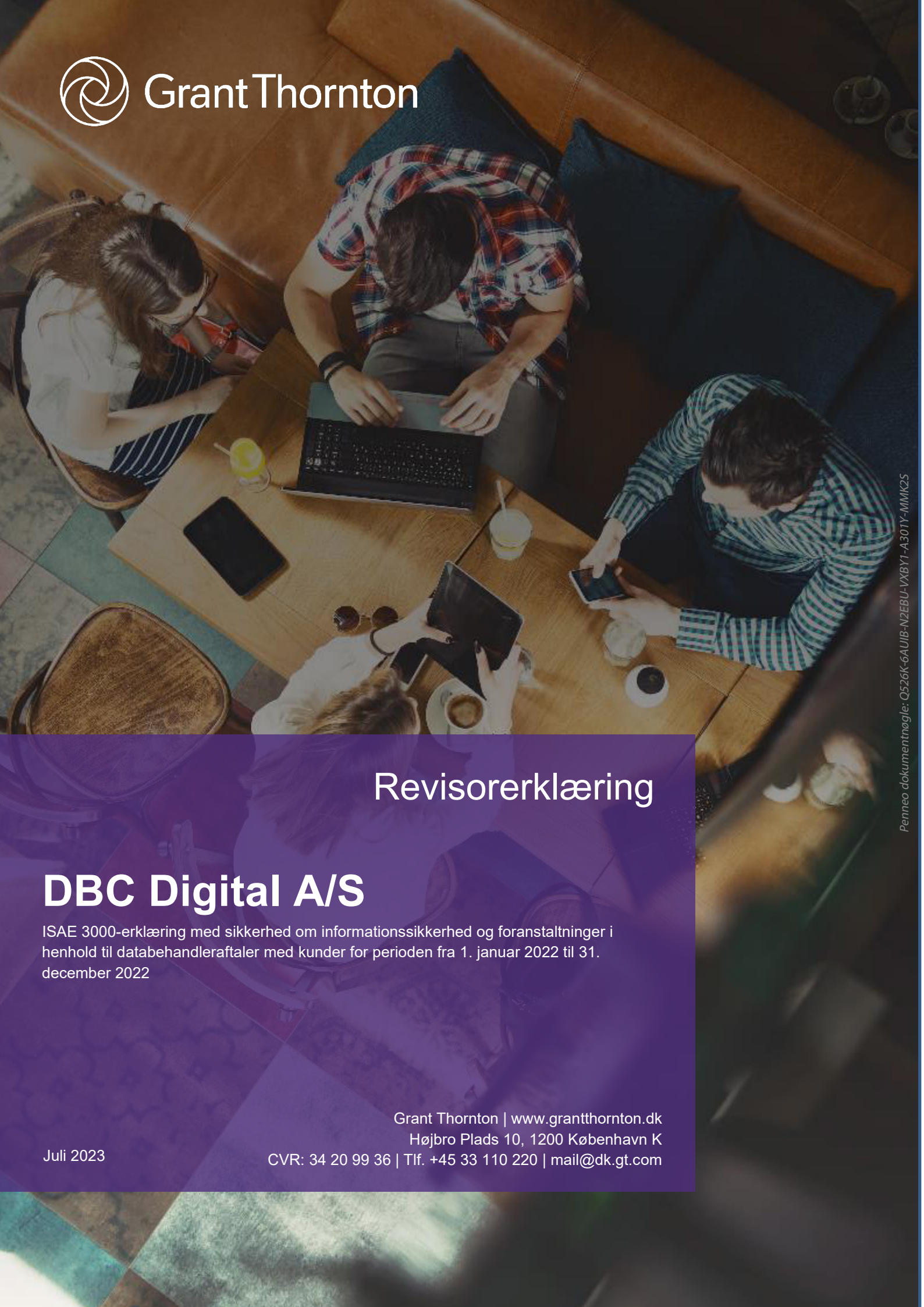

Grant Thornton

Revisorerklæring

DBC Digital A/S

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder for perioden fra 1. januar 2022 til 31. december 2022

Juli 2023

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Indholdsfortegnelse

Afsnit 1: DBC Digital A/S' beskrivelse af behandlingsaktivitet for leverancen af bibliografisk og systemmæssig infrastruktur til biblioteker

Introduktion

Formålet med denne beskrivelse er at levere oplysninger til DBC Digitals (herefter forkortet som DBC) kunder og deres interessenter (herunder revisorer) om kravene og indholdet af EU' s Generelle Databeskyttelsesforordning ("GDPR").

