AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 1. JUNI 2024 OM BESKRIVELSEN AF DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER I ADMINISTRATIONEN AF DAGINSTITUTIONER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Landsorganisationen Danske Daginstitutioner

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 1. JUNI 2024 OM BESKRIVELSEN AF DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER I ADMINISTRATIONEN AF DAGINSTITUTIONER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Landsorganisationen Danske Daginstitutioner
Landsorganisationen Danske Daginstitutioners kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Landsorganisationen Danske Daginstitutioner (databehandleren) pr. 1. juni 2024 udarbejdede beskrivelse i sektion 3 af databehandlerens behandling af personoplysninger i administrationen af daginstitutioner og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen pr. 1. juni 2024.

Vi har ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme og implementere kontroller for at opnå de anførte kontrolmål.

Revisors 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.

BDO Statsautoriseret revisionsaktieselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af databehandlerens behandling af personoplysninger i administrationen af daginstitutioner, som hver enkelt dataansvarlig måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

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 databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af databehandlerens behandling af personoplysninger i administrationen af daginstitutioner og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 1. juni 2024, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 1. juni 2024.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens databehandlerens behandling af personoplysninger i administrationen af daginstitutioner, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 26. juni 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. LANDSORGANISATIONEN DANSKE DAGINSTITUTIONER UDTALELSE

Landsorganisationen Danske Daginstitutioner varetager behandling af personoplysninger i forbindelse med databehandlerens behandling af personoplysninger i administrationen af daginstitutioner for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt databehandlerens behandling af personoplysninger i administrationen af daginstitutioner og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Landsorganisationen Danske Daginstitutioner anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Landsorganisationen Danske Daginstitutioner bekræfter, at den medfølgende beskrivelse på side [xx til xx] giver en retvisende beskrivelse af databehandlerens behandling af personoplysninger i administrationen af daginstitutioner og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 1. juni 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for behandling af personoplysninger i administrationen af daginstitutioner, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at begrænse behandling af personoplysninger.
    - De processer der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - De processer der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
    - De processer der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
    - De processer der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af databehandlerens behandling af personoplysninger i administrationen af daginstitutioner og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved databehandlerens behandling af personoplysninger i administrationen af daginstitutioner, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

Landsorganisationen Danske Daginstitutioner bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 1. juni 2024. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. 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.

Landsorganisationen Danske Daginstitutioner bekræfter, at der er implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Allerød, den 26. juni 2024

Landsorganisationen Danske Daginstitutioner

Palle Woss
Direktør

3. LANDSORGANISATIONEN DANSKE DAGINSTITUTIONER'S BESKRIVELSE AF BEHANDLING AF PERSONOPLYSNINGER I ADMINISTRATIONEN AF DAGINSTITUTIONER

LANDSORGANISATIONEN DANSKE DAGINSTITUTIONER

Det er LDD's formål, gennem frivilligt arbejde, at virke for tilvejebringelse af de bedst mulige vilkår for børns opvækst, udvikling og trivsel, blandt andet ved på landsplan at virke for og medvirke ved etablering og drift af private og selvejende institutioner - primært for børn og unge, samt i øvrigt at arbejde for at fremme den selvejende institutionsform.

LDD udfører blandt andet administrative funktioner i forbindelse med den daglige drift af selvejende institutioner, herunder løn og personaleadministration, regnskabsførelse samt rådgivning og konsulentbistand til bestyrelse og ledelse i de til organisationen knyttede medlemsinstitutioner.

LDD styrer persondatasikkerhed i forhold til den behandling, som LDD varetager på vegne af sine kunder, herunder indgåelse af databehandleraftaler, besvarelse af henvendelser fra den dataansvarlige, underretning om brud på persondatasikkerheden, efterlevelse af interne politikker og procedurer og lignende.

ADMINISTRATIONEN AF DAGINSTITUTIONER OG BEHANDLING AF PERSONOPLYSNINGER

LDD behandler personoplysninger på vegne af sine kunder, der er dataansvarlige, når LDD bistår med administrationen af daginstitutioner. LDD har indgået databehandleraftaler med de dataansvarlige om denne behandling.

De personoplysninger, der behandles, henhører under databeskyttelsesforordningens artikel 6 om almindelige personoplysninger og omfatter blandt andet personnavn, e-mail, telefonnummer og identifikation.

STYRING AF PERSONDATASIKKERHED

LDD har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter:

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
Risikovurdering	• Risikovurdering	• Artikel 28, stk. 3, litra c
A.5: Informationssikkerhedspolitikker	• Politikker for informationssikkerhed og databeskyttelse • Gennemgang af persondatapolitik herunder tekniske sikkerhedsforanstaltninger	• Artikel 28, stk. 1
A.6: Organisering af informationssikkerhed	• Roller og ansvarsområder • Politik for mobilt udstyr • Fjernarbejdspladser og fjernadgang til systemer og data	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra c
A.7: Personalesikkerhed	• Rekruttering af medarbejdere	• Artikel 28, stk. 1

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
	• Uddannelse og instruktion af medarbejdere, der behandler personoplysninger • Tavsheds- og fortrolighedsaftale med medarbejdere og eksterne leverandører og konsulenter • Fratrædelse af medarbejdere	• Artikel 28, stk. 3, litra b
A.8: Styring af aktiver	• Fortegnelse over kategorier af behandlingsaktiviteter • Opbevaring af fortegnelsen • Datatilsynets adgang til fortegnelsen • Bortskaffelse af medier	• Artikel 30, stk. 2, 3 og 4
A.9: Adgangsstyring	• Brugerregistrering og -afmelding • Tildeling af brugeradgange • Gennemgang af brugeradgangsrettigheder • Procedure for sikker log-on	• Artikel 28, stk. 3, litra c
A.10: Kryptografi	• Politik for anvendelse af kryptografi	• Artikel 28, stk. 3, litra c
A.11: Fysisk sikring og miljøsikring	• Fysisk adgangskontrol • Fysisk sikkerhed • Vedligeholdelse af udstyr • Sikring af udstyr og aktiver for organisationen • Reparation og service samt bortskaffelse af it-udstyr • Politik for ryddeligt skrivebord og blank skærm	• Artikel 28, stk. 3, litra c
A.12: Driftssikkerhed	• Vedligeholdelse af systemsoftware • Antivirusprogram • Sikkerhedskopiering og retablering af data • Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger	• Artikel 28, stk. 3, litra c
A.13: Kommunikationssikkerhed	• Netværkssikkerhed • Firewall • Eksterne kommunikationsforbindelser	• Artikel 28, stk. 3, litra c
A.14: Anskaffelse, udvikling og vedligeholdelse	• Analyse og specifikation af informationssikkerhedskrav • Udvikling og vedligeholdelse af systemer • Informationssikkerhed i ændring og udvikling • Adskillelse af udviklings-, test- og produktionsmiljø • Personoplysninger i udviklings- og testmiljø	• Artikel 25
A.15: Leverandørforhold	• Underdatabehandleraftale og instruks • Godkendelse af underdatabehandlere • Ændringer i godkendte underdatabehandlere • Oversigt over godkendte underdatabehandlere • Tilsyn med underdatabehandlere	• Artikel 28, stk. 2 og 4
A.16: Styring af informationssikkerhedsbrud	• Ansvar og procedurer • Underretning om brud på persondatasikkerheden • Identifikation af brud på persondatasikkerheden • Registrering af brud på persondatasikkerheden	• Artikel 33, stk. 2
A.18: Overensstemmelse	• Indgåelse af databehandleraftale med den dataansvarlige • Instruks for behandling af personoplysninger • Efterlevelse af instruks for behandling af personoplysninger • Underretning af den dataansvarlige ved ulovlig instruks • De registreredes rettigheder • Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser • Revision og inspektion • Sletning af personoplysninger • Tilbagelevering af personoplysninger • Overførsel af personoplysninger til tredjelande • Instruks fra den dataansvarlige • Gyldigt overførselsgrundlag	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra a, c, e, f, g og h • Artikel 29 • Artikel 32, stk. 4 • Artikel 28, stk. 10 • Artikel 44 – 49

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
	• Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger	

RISIKOVURDERING

LDD er ansvarlig for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som LDD til enhver tid står over for, således at indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

Der foretages en løbende vurdering af, hvilket sikkerhedsniveau, der er passende. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller udføres der en gang årligt en risikovurdering. Risikovurderingen belyser sandsynligheden for og konsekvenserne af hændelser, der kan true persondatasikkerheden og dermed fysiske personers rettigheder og frihedsrettigheder, herunder tilfældige, forsætlige og uforsætlige hændelser. Risikovurderingen tager hensyn til det aktuelle tekniske niveau og implementeringsomkostningerne.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller vedrører alle processer og systemer, som behandler personoplysninger på vegne af den dataansvarlige. De i kontrolskemaet anførte kontrolmål og kontrolaktiviteter er en integreret del af den efterfølgende beskrivelse.