Desuden er formålet med denne beskrivelse at give specifikke oplysninger om spørgsmål vedrørende sikkerheden ved behandling, tekniske og organisatoriske foranstaltninger, ansvar mellem dataansvarlige (vores kunder) og processoren (DBC), og hvordan de tilbudte tjenester kan hjælpe med at understøtte de registreredes rettigheder.

Kontrolmål, herunder regler og procedurer samt gennemførte kontroller

DBC driver, vedligeholder og videreudvikler på opdrag fra KOMBIT en portefølje af produkter, som til sammen udgør den fælles nationale biblioteksinfrastruktur (FBI). Desuden driver, vedligeholder og videreudvikler DBC en række egne produkter primært målrettet bibliotekssektoren.

Principper vedrørende behandling af personoplysninger

Personoplysninger behandles i henhold til den gældende informationssikkerhedspolitik baseret på ISO27001-standarden, samt de indgåede databehandleraftaler med kunder, hvis persondata behandles. Komponenter som enten opbevarer eller indgår i behandling af persondata er identificeret i databehandleraftalerne, med specifik redegørelse for de involverede data, samt behandling og sikring af disse. Derudover forefindes en slettepolitik, som omhandler anonymisering eller sletning af data, når der ikke længere har forretningsmæssig relevans.

Alle persondata behandles i DBC's egne datacentre og der er således ikke en tredjepart involveret i behandlingen.

Risikostyring i DBC

Personoplysninger behandles hovedsagelig som led i biblioteksbetjening og denne behandling er derfor kortlagt i samarbejde med KOMBIT gennem risikovurderinger af de forskellige spor, persondata behandles i. I risikovurderingerne er der foretaget konsekvensanalyser, hvor både konsekvenser for KOMBIT og de registrerede analyseres. Ved siden af dette, kan der forekomme personoplysninger i enkelte produkter, dog ikke følsomme personoplysninger (CPR).

Organisation og ansvar

Informationssikkerhedsorganisationen på DBC er organiseret i form to arbejdsgrupper, samt et operationelt ansvar forankret i linjeorganisationen. I relation til behandling af GDPR-relaterede problemstillinger, er ansvarsfordelingen således:

	Udfører	Ansvarlig	Konsulteres	Informeres
Driftschef		X		
PUD-direktør			X	
Administrerende direktør				X
Incident Manager	X			
Infrastrukturarkitekt			X	
Leverancechef			X	
Chefarkitekt			X	
Informationssikkerhedsudvalg	X			
Teknisk sikkerhedsforum	X			

GDPR og DBC's rolle og ansvar som processor

DBC behandler persondata ud fra retningslinjerne i de indgåede databehandleraftaler.

Samtykke

Samtykke anvendes generelt ikke som behandlingsgrundlag for personoplysninger, da databehandlingen er lovfæstet. For produktet Filmstriben gælder det, at brugeren selv aktivt kan vælge at gemme oplysninger om favoritfilm, lister med titler og ratings i Filmstribens CMS. Disse oplysninger knyttes til et generisk user-id, der er udleveret ved login, styret igennem Bibliotekslogin (Adgangsplatformen), der er en del af FBI-komplekset. Således er den del af persondatahåndteringen underlagt databehandleraftalen for FBI-komplekset.

Behandling af forskellige kategorier af personoplysninger

Som en del af biblioteksbetjeningen, behandles dels almindelige personoplysninger, dels CPR-numre, som anvendes af bibliotekerne til låneridentifikation. Der skelnes ikke mellem almindelige personoplysninger og CPR-numre i forbindelse med databehandlingen. Der er etableret en dataklassifikation, som sikrer at alle komponenter der indgår i behandlingen af personoplysninger, er markeret som indeholdende personhenførbare oplysninger. Klassifikationen revideres årligt, samt ved tilkomst af nye produkter.

Den registreredes rettigheder

Der er etableret procedurer for overholdelse af de registreredes rettigheder. Det tilstræbes, at de registrerede i videst muligt omfang, har adgang til at se sine data eller slette disse. Da oplysningerne gives af de registrerede, er der ikke mulighed for at foretage en berigtigelse. En begrænsning i behandlingen er ikke mulig, da de registrerede derved, ikke kan opnå biblioteksbetjening.

Generelle forpligtelser som processor

DBC er som databehandler bemyndiget til at foretage behandling af personoplysninger for de dataansvarlige. Hvis DBC ønsker at gøre brug af underunderdatabehandlere, skal dette godkendes af kunden. DBC er desuden forpligtet til at sikre personoplysninger ikke databehandles uden for EU.

Databeskyttelsesansvarlig (DPO)

Der er ikke valgt en DPO, da dette ikke vurderes som nødvendigt givet karakteren af de personoplysninger som behandles.

Overførsel af personoplysninger

Der overføres ikke personoplysninger til parter uden for EU.

Sikkerhed for behandling, anmeldelse og kommunikation

Der er etableret tekniske og organisatoriske foranstaltninger baseret på ISO27002.

Der anvendes følgende sikkerhedsforanstaltninger på DBC:

DDOS-angreb

- Leverandøren anvender proxyløsning til DDOS-mitigering, samt abonnerer på anti-DDOS-løsning hos internetudbyderen.

Virus og malware

- Der anvendes antivirus på alle Windows servere. Definitioner opdateres minimum en gang om dagen – og der foretages scanninger minimum én gang om dagen. Der anvendes generelt ikke anti-virus på Linux-miljøet, dog undtaget der, hvor der modtages filer udefra.
- Virus-definitioner opdateres dagligt på Leverandørens arbejdsstationer for at beskytte mod malware og virus, der potentielt vil kunne sprede sig fra de enkelte arbejdsstationer til miljøerne.
- Hvor det er sikkerhedsmæssigt nødvendigt, vil der blive anvendt jump-servere til at tilgå miljøer.
- Der anvendes både enterprise-firewalls til netværkssegmentering og lokale firewalls på alle servere i alle miljøer.

Kompromittering af platform

- Både den centrale sikkerhedsansvarlige og den system-specifikke sikkerhedsansvarlige hos Leverandøren gennemgår løbende meldinger om fundne sårbarheder fra anerkendte kilder og fra de anvendte software/hardware-leverandører.
- Alle niveauer af Systemet og infrastrukturen patches løbende i henhold til gældende sikkerhedspolitik.
- Systemet og infrastrukturen er etableret med høj netværkssikkerhed, hvor det samlede system er placeret på egne netværkssegmenter samt flere lag af firewalls. Internetvendte services er yderligere sikret gennem proxy-løsninger.
- Netværket overvåges løbende ift. anomalier ift. trafikmængder og destinationer, DNS-opslag mv.
- Sikkerhedslogs overvåges løbende for anomalier ift. loginforsøg, rettighedstildelinger mv.
- Der foretages mindst én gang årligt en penetrationstest af Systemet og infrastrukturen.

Datatab

- Der foretages løbende fuld og inkrementel backup og sikring af de vigtigste og mest essentielle data i Systemet.
- Al data opbevares redundant i to geografisk adskilte datacentre.
- Der sikkerhedsopbevares mindst tre sæt af backup-bånd (månedspuljer) hos ekstern leverandør.

Misbrug af data

- Der anvendes detaljeret brugerstyring i Systemet og infrastruktur, så der sikres least-privilege adgang.
- Rettigheder til Systemet og infrastrukturen som Leverandøren administrerer gennemgås løbende i forhold til *least-privilege*. Gennemgangen gennemføres løbende. Når en medarbejder stopper hos Leverandøren fjernes dennes adgange til Leverandørens løsninger.
- Som udgangspunkt holdes al forretningsdata udelukkende i Systemet og kopieres ikke. Hvis kopiering er nødvendig, definerer Leverandørens sikkerhedshåndbog politikker for kopiering – herunder korttidsopbevaring og kryptering.
- Systemet og infrastrukturen revideres ved driftskontraktens ikrafttræden, og herefter årligt i henhold til gængse ISAE- og ISRS-standarder, ud fra en vurdering af de til enhver tid gældende sikkerhedsmæssige behov og krav.