Softwareudviklingen af it-løsninger er outsourcet til KMD A/S, som underdatabehandler, ligesom IT services herunder hosting, backup, patch management og overvågning af virtuelle servere er outsourcet til Advania Danmark A/S. Der benyttes endvidere andre underdatabehandlere, som der tillige er indgået databehandleraftaler med.

A.5: Informationssikkerhedspolitikker

LDD har indført politikker og procedurer, der er med til at sikre, at LDD kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. LDD har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres.

A.6: Organisering af informationssikkerhed

Roller og ansvarsområder

LDD har indført ledelsesstyring af informationssikkerhed og databeskyttelse, herunder LDD's rolle kontra den enkelte ansattes personlige ansvar og eventuel bøde- og/eller fængselsstraf ved overtrædelse af databeskyttelsesreglerne.

LDD fører endvidere en fortegnelse over behandlingsaktiviteter opdelt på dets interne faggrupper, der omfatter (1) HR-gruppe, (2) Konsulentgruppe, (3) Løngruppe og (4) Regnskabsgruppe. Det sker med henblik på at sikre overskuelighed over de forskellige behandlingsaktiviteter, hvormed LDD's niveau af ansvarlighed ("accountability") højnes, da opdelingen tillige er naturlig i forhold til LDD's drift.

Politik for mobilt udstyr
LDD har indført procedurer, der er med til at sikre, at adgang via bærbare computere, tablets og smartphones begrænses, og at de ansatte skal overholde interne retningslinjer for alle enheder.

LDD opretholder krav om adgangskode, således at de ansatte ikke kan opnå adgang til LDD's servere uden at overholde dets interne procedure for henholdsvis udformning af og periodeskift for den adgangskode, der er adgangsgivende til serveren.

Fjernarbejdspladser og fjernadgang til systemer og data
LDD har indført procedurer, der er med til at sikre, at adgang fra arbejdspladser uden for LDD's lokaler og fjernadgang til systemer og data sker via Awingu. Awingu er et single sign-on system (SSO) med Remote Desktop Protokol (RDP).

Herudover beskyttes de behandlede personoplysninger ved kontinuerligt at opdatere henholdsvis firewall og antivirus, hvormed det sikres, at udefrakommende fjendtlige angreb forhindres, da organisationens IT-sikkerhed dermed er bedst muligt rustet mod kendte såvel som ukendte IT-trusler.

A.7: Personalesikkerhed

Rekruttering og fratrædelse af medarbejdere
Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere.

Der udføres ansættelsessamtaler og indhentes referencer med henblik på udvælgelse af kvalificerede medarbejdere, herunder indhentning af samtykkeerklæring og tavshedserklæring.

Herudover er proceduren for fratrædelse af medarbejdere med til at sikre, at adgange til IT-systemer og brugerprofil lukkes. Ligesom udleveret mobilt IT-udstyr og Ipad, nøgler mv. skal leveres tilbage.

Uddannelse og instruktion af medarbejdere, der behandler personoplysninger, og Awareness og oplysningskampagner for medarbejdere
Der er krav om, at de ansatte kontinuerligt oplæres i relevant databeskyttelseslovgivning, og gøres bekendt med, hvilke sikkerhedsrisici LDD's databehandling er udsat for, samt hvilke sikkerhedsforanstaltninger LDD har implementeret til imødegåelse heraf, og hvordan disse benyttes. Med andre ord vil LDD benytte sig af princippet: "Raising User Awareness". Der blandt andet er et fast punkt vedrørende information omhandlende GDPR på kvartalsvise personalemøder.

Fortrolighed og lovbestemt tavshedspligt
LDD har indført politikker og procedurer, der er med til at sikre fortrolighed ved behandlingen af personoplysninger. Alle medarbejdere i LDD har forpligtet sig til fortrolighed ved at underskrive en ansættelseskontrakt, der indeholder vilkår om tavshed og fortrolighed. Tillige underskriver eksterne konsulenter en tavshedserklæring, der fortsat gælder efter afslutning af deres arbejde for LDD.

A.8: Styring af aktiver

Fortegnelse over kategorier af behandlingsaktiviteter
LDD har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

Bortskaffelse af medier

LDD forestår bortskaffelse eller destruktion af samtlige dokumenter indeholdende personoplysninger, der lagres på et lagringsmedie, såsom USB-nøgler, eksterne harddiske eller lignende. I den henseende slettes samtlige filer, der indeholder personoplysninger, forinden lagringsmediet bortskaffes eller destrueres.

Ekstern leverandør destruerer datamedier sikkert og forsvarligt. Proceduren for kassering af medier er med til at sikre, at det kontrolleres, at leverandøren kan leve op til sikker destruktion af datamedier. Ligesom leverandøren afhenter datamedier hos LDD mod kvittering, og ligesom leverandøren efter destruktion skal fremsende dokumentation for, at destruktionen er sket.

A.9: Adgangsstyring

LDD har indført procedurer, der er med til at sikre, at adgange til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikationen anvendes ved tildeling af adgange til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde og kompleksitet følger best practice for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

A.10: Kryptografi

LDD har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier og øvrige lagringsmedier. Gemmes dokumenterne lokalt på arbejdscomputeren, skal disse krypteres.

LDD anvender Advania som leverandør af opsætning af Awingu, som sikrer en begrænset adgang på en krypteret https protokol.

A.11: Fysisk sikring og miljøsikring

Fysisk adgangskontrol

LDD har indført procedurer, som er med til at sikre, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne.

Fysisk sikkerhed

LDD har indført procedurer, der er med til at sikre, at servere er beskyttet mod uautoriseret adgang, beskadigelse, driftsafbrydelser og lignende hændelser ved særlige sikkerhedsforanstaltninger.

Vedligeholdelse af udstyr

LDD's eksterne såvel som interne harddiske sendes som udgangspunkt ikke til reparation, da det ikke vurderes muligt at beskytte de lagrede personoplysninger tilstrækkeligt fra det tidspunkt, hvor harddisken forlader organisationens lokaliteter. LDD har på den baggrund implementeret en politik om, at harddiske i stedet destrueres og erstattes af nye.

Sikring af udstyr og aktiver for organisationen

LDD har indført procedurer, der særligt vedrører mobilt udstyr, herunder bærbare computere, tablets og smartphones, og at de ansatte skal overholde interne retningslinjer for alle enheder.

Reparation og service samt bortskaffelse af it-udstyr

LDD har indført procedurer, der er med til at sikre, at udstyr, som udleveres til tredjemand for bortskaffelse, udleveres uden datadiske, og at brugte og kasserede datamedier og diske registreres og destrueres af certificeret leverandør.

Politik for ryddeligt skrivebord og blank skærm
LDD har indført procedurer om, at skærmlås skal aktiveres automatisk efter 5 min., medarbejdere skal aktivere skærmlås, når klienten forlades. Ligesom fysisk materiale med personoplysninger skal opbevares i aflåst skab, når materialet forlades, og fysisk materiale må kun printes med 'follow-me' funktion og fjernes straks fra printeren.

A.12: Driftssikkerhed

Vedligeholdelse af systemsoftware
LDD har via outsourcing til Advania indført procedurer, der er med til at sikre, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og software installeret på servere og arbejdsstationer.