Utilsigtet tilgang til data

- Der anvendes personlige brugere på alle niveauer i Systemet og infrastrukturen – både ved normal brug og i forbindelse med vedligeholdelse.
- Dataanvendelse logges for at danne et detaljeret revisionsspor, der kan bruges til at klarlægge al anvendelse af persondata.

Utilsigtet tilgang til fysisk lokation

- Al adgang til datacentre og andre sikrede områder er aflåste, og beskyttet med kodelås.

Omfattende Infrastrukturnedbrud – servere, netværk mv.

- Datacentre er sikret med UPS-anlæg. Herudover er et af datacentrene sikret med en dieselgenerator.
- Storage tilknyttet Systemet er placeret adskilt i forskellige datacentre/kuber. Der anvendes både Aktiv/passiv samt aktiv/aktiv teknologier til lagring ad Systemets data. Backup foretages både på diske (korttidsbackup) samt på bånd.
- Alle netværkskomponenter er redundante. Internetforbindelser er ligeledes redundante og opkoblet til forskellige centraler.

Miljømæssig påvirkning (storm, lyn mv.)

- Der er opsat Brandmeldeanlæg med aspirationsdetektering i alle datacentre. Disse er tilkoblet til overvågning samt viderestilling af alarm til brandvæsen ved aktivering.
- Datacentre er udstyret lækagedetektorer og disse er tilkoblet overvågning hvorved vagten alarmeres.
- Elinstallationerne i Datacentrene er jordet særskilt, som sikrer mod fejlstrøm.

Kryptografi

- Al datatransmission benytter mindst TLS 1.2 til kryptering af datastrømmen.
- CPR-numre gemmes i krypteret form (256-bit nøgle).

Leverandørforhold

- Der anvendes kun anerkendte leverandører til den tekniske og sikkerhedsmæssige infrastruktur.

Informationssikkerhedshændelse og hændelseshåndtering

- Alle sikkerhedshændelser registreres med en separat kategori i servicedesk. Incident Manager informerer den sikkerhedsansvarlige (IT-chefen) om alle hændelser og der tages stilling til, om beredskabsplanen for informationssikkerhed skal tages i anvendelse.

Informationssikkerhedsaspekter ved styring af forretnings kontinuitet

- Der foretages årlige disaster recovery øvelser, samt kvartalsmæssige restoretests.

Fuld gennemsigtighed for datakontrollere og registrerede

Den registrerede har mulighed for i videst muligt omfang selv at kontrollere de data, der måtte være opsamlet på vedkommendes brugerprofil.

Fortrolighed ved design / standard

Der er beskrevet retningslinjer for kryptering og pseudonymisering af personoplysninger, som skal indarbejdes i forbindelse med design af komponenter, der håndterer personoplysninger.

Compliance

Overholdelse af disse retningslinjer sikres gennem årlig revision ud fra ISAE3000.

Ændringer i perioden

Der er ikke sket væsentlige ændringer i perioden.

Komplementerende kontroller hos de dataansvarlige

På vegne af de dataansvarlige har KOMBIT instruksbeføjelsen over for DBC i henhold til dataansvaret. Desuden er KOMBIT overordnet governance organ for DBC, hvilket reguleres i et kontraktkompleks baseret på KOMBITs standardkontrakter.

I praksis har KOMBIT ikke adgang til DBC's test- eller produktionssystemer, men der aftales på sagsbasis, såfremt der skal udføres specifikke kontroller.

Afsnit 2: DBC Digital A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for DBC Digital A/S' kunder, som har indgået en databehandleraftale med DBC Digital A/S, 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.

Enkelte af de kontrolmål, der er anført i DBC Digital A/S' beskrivelse i afsnit 1 af bibliografisk og systemmæssig infrastruktur til biblioteker, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos DBC Digital A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

DBC Digital A/S bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af, hvordan DBC Digital A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 1. januar 2022 til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan DBC Digital A/S' 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 DBC Digital A/S' 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 bibliografiske og systemmæssige infrastruktur til biblioteker til behandling af personoplysninger foretaget i perioden fra 1. januar 2022 til 31. december 2022

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne bibliografiske og systemmæssige infrastruktur til biblioteker 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 bibliografisk og systemmæssig infrastruktur til biblioteker, 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 perioden fra 1. januar 2022 til 31. december 2022, hvis dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af DBC Digital A/S' kontroller i perioden fra 1. januar 2022 til 31. december 2022. 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 perioden fra 1. januar 2022 til 31. december 2022

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.

Ballerup, den 5. juli 2023
DBC Digital A/S

Jane Wiis
Adm. direktør

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. januar 2022 til 31. december 2022

Til DBC Digital A/S og DBC Digital A/S' kunder i rollen som dataansvarlige.

Omfang

Vi har fået til opgave at afgive erklæring med høj grad af sikkerhed om DBC Digital A/S' beskrivelse i "Afsnit 1" af bibliografisk og systemmæssig infrastruktur til biblioteker i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig i perioden fra 1. januar 2022 til 31. december 2022 og b+c om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Enkelte af de kontrolmål, der er anført i DBC Digital A/S' beskrivelse i afsnit 1 af bibliografisk og systemmæssig infrastruktur til biblioteker, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos DBC Digital A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

DBC Digital A/S' ansvar

DBC Digital A/S 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.

Grant Thorntons 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.

Grant Thornton 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 DBC Digital A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, 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.

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

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 bibliografisk og systemmæssig infrastruktur til biblioteker 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 2".

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

Begrænsninger i kontroller hos en databehandler

DBC Digital A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved bibliografisk og systemmæssig infrastruktur til biblioteker, 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 bibliografisk og systemmæssig infrastruktur til biblioteker, således som denne var udformet og implementeret i perioden fra 1. januar 2022 til 31. december 2022, 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 1. januar 2022 til 31. december 2022, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af DBC Digital A/S' kontroller i perioden fra 1. januar 2022 til 31. december 2022 , 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 1. januar 2022 til 31. december 2022.

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 DBC Digital A/S' bibliografiske og systemmæssige infrastruktur til biblioteker, 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 5. juli 2023

Grant Thornton
Statsautoriseret Revisionspartnerselskab

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Basel Rimon Obari
Executive director, CISA, CISM

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-J 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 1. januar 2022 til 31. december 2022.

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

Vi har udført vores tests af kontroller hos DBC Digital A/S via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos DBC Digital A/S. 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**	*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

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
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*