Antivirusprogram
LDD har indført procedurer, der er med til at sikre, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer i forhold til det aktuelle trusselsniveau, og der er opsat en løbende overvågning af disse systemer.

Sikkerhedskopiering og retablering af data
LDD har via outsourcing til Advania indført procedurer, der er med til at sikre, at systemer og data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation. Sikkerhedskopier er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde, eller at sikkerhedskopier ødelægges ved brand, vand, hærværk eller hændelig skade.

Logning i systemer, databaser og netværk
LDD har indført procedurer, der er med til at sikre, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret mod tab og sletning.

A.13: Kommunikationssikkerhed

Netværkssikkerhed
LDD har indført procedurer, der sikrer, at netværk i forhold til anvendelse og sikkerhed er opdelt i et antal virtuelle netværk (VLAN), hvor trafik mellem de enkelte virtuelle netværk kontrolleres af firewall. Servere med indbygget firewall benytter denne til at sikre, at der kun gives adgang til nødvendige services.

Firewall
LDD har indført procedurer, der via underdatabehandler Advania sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Eksterne kommunikationsforbindelser
LDD har indført procedurer, der via underdatabehandler Advania sikrer, at eksterne kommunikationsforbindelser er sikret med kryptering ved brug af Awingu, og at e-mail og anden kommunikation, der indeholder følsomme personoplysninger, er krypteret i forsendelsen ved anvendelse af sikker mail.

A.14: Anskaffelse, udvikling og vedligeholdelse

Udvikling og vedligeholdelse af systemer
LDD har indført politikker og procedurer for udvikling og vedligeholdelse af administrative IT-systemer, der sikrer en styret ændringsproces. Udvikling foretages af ekstern leverandør, mens brugertest foretages i test-

system af LDD, inden ændringer overføres til produktion. Enhver udviklings- og ændringsopgave gennemløber således et testforløb. Der er hos ekstern leverandør indført procedurer for versionskontrol, logning og sikkerhedskopiering, således at det er muligt at geninstallere tidligere versioner.

A.15: Leverandørforhold

Underdatabehandleraftale og instruks

LDD har indført politikker og procedurer, der sikrer, at underdatabehandlere er blevet pålagt de samme databeskyttelsesforpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og LDD, og at underdatabehandlerne kan give tilstrækkelige garantier til beskyttelse af personoplysninger. Procedurer sikrer, at den dataansvarlige giver en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere, herunder at der sker en styring af ændringer i godkendte underdatabehandlere.

LDD vurderer underdatabehandleren og dennes garantier, forinden der indgås aftale, for at sikre, at underdatabehandleren kan overholde de forpligtelser, som er pålagt LDD. LDD fører et årligt tilsyn med sine underdatabehandlere, baseret på en risikovurdering af den konkrete behandling af personoplysninger, ved blandt andet at indhente revisorerklæringer af typen ISAE 3000 eller SOC 2 eller lignende dokumentation.

A.16: Styring af informationssikkerhedsbrud

LDD har indført politikker og procedurer, der er med til at sikre, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at LDD er blevet opmærksom på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at foretage en vurdering af, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring

Beredskabsplaner

Med udspring i den aktuelle risikovurdering vurderes det, at der ikke er behov for at etablere fastlagte beredskabsplaner i virksomheden. Beredskabsplan ved datasikkerhedsbrud forefindes.

A.18: Overensstemmelse

Indgåelse af databehandleraftale med dataansvarlige

LDD har indført politikker og procedurer for indgåelse af databehandlingsaftaler, der sikrer, at LDD i tilknytning til kundekontrakten indgår en databehandleraftale, der angiver betingelserne for behandling af personoplysninger på vegne af den dataansvarlige. LDD anvender en skabelon for databehandleraftaler i overensstemmelse med de ydelser, der leveres, herunder information om brugen af underdatabehandlere. Databehandleraftalerne er underskrevet og opbevares elektronisk.

Instruks for behandling af personoplysninger

LDD har indført politikker og procedurer, der sikrer, at LDD handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske. Proceduren sikrer desuden, at LDD informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

Bistand til den dataansvarlige

LDD's bistand omfatter, at LDD skal bistå dets kunder med at iagttage dets pligter i relation til at besvare anmodninger om udøvelse af de registreredes rettigheder. Dette kan indeholde aktiviteter såsom ekstraktion af oplysninger, indsamling og/eller berigtigelse af oplysninger.

LDD har indført politikker og procedurer, der sikrer, at LDD kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 34 – 36 om konsekvensanalyser.

LDD har indført politikker og procedurer, der sikrer, at LDD kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige. LDD sikrer løbende dets overholdelse af de indgående databehandleraftaler, ligesom overholdelsen årligt vil blive påset af en uafhængig tredjepart i form af udfærdigelse af en revisionserklæring. Desuden giver LDD mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

Sletning og tilbagelevering af personoplysninger

LDD har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Afprøvning, vurdering og evaluering

LDD har indført procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i Landsorganisationen Danske Daginstitutioners beskrivelse af databehandlerens behandling af personoplysninger i administrationen af daginstitutioner samt for udformningen af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

BDO's test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af Landsorganisationen Danske Daginstitutioner, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 1. juni 2024.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion og observation.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.

Softwareudviklingen af it-løsninger er outsourcet til Azets Perspektiv A/S, hvorfra vi har modtaget ISAE 3000 GDPR-erklæring for perioden fra 1. juli 2023 til 31. december 2023. Herudover er IT services herunder hosting, backup, patch management og overvågning af virtuelle servere outsourcet til Advania Danmark A/S, hvorfra vi har modtaget ISAE 3402 erklæring for perioden fra 1. juni 2022 til 31. maj 2023 Herudover anvendes Microsoft Office 365 i administrationen hvorfra vi har modtaget SOC 2 erklæring for perioden 1. oktober 2022 til 30. september 2023.

Disse underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Landsorganisationen Danske Daginstitutioners beskrivelse af databehandlerens behandling af personoplysninger i administrationen af daginstitutioner og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos Landsorgani-

sationen Danske Daginstitutioner, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

Resultatet af de udførte test af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet eller implementeret.

Risikovurdering		
Kontrolmål ▶ *At sikre, at databehandleren udfører en årlig risikovurdering i forhold til konsekvenserne for de registrerede, der danner grundlag for de tekniske og organisatoriske sikkerhedsforanstaltninger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risikovurderinger opdateres løbende efter behov, og som minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, risikovurderingen, hvor det fremgår, at risikovurderingen er foretaget ud fra en samlet vurdering af det aktuelle tekniske niveau, implementeringsomkostninger og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. Vi har ligeledes inspiceret, at sårbarheder af systemer og processer vurderes ud fra identificerede trusler. Vi har inspiceret, at risikovurderingen opdateres løbende og som minimum en gang årligt.	Ingen afvigelser konstateret.

A.5: Informationssikkerhedspolitikker

Kontrolmål

- *At give retningslinjer for og understøtte informationssikkerheden og behandling af personoplysninger i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter – GDPR artikel 28, stk.1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politikker for informationssikkerhed og databeskyttelse - Databehandleren har udarbejdet og implementeret en persondatapolitik indeholdende tekniske sikkerhedsforanstaltninger i forhold til informationssikkerhed. - Databehandleren har udarbejdet og implementeret en politik, indeholdende en garanti om bistand og forpligtelse til, at opnå overholdelse af relevante krav, love og forskrifter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har Inspiceret databehandlerens persondatapolitik hvor det fremgår, at denne indeholder politikker for tekniske sikkerhedsforanstaltninger i forhold til informationssikkerhed. Vi har inspiceret, at databehandleren anvender professionel bistand således, at databehandleren sikrer efterlevelse af databeskyttelseslovgivningen herunder bistand til den dataansvarlige. Databehandleren sikrer løbende overholdelse af relevante forretningsmæssige krav og relevante love og forskrifter.	Ingen afvigelser konstateret.
Gennemgang af persondatapolitik herunder tekniske sikkerhedsforanstaltninger - Databehandlerens persondatapolitik og tekniske sikkerhedsforanstaltninger bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har Inspiceret, at databehandlerens persondatapolitik. Vi har inspiceret, at databehandlerens persondatapolitik senest er opdateret april 2024.	Ingen afvigelser konstateret.