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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede politikker, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at politikkerne er opdaterede.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	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.	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. 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.	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. Ingen afvigelser konstateret.
A.4	Databehandler opdaterer løbende fortegnelse over behandling af personoplysninger.	Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Vi har inspiceret, at procedurer er opdaterede.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Vi har inspiceret, at antivirus software er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall. Der anvendes DDoS mitigering.	Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Vi har inspiceret, at firewall er konfigureret i henhold til intern politik herfor. Vi har stikprøvevis inspiceret dokumentation for, at der er opsat DDoS mitigering med alarmering.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Netværkskomponenter (f.eks. forbindelser, routere, switches, load balancers) er redundante.	Vi har inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering. Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til netværkssegmentering. Vi har stikprøvevis inspiceret, at netværkskomponenter er redundante.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor. Der anvendes detaljeret brugerstyring i systemet så der sikres least-privilege adgang. Der må ikke anvendes fællesbrugerkonto på systemet.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Vi har stikprøvevis inspiceret adgange, og stikprøvevis påset, at der er et arbejdsbetinget behov. Vi har stikprøvevis inspiceret privilegerede brugere, og stikprøvevis påset, at disse er tilknyttet specifikke medarbejdere.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har stikprøvevis inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Vi har stikprøvevis inspiceret dokumentation for, at der er opsat DDoS mitigering med alarmering.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail. Politikker for håndtering og kopiering af forretningsdata; Som udgangspunkt holdes al forretningsdata udelukkende i systemet og kopieres ikke. Hvis kopiering er nødvendig, definerer underdatabehandlerens sikkerhedshåndbog politikker for kopiering – herunder korttidsopbevaring og kryptering.	Vi har stikprøvevis inspiceret transmission over nettet, og stikprøvevis påset, at dette er krypteret i henhold til intern politik. Vi har stikprøvevis inspiceret, at opbevaring af personoplysninger sker i henhold til intern politik herfor.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.9	Der er etableret logning i systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har stikprøvevis inspiceret den etablerede logning, og stikprøvevis påset, at denne er konfigureret i overensstemmelse med intern politik. Vi har stikprøvevis inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Vi har stikprøvevis inspiceret testdata, og stikprøvevis påset, at dette følger proceduren. Vi har stikprøvevis inspiceret dokumentation for, at udviklingsmøder er blevet afholdt i perioden. Vi har forespurgt til håndtering af supportsager i perioden.	Vi har fået oplyst, at størstedelen af supportsager i perioden er blevet slettet i forbindelse med implementering af et nyt supportsystem, hvorfor det ikke har været muligt at teste kontrollen for supportsager for perioden. Ingen yderligere 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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Vi har inspiceret dokumentation for løbende overvågning af sårbarheder. Vi har stikprøvevis inspiceret netværkskomponenter, og stikprøvevis påset, at dette er vedligeholdt i henhold til intern politik herfor.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	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. Vi har stikprøvevis inspiceret ændringer i perioden, og stikprøvevis påset, at ændringer sker efter den interne procedure.	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.	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. Vi har stikprøvevis inspiceret, at medarbejdernes adgange til systemer og databaser er godkendt, og at der er et arbejdsbetinget behov. Vi har stikprøvevis inspiceret, at fratrådte medarbejderes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Vi har inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering af tildelte brugeradgange.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der er en formel politik for den fysiske sikkerhed. Vi har inspiceret datacenteret, og påset, at sikkerheden er i overensstemmelse med intern politik.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.16	Der foretages løbende backup eller sikring vha. redundans eller lignende af de vigtigste og mest essentielle data i systemet, så der altid er mindst 2 kopier af alle data.	Vi har stikprøvevis påset, at backup bliver foretaget i henhold til intern politik.	Ingen afvigelser konstateret.
B.17	Al data opbevares georedundant i flere datacentre.	Vi har inspiceret dokumentation for georedundante datacentre.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.1	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. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er tilgængelig for databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har stikprøvevis inspiceret, at der er sket efterprøvelse af ansættelser i perioden.	Vi har observeret, at der for tre ud af fem stikprøver, enten ikke er blevet foretaget screening eller været muligt at fremskaffe dokumentation for screening af nyansatte medarbejdere. Ingen yderligere afvigelser konstateret.
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.	Vi har stikprøvevis inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale. Vi har stikprøvevis inspiceret at nyansatte medarbejdere i erklæringsperioden er blevet introduceret til relevante procedurer.	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.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har stikprøvevis inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget for fratrådte medarbejdere i erklæringsperioden.	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.	Vi har stikprøvevis inspiceret, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt for fratrådte medarbejdere i erklæringsperioden.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
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.	Vi har inspiceret dokumentation for, at databehandleren har vurderet behov for en databeskyttelsesrådgiver i perioden.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