A.6: Organisering af informationssikkerhed

Kontrolmål

- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed og behandling af personoplysninger I organisationen – GDPR artikel 37, stk. 1.*
- *At sikre fjernarbejdspladser og brugen af mobilt udstyr - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Roller og ansvarsområder ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed og databeskyttelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret persondatapolitikken hvor det fremgår, at der er etableret ledelsesstyring af informationssikkerhed og databeskyttelse. Vi har inspiceret, at persondatapolitikken er godkendt af ledelsen.	Ingen afvigelser konstateret.
Politik for mobilt udstyr ▶ Databehandleren har udarbejdet og implementeret en politik og understøttende sikkerhedsforanstaltninger til styring af risici for personoplysninger, der opstår ved anvendelse af mobilt udstyr.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at denne indeholder en politik vedrørende mobilt udstyr. Vi har inspiceret, at databehandleren har udarbejdet og implementeret understøttende foranstaltninger, herunder adgangskode. skærmlås samt Bitlocker på mobilt udstyr.	Ingen afvigelser konstateret.
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. ▶ Fjernadgang til databehandlerens systemer og data sker via Awingu.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er installeret antivirus og Bitlocker kryptering på alle computere. Vi har inspiceret, at der anvendes Awingu til fjernadgang for at kunne tilgå LDDs systemer og data.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt - GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra b og artikel 37, stk. 1.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar - GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra c.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør - GDPR artikel 28, stk. 3, litra b.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Rekruttering af medarbejdere ▶ Databehandleren indhenter referencer på jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for rekruttering, hvor det fremgår, at referencer skal indhentes på jobkandidater. Vi har på forespørgsel fået oplyst, at der indhentes referencer på jobkandidater.	Ingen afvigelser konstateret.
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. ▶ Databehandleren foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og persondatapolitik og procedurer herfor.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for uddannelse hvor det fremgår, at denne anfører, hvem der er ansvarlig for sikring af uddannelse inden for persondatasikkerhed samt slette- og opbevaringspolitikker. Dette gælder for alle medarbejdere i LDD. Vi har på forespørgsel fået oplyst, at nye medarbejdere gennemfører et introprogram. Vi har Inspiceret en stikprøve på den seneste tiltrådte medarbejder hvor det fremgår, at der er skrevet under på erklæring vedr. introduktion til LDD's persondatapolitik for nyansatte. Vi har inspiceret, at databehandleren afholder løbende personalemøder, hvor GDPR bliver drøftet samt Awareness-kampagner i form af plakater.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt - GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra b og artikel 37, stk. 1.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar - GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra c.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør - GDPR artikel 28, stk. 3, litra b.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Tavsheds- og fortrolighedsaftale med medarbejdere og eksterne leverandører og konsulenter ▶ Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshed og fortrolighed. ▶ Eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret en stikprøve på den seneste tiltrådte medarbejder hvor det fremgår, at ansættelseskontrakten er underskrevet samt indeholder en bestemmelse vedrørende tavshedspligt samt tro- og loveerklæring. Vi har inspiceret skabelon for eksterne konsulenters tavshedspligt og observeret, at denne anfører, at tavshedspligten gælder under og efter leverandørforholdets beståen. Vi har inspiceret den seneste indgåede erklæring om tavshedspligt med ekstern konsulent og har observeret, at der foreligger en underskreven tavshedserklæring.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure vedrørende fratrædelse hvor det fremgår, at der er en klar procedure i forbindelse med, at medarbejdere fratræder deres stilling. Vi har udtaget stikprøve til dokumentation for fratrædelse, og inspiceret, at databehandleren dokumenterer, at den senest fratrådte medarbejder har fået fjernet adgange til AD i henhold til proceduren.	Ingen afvigelser konstateret.

A.8: Styring af aktiver

Kontrolmål

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf. GDPR artikel 30, stk. 2, artikel 30, stk. 3 og artikel 32, stk. 2.*
- *At sikre passende beskyttelse af information og personoplysninger, der står i forhold til informationens og personoplysningernes betydning for organisationen og de registrerede - GDPR artikel 30, stk. 3 og artikel 30, stk. 4.*
- *At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information og personoplysninger lagret på medier - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at fortegnelse over behandlingsaktiviteter indgår heri. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at denne specificerer, at fortegnelsen løbende skal gennemgås og af hvem. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at fortegnelsen senest er opdateret i marts 2024.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at fortegnelsen opbevares elektronisk.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure, hvor det fremgår, at der heri er anført, at databehandleren skal udlevere fortegnelsen på anmodning fra Datatilsynet. Vi har på forespørgsel fået oplyst, at databehandleren ikke har modtaget anmodning om udlevering af fortegnelsen til datatilsynet hvorfor vi ikke har kunnet efterprøve proceduren.	Vi har på forespørgsel fået oplyst, at databehandleren ikke har modtaget anmodning om udlevering af fortegnelsen til datatilsynet hvorfor vi kan udtale os om kontrollens implementering. Ingen afvigelser konstateret.

A.8: Styring af aktiver

Kontrolmål

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf. GDPR artikel 30, stk. 2, artikel 30, stk. 3 og artikel 32, stk. 2.*
- *At sikre passende beskyttelse af information og personoplysninger, der står i forhold til informationens og personoplysningernes betydning for organisationen og de registrerede - GDPR artikel 30, stk. 3 og artikel 30, stk. 4.*
- *At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information og personoplysninger lagret på medier - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Bortskaffelse af medier ▶ Databehandleren har udarbejdet og implementeret en procedure for bortskaffelse af medier, hvor der opbevares personoplysninger på forsvarlig vis. ▶ Databehandleren anvender en leverandør til bortskaffelse af medier på forsvarlig vis, herunder medier hvor personoplysninger er opbevaret, som sikrer, at opbevarede personoplysninger ikke kan tilgås.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for bortskaffelse af medier, hvor der opbevares personoplysninger på forsvarlig vis Vi har på forespørgsel fået oplyst, at den leverandør, databehandleren anvendte til bortskaffelse af medier, er gået konkurs grundet COVID19, og at databehandleren finder en ny leverandør, når der er behov for dette. Vi har på forespørgsel fået oplyst, at der ikke har været bortskaffelse, siden underleverandøren gik konkurs, hvorfor vi ikke har kunnet efterprøve proceduren.	Vi har konstateret, at der er etableret en procedure for bortskaffelse af udstyr. Der er ikke bortskaffet udstyr. Vi har derfor ikke kunnet udtale os om kontrollens implementering Ingen afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester - GDPR artikel, 28, stk. 3, litra c.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre uautoriseret adgang til systemer og applikationer - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Brugerregistrering og -afmelding ▶ Databehandleren har implementeret procedure for brugeradministration, der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriserede.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for logiske adgangskontroller hvor det fremgår, at der heri er en forretningsgang for både brugeroprettelser og -nedlæggelser. Vi har inspiceret, at it-chefen godkender brugeroprettelser og-nedlæggelser af medarbejdere (brugeradministrationen). Vi har på forespørgsel fået oplyst, at it-chefen får oplyst mundtligt, når der sker tiltrædelser og fratrædelser.	Ingen afvigelser konstateret.
Tildeling af brugeradgange ▶ Databehandleren har en fortegnelse over brugere med adgang til systemer med personoplysninger. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret en oversigt over brugere hvor det fremgår, at databehandleren har en fortegnelse over brugere i systemet, og at der for hver enkelt bruger fremgår, hvilke systemer den pågældende bruger har adgang til. Vi har inspiceret kontrolarket for it-kontroller hvor det fremgår, at nye medarbejdere tildeles adgang ud fra et arbejdsbetinget behov. Vi har på forespørgsel fået oplyst, at alle administratorer har forskellige logins alt efter hvilken funktion, de skal varetage, samt hvilke systemer de skal tilgå.	Ingen afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester - GDPR artikel, 28, stk. 3, litra c.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre uautoriseret adgang til systemer og applikationer - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Gennemgang af brugeradgangsrettigheder ▶ Der foretages årlig gennemgang af brugere og bruger-rettigheder.	Vi har udført forespørgsel hos passende personale hos databe-handleren. Vi har inspiceret databehandlerens årshjul og observeret, at bru-gere gennemgås årligt i april. Vi har inspiceret, at databehandleren har foretaget den årlige bru-gergennemgang.	Ingen afvigelser konstateret.
Procedure for sikker log-on ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger. ▶ Databehandleren har etableret regler for krav til ad-gangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter. ▶ Databehandlerens medarbejdere tilgår systemer via Awingu ▶ Databehandlerens medarbejdere tilkendegiver via en tro og love-erklæring, at de kun tilgår systemer via en computer med opdateret software.	Vi har udført forespørgsel hos passende personale hos databe-handleren. Vi har inspiceret, databehandlerens password politik og default domain policy. Vi har inspiceret, at databehandleren anvender Awingu, når med-arbejdere skal tilgå systemer. Vi har konstateret, at databehandleren ikke har en tilstrækkelig stærk passwordkrav. Vi har på forespørgsel fået oplyst, databehandleren er i gang med at implementere en ny passwordpolitik Vi har inspiceret procedure for sikkert log-on hvor det fremgår, at medarbejdere skriver under på en tro og love-erklæring på, at de kun tilgår databehandlerens systemer fra PC'ere, der har opdate-ret antivirus software.	Vi har konstateret, at databehandleren ikke har en tilstrækkelig stærk passwordpolitik. Ingen øvrige afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester - GDPR artikel, 28, stk. 3, litra c.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre uautoriseret adgang til systemer og applikationer - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har for den seneste tiltrådte medarbejder observeret at medarbejderen har underskrevet en tro og love-erklæring.	

A.10: Kryptografi

Kontrolmål

- *At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers og personoplysningers fortrolighed, autenticitet og/eller integritet - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik for anvendelse af kryptografi - Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. Politikken definerer styrken og protokollen for kryptering. - Bærbare medier med personoplysninger er krypteret. - Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mails.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret persondatapolitikken hvor det fremgår, at det er databehandlerens politik, at alle arbejdsstationer skal være krypteret, samt at al afsendelse af mail foregår via sikker mail. Vi har på forespørgsel fået oplyst, at samtlige bærbare har installeret Bitlocker, og har på en medarbejders bærbare observeret, at dette er tilfældet. Vi har inspiceret Bitlocker krypteringskoderne. Vi har inspiceret at medarbejderne har deres egen unikke kode. Vi har inspiceret procedure for overførsel, sikker mail mv. hvor det fremgår, at der anvendes Secure Mail til afsendelse af sikker mails, samt at proceduren foreskriver, at databehandlerens Exchange server er standard sat op til at anvende TLS. Vi har inspiceret, at sikker mail er implementeret.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring af, at kun autoriserede personer har adgang. ▶ Alle adgange registreres og logges. ▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at gæster modtages i receptionen og herefter følges hen til, hvor de skal sidde. Vi har inspiceret, at databehandleren har implementeret et låsesystem. Vi har inspiceret, at databehandleren registrerer og logger alle adgange Vi har inspiceret, at fysiske adgange gennemgås årligt.	Ingen afvigelser konstateret.
Fysisk sikkerhed ▶ Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. Den fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav. ▶ Databehandleren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum omfattende følgende forhold: ○ Bygning ○ Gulve ○ Klima ○ Strøm ○ Adgang ○ Alarmmonitorering ○ Brandslukning	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren registrerer og logger alle adgange. Vi har inspiceret, at databehandleren har etableret en branddør til serverrummet. Vi har inspiceret, at der er branddør, Brandalarm, Klimaanlæg og brandudstyr. Vi har på forespørgsel fået oplyst, at serverrummet ligger på 1. sal.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring		
Kontrolmål ▶ *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.* ▶ *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen - GDPR artikel 28, stk. 3, litra c.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
○ Kabling		
Vedligeholdelse af udstyr ▶ Vedligeholdelse af udstyr følger en vedligeholdelsesplan og udføres af autoriseret personale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for reparation og service af it-udstyr hvor det fremgår, at denne indeholder en klar forretningsgang mht. reparation af it-udstyr samt proces for dokumentation af support sager. Vi har inspiceret at vedligeholdelsen varetages af autoriseret personale.	Ingen afvigelser konstateret.
Sikring af udstyr og aktiver for organisationen ▶ Udstyr uden for organisationen må ikke efterlades uden opsyn på offentlige steder. ▶ Adgang til organisationens server fra fjernarbejdspladser, kan kun tilgås via Awingu.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at denne indeholder en politik vedrørende mobilt udstyr. Vi har inspiceret, at der anvendes Awingu til fjernadgang. Vi har på forespørgsel fået oplyst, at underdatabehandler tilgår systemerne via Awingu.	Ingen afvigelser konstateret.
Reparation og service samt bortskaffelse af it-udstyr ▶ Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger. ▶ Databehandleren bortskaffer it-udstyr ved fysisk destruktion af databærende medier.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Vi har fået oplyst, at der ikke er foretaget reparation af it-udstyr. Vi kan derfor ikke udtale os om kontrollens implementering. Vi har fået oplyst, at der ikke er foretaget kassation i nyere tid. Vi kan derfor ikke udtale os om kontrollens implementering.