D.1	Der foreligger skriftlige politikker, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om politikker skal opdateres.	Vi har inspiceret, at der foreligger formaliserede politikker, som foreskriver, at databehandleren skal handle efter instruks fra den dataansvarlige. Vi har inspiceret, at politikkerne er opdaterede.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har inspiceret databehandleraftale, og påset, at der er taget stilling til sletning og tilbagelevering af personoplysninger ved ophør af databehandleraftalen. Vi har forespurgt til ophørte databehandlinger i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været ophørte databehandlinger i perioden, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. 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.	Vi har forespurgt til ophørte databehandlinger i erklæringsperioden. Vi har stikprøvevis påset den løbende sletning af personoplysninger.	Vi er blevet informeret om, at der ikke har været ophørte databehandlinger i perioden, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. 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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
E.1	Der foreligger skriftlige politikker, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om politikker skal opdateres.	Vi har inspiceret, at der foreligger formaliserede politikker, som foreskriver, at databehandleren skal handle efter instruks fra den dataansvarlige. Vi har inspiceret, at politikkerne er opdaterede.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	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. Vi har stikprøvevis påset, at backup bliver foretaget i henhold til intern politik.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt til, om databehandleren anvender underdatabehandlere.	Vi er blevet informeret om, at databehandleren ikke har underdatabehandlere, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har forespurgt til, om databehandleren anvender underdatabehandlere.	Vi er blevet informeret om, at databehandleren ikke har underdatabehandlere, hvorfor punktet ikke er relevant. 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.	Vi har forespurgt til, om databehandleren anvender underdatabehandlere.	Vi er blevet informeret om, at databehandleren ikke har underdatabehandlere, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har forespurgt til, om databehandleren anvender underdatabehandlere.	Vi er blevet informeret om, at databehandleren ikke har underdatabehandlere, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har forespurgt til, om databehandleren anvender underdatabehandlere.	Vi er blevet informeret om, at databehandleren ikke har underdatabehandlere, hvorfor punktet ikke er relevant. 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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons 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 revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har forespurgt til, om databehandleren anvender underdatabehandlere.	Vi er blevet informeret om, at databehandleren ikke har underdatabehandlere, hvorfor punktet ikke er relevant. 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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons 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.	Vi har inspiceret, at der er en politik, som sikrer, at databehandleren ikke må handle uden direkte instruks fra den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har inspiceret databehandleraftaler med dataansvarlige, og påset, at der er taget stilling til tredjelandsoverførsler. Vi har forespurgt til, om databehandleren overfører personoplysninger til tredjelande eller internationale organisationer.	Vi er blevet informeret om, at databehandleren ikke overfører persondata til tredjelande, og vi finder det sandsynliggjort baseret på vores testhandlinger. 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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret databehandleraftaler med dataansvarlige, og påset, at der er taget stilling til tredjelandsoverførsler. Vi har forespurgt til, om databehandleren overfører personoplysninger til tredjelande eller internationale organisationer.	Vi er blevet informeret om, at databehandleren ikke overfører persondata til tredjelande, og vi finder det sandsynliggjort baseret på 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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdaterede.	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.	Vi har forespurgt, om databehandleren har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder.	Vi er blevet informeret om, at databehandleren ikke har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. 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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Vi har stikprøvevis inspiceret dokumentation for, at databehandleren har afholdt sikkerhedsmøder i perioden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har forespurgt, om der har været persondatassikkerhedsbrud i perioden.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. 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.	Vi har inspiceret, at de foreliggende procedurer understøtter de dataansvarlige ved brud på persondatasikkerheden.	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.	*DBC Digital A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
J.1	Der foreligger skriftlige procedurer for indhentelse af skriftligt samtykke til behandling af personoplysninger.	Vi har forespurgt til, om virksomheden indhenter samtykke på vegne af dataansvarlige.	Vi er blevet informeret om, at databehandleren ikke indhenter samtykke på vegne af de 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.	Vi har forespurgt til, om virksomheden indhenter samtykke på vegne af dataansvarlige.	Vi er blevet informeret om, at databehandleren ikke indhenter samtykke på vegne af de 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.	Vi har inspiceret privatlivspolitikken, og påset, at denne indeholder relevante oplysninger om behandlingen af personoplysninger.	Ingen afvigelser konstateret.
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.	Vi inspiceret den løbende kontrol af oplysningstekster, og påset, at oplysningstekster er blevet opdateret i perioden.	Ingen afvigelser konstateret.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jane Wiis
Underskriver 1
Serienummer: 6e418266-10c0-4ff0-be24-3de9f17a3264
IP: 212.112.xxx.xxx
2023-07-05 17:10:58 UTC

Basel Rimon Obari
GRANT THORNTON,STATSAUTORISERET REVISIONSPARTNERSELSKAB
CVR: 34209936
Underskriver 2
Serienummer: 83192c2a-26a4-4658-812e-ed0c3d0b45d6
IP: 87.49.xxx.xxx
2023-07-05 19:39:48 UTC

Jacob Helly Juell-Hansen
GRANT THORNTON,STATSAUTORISERET REVISIONSPARTNERSELSKAB
CVR: 34209936
Underskriver 3
Serienummer: f17041a5-2020-4c05-998a-fb15e6cdd8f6
IP: 62.243.xxx.xxx
2023-07-06 05:45:28 UTC