A.11: Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Databehandleren foretager sikker sletning af data på databærende medier. ▶ Databehandleren fører en oversigt over destrueret it-udstyr.	Vi har inspiceret procedure for reparation og service af IT-udstyr, og har på forespørgsel fået oplyst, at der ikke er foretaget reparation af it-udstyr, hvorfor vi ikke har kunnet efterprøve proceduren. Vi har på forespørgsel fået oplyst, at kasserede medier fra tidligere år opbevares i et separat rum under opsyn, indtil en leverandør er fundet, men at der ikke er foretaget kassation i nyere tid, hvorfor vi ikke har kunnet efterprøve proceduren.	Ingen afvigelser konstateret.
Politik for ryddeligt skrivebord og blank skærm ▶ Skærmlås aktiveres automatisk efter 5 min. ▶ Medarbejdere skal aktivere skærmlås, når klienten forlades. ▶ Fysisk materiale med personoplysninger opbevares i aflåst skab, når materialet forlades. ▶ Fysisk materiale må kun printes med 'follow-me' funktion og fjernes straks fra printeren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret opsætningen af skærmlås hvor det fremgår, at skærmen låser automatisk efter 5 minutter. Vi har inspiceret persondatapolitik hvor det fremgår, at der heri indgår clean desk politik, og at medarbejdere skal låse skærmen, når de forlader deres plads, ligesom fysiske ringbind skal opbevares aflåst udenfor åbningstid. Vi har inspiceret, at print foretages ved brug af follow-me funktion, hvor en medarbejders unikke kort skal anvendes, for at kunne printe.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter - GDPR artikel 25 og artikel 28, stk. 3, litra c.*
- *At sikre, at information og personoplysninger, herunder informations- og databehandlingsfaciliteter er beskyttet mod malware - GDPR artikel 28, stk. 3, litra c.*
- *At beskytte mod tab af data - GDPR artikel 28, stk. 3, litra c.*
- *At registrere hændelser og tilvejebringe bevis - GDPR artikel 33, stk. 2.*
- *At sikre integriteten af driftssystemer - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre, at tekniske sårbarheder udnyttes - GDPR artikel 28, stk. 3, litra c.*
- *At minimere virkningen af auditaktiviteter på driftssystemer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Vedligeholdelse af systemsoftware ▶ Databehandler fører en oversigt over systemsoftware/tredjepartsprogrammer som vedligeholdes og opdateres løbende. ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende. ▶ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret kontrolark for it-kontroller hvor det fremgår, at databehandleren fører en oversigt over systemsoftware og tredjepartsprogrammer som løbende opdateres. Vi har på forespørgsel fået oplyst, at medarbejderne selv er ansvarlige for at holde software opdateret på deres bærbare, men de stationære computere, der står hos databehandleren opdateres automatisk i huset. Vi har for en udvalgt bærbar observeret, at software er opdateret. Vi har inspiceret aftale med Advania hvor det fremgår, , at servere opdateres af Advania, når der er patches til disse. Vi har inspiceret, at medarbejderne i forbindelse med deres ansættelse har underskrevet en tro og love-erklæring på, at de ikke tilgår databehandlerens systemer uden opdateret software/antivirus mv. Vi har inspiceret procedure for opdatering af systemsoftware hvor det fremgår, at databehandleren løbende fører kontrol af, at medarbejdere har opdateret deres software.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter - GDPR artikel 25 og artikel 28, stk. 3, litra c.*
- *At sikre, at information og personoplysninger, herunder informations- og databehandlingsfaciliteter er beskyttet mod malware - GDPR artikel 28, stk. 3, litra c.*
- *At beskytte mod tab af data - GDPR artikel 28, stk. 3, litra c.*
- *At registrere hændelser og tilvejebringe bevis - GDPR artikel 33, stk. 2.*
- *At sikre integriteten af driftssystemer - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre, at tekniske sårbarheder udnyttes - GDPR artikel 28, stk. 3, litra c.*
- *At minimere virkningen af auditaktiviteter på driftssystemer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateres med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret for den seneste tiltrådte medarbejder, at der er installeret antivirus-software. Vi har inspiceret kontrolark for it-kontroller, hvor det fremgår, at databehandleren fører en oversigt over seneste opdatering, og at alle computere er opdateret med seneste antivirus software.	Ingen afvigelser konstateret.
Sikkerhedskopiering og retablering af data ▶ Der foretages dagligt backup af systemer og data. ▶ Drift og opbevaring af backup er outsourcet til underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret it-service aftale indgået med Advania og observeret, at der heraf fremgår, at databehandleren har outsourcet backup af data. Vi har inspiceret indkommende backup log, som modtages hver dag, når backup er fuldført. Vi har på forespørgsel fået oplyst, at databehandleren løbende foretager restore-test. Vi har inspiceret dokumentation for at databehandleren har udført restore-test.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter - GDPR artikel 25 og artikel 28, stk. 3, litra c.*
- *At sikre, at information og personoplysninger, herunder informations- og databehandlingsfaciliteter er beskyttet mod malware - GDPR artikel 28, stk. 3, litra c.*
- *At beskytte mod tab af data - GDPR artikel 28, stk. 3, litra c.*
- *At registrere hændelser og tilvejebringe bevis - GDPR artikel 33, stk. 2.*
- *At sikre integriteten af driftssystemer - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre, at tekniske sårbarheder udnyttes - GDPR artikel 28, stk. 3, litra c.*
- *At minimere virkningen af auditaktiviteter på driftssystemer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges. ▶ Loggen overskrives, når der ikke længere er plads. ▶ Databehandler følger op på alarm-beskeder fra leverandør.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren logger succesfulde og mislykkede adgangsforsøg vha. Windows event log. Vi har på forespørgsel fået oplyst, at loggen ikke slettes efter et fast antal dage, men den ældste logning overskrives, når der ikke er mere plads. Vi har på forespørgsel fået oplyst, at Advania logger oppetid samt kritiske Windows services. Vi har på forespørgsel fået oplyst, at databehandleren ikke har modtaget alarmer fra leverandør og derfor kan vi ikke efterprøve kontrollens implementering.	Vi har konstateret, at databehandleren ikke har modtaget alarmer fra leverandør. Vi kan derfor ikke udtale os om kontrollens implementering. Ingen afvigelser konstateret.

A.13: Kommunikationssikkerhed

Kontrolmål

- *At sikre beskyttelse af informationer og personoplysninger i netværk og af understøttende informationsbehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At opretholde informationssikkerhed og databeskyttelse ved overførsel internt i en organisation og til en ekstern entitet - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Netværkssikkerhed ▶ Netværkstopologien er struktureret efter best-practice principper, hvilket betyder, at servere, som driver applikationer, ikke kan nås direkte fra internettet. ▶ Databehandlerens netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet. ▶ Databehandleren anvender kendte netværksteknologier og mekanismer (Firewall) for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens topologi hvor det fremgår at alle servere er placeret bag en firewall, og således ikke kan nås direkte fra internettet. Vi har desuden inspiceret, at kommunikationen internt hos databehandleren sker vha. MPLS.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall korrekt efter best-practice standard. ▶ Databehandler anvender kun services/porte, som de har behov for. ▶ Firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at Advania er ansvarlig for konfigurationen af firewallen. Vi har inspiceret udtræk af firewall regler og hvor det fremgår, at databehandlerens firewall blokerer alt trafik og kun tillader trafik på de porte, der bliver brugt af systemer i det daglige arbejde i forbindelse med kunder. Vi har på forespørgsel fået oplyst, at Advania overvåger, om der er usædvanlig trafik og kontakter databehandleren, hvis dette er tilfældet. Vi har inspiceret, at LDD modtager besked fra Advania, og at der følges op herpå. Vi har på forespørgsel fået oplyst, at hvis databehandleren lukker eller tilkøber en service, åbnes og lukkes porte ud fra det.	Ingen afvigelser konstateret.

A.13: Kommunikationssikkerhed

Kontrolmål

- *At sikre beskyttelse af informationer og personoplysninger i netværk og af understøttende informationsbehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At opretholde informationssikkerhed og databeskyttelse ved overførsel internt i en organisation og til en ekstern entitet - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Eksterne kommunikationsforbindelser ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og brug af Awingo. ▶ Udveksling af personoplysninger via e-mail, sker vha. sikkermail løsning. ▶ Eksterne kommunikationsforbindelser er krypteret. ▶ Databehandleren har en oversigt over, hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret persondatapolitikken hvor det fremgår at denne indeholder en politik vedrørende mobilt udstyr, herunder at alle arbejdsstationer skal være krypteret, samt at al afsendelse af mail foregår via sikker mail. Vi har inspiceret, at der anvendes Awingu til fjernadgang, samt at firewall kun tillader trafik på specifikke porte. Vi har inspiceret for en medarbejder, at sikker mail er implementeret, og at Bitlocker er installeret. Vi har inspiceret procedure for medarbejderes/leverandørers fjernadgang til servere og systemer med personoplysninger, hvori det fremgår, at oversigt over eksterne kommunikationsforbindelser fremgår.	Ingen afvigelser konstateret.

A.14: Anskaffelse, udvikling og vedligeholdelse

Kontrolmål

- *At sikre, at informationssikkerhed og databeskyttelse er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk - GDPR artikel 25.*
- *At sikre, at informationssikkerhed og databeskyttelse tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus - GDPR artikel 25.*
- *At sikre beskyttelse af data, som anvendes til test - GDPR artikel 25.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Informationssikkerhed i udvikling og ændringer ▶ Databehandler arbejder ud fra security-by-design principper i udviklings- og ændringsopgaver. ▶ Kun databehandlerens udviklere har adgang til kildekode. ▶ Rollback-plan er implementeret i tilfælde af fejl i produktionsmiljøet. ▶ Brugeroprettelse sker som udgangspunkt med laveste brugerrettighedsniveau.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at alt udvikling foregår hos ekstern leverandør, og underdatabehandleraftale er indgået, som således sikrer security-by-design. Vi har inspiceret, at der er indgået databehandleraftale med systemleverandør, således at databeskyttelse er en integreret del af systemernes livscyklus. Det er således kun leverandørens medarbejdere, der har adgang til kildekode. Vi har inspiceret ISAE 3000-erklæringen fra KMD, at der heri under "systemopdatering" anføres, at deres forretningsgange for opdatering af systemsoftware indeholder krav til versionsstyring og kontrolspor for alle ændringer, således at rollback er muligt. Vi har på forespørgsel fået oplyst, at brugere oprettes med laveste brugerrettigheder, herunder at der er få personer, som er oprettet i testmiljøet.	Ingen afvigelser konstateret.
Adskillelse af udviklings-, test og produktionsmiljø ▶ Der er indført funktionsadskillelse mellem udvikling og drift. ▶ Ændringer af funktionalitet testes, inden det sættes i drift. ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. ▶ Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at udvikling i udviklingsmiljø foregår hos ekstern leverandør, og underdatabehandleraftale er indgået. Vi har på forespørgsel fået oplyst, at funktionalitet testes i separat testsystem af LDD, inden det sættes i drift.	Ingen afvigelser konstateret.

A.14: Anskaffelse, udvikling og vedligeholdelse

Kontrolmål

- *At sikre, at informationssikkerhed og databeskyttelse er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk - GDPR artikel 25.*
- *At sikre, at informationssikkerhed og databeskyttelse tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus - GDPR artikel 25.*
- *At sikre beskyttelse af data, som anvendes til test - GDPR artikel 25.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at der er adskillelse af test- og produktionsmiljø. Vi har inspiceret, at der anvendes versionsstyring således, at roll-back er muligt i tilfælde af fejl.	
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes anonymiseret testdata i udviklings- og testmiljø.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at testdata er en kopi af produktionsdata. Disse data ligger ikke på databehandlerens egne servere men på underdatabehandlerens.	Vi har konstateret, at databehandleren ikke anvender anonymiseret testdata i testmiljø. Ingen øvrige afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

- *At sikre beskyttelse af organisationens aktiver og personoplysninger, som leverandører har adgang til - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*
- *At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandlers indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for en databehandleraftale hvor det fremgår, at databehandleren herigennem pålægger deres underdatabehandlere de samme databeskyttelsesforpligtelser, som databehandleren selv er pålagt. Vi har inspiceret en underdatabehandleraftale hvor det fremgår, at underdatabehandler er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er underlagt. Vi har inspiceret en underdatabehandleraftale hvor det fremgår, at instrukser fra den dataansvarlige er videregivet til underdatabehandlerne. Vi har observeret, at underdatabehandleraftaler er underskrevet af parterne og opbevares elektronisk. Vi har inspiceret, at underdatabehandleraftalen indeholder informationer om brugen af underdatabehandlere.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for en databehandleraftale hvori der fremgår, en oversigt over underdatabehandlere. Vi har ved stikprøve inspiceret en databehandleraftale hvor det fremgår, at den indeholder en oversigt over godkendte underdatabehandlere.	Ingen afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

- *At sikre beskyttelse af organisationens aktiver og personoplysninger, som leverandører har adgang til - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*
- *At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Ændringer i godkendte underdatabehandlere ▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere. ▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler. ▶ Dataansvarlig har mulighed for at gøre indsigelse vedr. udskiftning af underdatabehandler. ▶ Ved udskiftning af underdatabehandler skal databehandleren have en ny forudgående specifik skriftlig godkendelse fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at der ikke er udarbejdet formel procesbeskrivelse for udskiftning af underdatabehandlere, men at der udsendes tillæg til databehandleraftaler ved ændringer. Dog står det beskrevet i deres databehandleraftale. Vi har inspiceret databehandlerens skabelon for databehandleraftale og observeret, at den dataansvarlige skal godkende alle underdatabehandlere. Vi har inspiceret databehandlerens databehandleraftale hvor det fremgår, at databehandleren skal kontakte den dataansvarlige ved udskiftning i anvendelsen af underdatabehandlere. Vi har inspiceret databehandlerens databehandleraftale hvor det fremgår, at den dataansvarlige kan gøre indsigelse ved databehandlerens udskiftning af underdatabehandlere. Vi har inspiceret databehandlerens databehandleraftale hvor det fremgår, at databehandleren skal have en specifik godkendelse fra den dataansvarlige forud for udskiftningen af underdatabehandlere.	Ingen afvigelser konstateret.
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. ▶ Oversigt over godkendte underdatabehandlere indeholder navn, cvr, adresse og beskrivelse af behandling, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon for en databehandleraftale hvor der fremgår, oversigt over underdatabehandlere. Vi har inspiceret en databehandleraftale hvor det fremgår, at den indeholder en oversigt over godkendte underdatabehandlere.	Ingen afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

- *At sikre beskyttelse af organisationens aktiver og personoplysninger, som leverandører har adgang til - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*
- *At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandler udfører tilsyn af underdatabehandleren baseret på en risikovurdering ▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for tilsyn med underdatabehandlere hvor det fremgår, at der ud fra en risikobaseret tilgang udføres årligt tilsyn med underdatabehandlere ved indhentning og gennemgang af revisionserklæring mv. Vi har inspiceret databehandlerens årshjul hvor det fremgår, at der bliver foretaget tilsyn med underdatabehandlerne årligt i april. Vi har inspiceret dokumentation for det udførte tilsyn herunder stillingtagen til modtagne revisorerklæringer mv.	Ingen afvigelser konstateret.

A.16: Styring af informationssikkerhedsbrud

Kontrolmål

- *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud og brud på persondatasikkerheden, herunder kommunikation om sikkerhedshændelser og –svagheder - GDPR artikel 33, stk. 2.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Ansvar og procedurer ▶ Der er fastlagt ledelsesansvar og roller i forbindelse med brud på persondatasikkerheden. ▶ Databehandleren har implementeret procedure for brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik, som indeholder en sikkerhedsbrudsprocedure, hvor ansvar og handlingsplan er beskrevet. Vi har inspiceret, at selve håndteringen af databehandlerens procedure varetages af et internt udvalgt responshold, hvis primære opgave er at håndtere potentielle sikkerhedsbrud på et operationelt niveau. Vi har inspiceret databehandlerens persondatapolitik, som indeholder en sikkerhedsbrudsprocedure. Af sikkerhedsbrudsproceduren fremgår en handlingsplan, der viser samtlige aktiviteter der iværksættes, hvis der er identificeret et brud eller mistanke herom. Vi har inspiceret en oversigt over sikkerhedsbrud. Vi har inspiceret det seneste sikkerhedsbrud, hvor det fremgår at databehandleren har fulgt deres procedure.	Ingen afvigelser konstateret.
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og den dataansvarlige dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databehandleraftale hvor det fremgår, at databehandleren er forpligtet til at underrette den dataansvarlige om brud på persondatasikkerheden skal om muligt straks ellers uden unødig forsinkelse. Vi har inspiceret databehandlerens sikkerhedsbrudsprocedure hvor det fremgår, at databehandleren har etableret en proces, der sikrer rettidig underretning.	Ingen afvigelser konstateret.

A.16: Styring af informationssikkerhedsbrud

Kontrolmål

- *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud og brud på persondatasikkerheden, herunder kommunikation om sikkerhedshændelser og –svagheder - GDPR artikel 33, stk. 2.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret en oversigt over sikkerhedsbrud. Vi har inspiceret det seneste sikkerhedsbrud, hvor det fremgår at databehandleren har fulgt deres procedure.	
Identifikation af brud på persondatasikkerheden - Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedsbrudsprocedure hvor det fremgår, at der er udarbejdet en handlingsplan for håndteringen af brud på persondatasikkerheden samt identificering af potentielle brud. Vi har inspiceret referat af personalemøde, hvoraf fremgår, at tidligere hændelser og læring heraf er drøftet til sikring af løbende awareness af medarbejdere.	Ingen afvigelser konstateret.
Registrering af brud på persondatasikkerheden - Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen. - Databehandleren har udarbejdet og implementeret en procedure for erfaringsopsamling ved brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedsbrudslog hvor det fremgår, at databehandleren registrerer brud på persondatasikkerheden. Vi har inspiceret, at underretning er foretaget i henhold til proceduren. Vi har inspiceret databehandlerens sikkerhedsbrudsprocedure hvor det fremgår, at proceduren indeholder en handlingsplan, hvor databehandleren til sidst vurderer læringen af bruddet.	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige - Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. - Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. - Ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, anvender databehandleren en tjekliste, som fastlægger, hvad databehandleren kan leve op til. - Databehandleraftaler underskrives og opbevares elektronisk. - Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at databehandleren har en procedure for indgåelse af databehandleraftaler. Vi har inspiceret databehandleraftale skabelon, som databehandleren har udfærdiget som brancheorganisation. Vi har inspiceret at databehandleren herigennem sikrer efterlevelse af databeskyttelseslovgivningens pligter for henholdsvis kunden, som dataansvarlig samt databehandleren. Vi har på forespørgsel fået oplyst at databehandleraftale skabelonen fungerer som en standard, og indeholder de bestemmelser, som databehandleren skal leve op til. Vi har inspiceret, at databehandleraftalerne opbevares elektronisk. Vi har ved gennemført stikprøve observeret, at databehandleraftalen er underskrevet. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår at aftalen indeholder et bilag B med en liste over underdatabehandlere. Vi har inspiceret, at der er overensstemmelse mellem bilag B i standardskabelonen og tillæg til databehandleraftaler.	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Instruks for behandling af personoplysninger ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret den seneste indgåede databehandleraftale med den dataansvarlige hvor det fremgår, at denne indeholder en instruks fra den dataansvarlige om, at databehandleren ikke må behandle personoplysninger til egne formål.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra den dataansvarlige. ▶ Databehandlerens procedurer gennemgås og opdateres løbende og minimum en gang årligt. ▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at databehandleren udelukkende må behandle personoplysninger efter den dataansvarliges instruks. Vi har inspiceret, at databehandleren har anvendt deres databehandlerskabelon på den seneste indgåede databehandleraftale. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at databehandleren har udarbejdet relevante procedurer, der sikrer, at personoplysninger alene behandles efter instruks fra den dataansvarlige. Vi har Inspiceret, at databehandleren gennemgår og opdaterer procedurer løbende. Vi har modtaget og inspiceret databehandlerens log over ajourføring af persondatapolitikken, hvor det fremgår, at den er opdateret i april 2024.	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at databehandleren gennemgår og opdaterer sine procedurer løbende og minimum en gang årligt for at sikre, at databehandleren til stadighed behandler personoplysninger i overensstemmelse med den dataansvarliges instruks.	
Underretning af den dataansvarlige ved ulovlig instruks - Databehandleren har udarbejdet en procedure for underretning af den dataansvarlige i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen. - Databehandleren underretter straks den dataansvarlige i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at databehandleren har en procedure for vurdering om behandling beror på lovligt grundlag, og underretning til den dataansvarlige, hvis instruksen strider imod databeskyttelseslovgivningen. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at databehandleren omgående skal underrette den dataansvarlige, hvis en instruks er i strid med databeskyttelseslovgivningen. Vi har inspiceret, at databehandleren har anvendt deres databehandlerskabelon på den seneste indgåede databehandleraftale. Vi har ved forespørgsel fået oplyst, at der ikke har været tilfælde, hvor instruks stred imod databeskyttelseslovgivningen, hvorfor det ikke har været muligt at efterprøve kontrollen.	Vi har konstateret, at der ikke har været tilfælde, hvor instruks stred imod databeskyttelseslovgivningen. Vi har derfor ikke kunnet udtale os om kontrollens implementering. Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
De registreredes rettigheder ▶ Databehandler har udarbejdet en procedure for bistand til den dataansvarlige ved opfyldelse af de registreredes rettigheder. ▶ Det er muligt at give indsigt i alle oplysninger, der er registreret i C5 + KMD-lønsystem.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at der heri er anført, at databehandleren er forpligtet til at bistå den dataansvarlige. Vi har inspiceret, at databehandleren har anvendt deres databehandlerskabelon på den seneste indgået databehandleraftale. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at databehandleren har en procedure for håndteringen af bistand til den dataansvarlige ved opfyldelse af de registreredes rettigheder. Vi har ved forespørgsel fået oplyst, at der ikke har været anmodninger om indsigt det seneste år, hvorfor det ikke har været muligt at efterprøve kontrollen.	Vi har konstateret, at databehandleren ikke har haft anmodninger om indsigt. Vi har derfor ikke kunnet udtale os om kontrollens implementering Ingen afvigelser konstateret.
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at der findes procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Revision og inspektion ▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandler bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at databehandleren herigennem forpligter sig til årligt at fremsende dokumentation for, at sikkerhedsforanstaltningerne er truffet, og at der føres tilsyn med, at de overholdes. Dette skal ske i form af en revisionserklæring udarbejdet af en uafhængig tredjemand. Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at databehandleren herigennem forpligter sig til at bistå den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at databehandleren herigennem forpligter sig til at stille den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden i forbindelse med revision og inspektion af databehandleraftalen. Vi har inspiceret, at databehandleren har anvendt deres databehandlerskabelon på den seneste indgået databehandleraftale.	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at databehandleren efter den dataansvarliges skriftlige anvisninger skal slette data eller informationer af enhver art. Vi har inspiceret, at databehandleren har anvendt deres databehandlerskabelon på den seneste indgået databehandleraftale. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at databehandleren har fastsat generelle slettefrister, der er udfærdiget på baggrund af en række lovbestemte frister. Vi har på forespørgsel fået oplyst, at der ikke har været anmodninger om sletning, hvorfor vi ikke har kontrolleret databehandlerens sletteprocedure yderligere.	Vi har konstateret, at databehandleren ikke har haft anmodninger om sletning. Vi har derfor ikke kunnet udtale os om kontrollens implementering Ingen afvigelser konstateret.
Tilbagelevering af personoplysninger ▶ Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen. ▶ Dataansvarlig og databehandler har aftalt i hvilket format, overførelse og medie, data skal tilbageleveres, når det anmodes af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at der heri er anført, at databehandleren på den dataansvarliges anmodning kan tilbagelevere personoplysninger. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale at der heri er anført, at tilbagelevering skal ske til den dataansvarlige og/eller til en af den dataansvarlige udpeget tredjemand i et læsbart format.	Vi har konstateret, at databehandleren ikke har haft anmodninger om tilbagelevering. Vi har derfor ikke kunnet udtale os om kontrollens implementering. Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at databehandleren har anvendt deres databehandlerskabelon på den seneste indgået databehandleraftale. Vi har på forespørgsel fået oplyst, at der ikke har været anmodninger om tilbagelevering, hvorfor vi ikke har kontrolleret databehandlerens procedure yderligere.	
Overførsel af personoplysninger til tredjelande - Der foreligger skriftlige procedurer for overførsel af personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at databehandler heri af opsat procedure for overførsel af personoplysninger til tredjeland, herunder, at der alene vil ske fremsendelse af personoplysninger til databehandleren, der befinder sig i et tredjeland, såfremt Kommissionen forinden har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, såfremt de fornødne eller passende garantier i øvrigt er garanteret ved eksempelvis bindende virksomhedsregler, der er samtykket til fremsendelsen, eller såfremt det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som organisationen er underlagt. Vi har inspiceret databehandlerens oversigt over underdatabehandlere hvor det fremgår, at databehandleren anvender underdatabehandlere, der er reguleret af amerikansk lovgivning, og at der derved kan ske en utilsigtet overførsel til tredjelande. Det drejer sig om underdatabehandleren Microsoft. Vi har inspiceret at databehandlerens udarbejdede TIA-analyser (Transfer Impact Assessment) for amerikanske underdatabehandlere i forbindelse med EDPB's (European Data Protection Board) hvor databehandlerens beskyttelsesniveau på overførsel af personoplysninger til tredjelande fremgår.	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at Microsoft har en aktiv certificering og dermed har databehandleren et gyldigt overførselsgrundlag for at overføre dataansvarliges personoplysninger til underbehandleren Microsoft.	
Instruks fra den dataansvarlige - Databehandleren overfører kun personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige. - Databehandleren dokumenterer indhentet instruks vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer fra dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standardskabelon for en databehandleraftale hvor det fremgår, at der i instruksen er anført, at den dataansvarlige godkender, at databehandler i det omfang det er nødvendigt for opfyldelse af parternes hovedaftale anvender underdatabehandlere, samt at underdatabehandler anvender underdatabehandlere, der kan medføre overførsel af personoplysninger til tredjelande.	Ingen afvigelser konstateret.
Gyldigt overførselsgrundlag - Databehandleren vurderer og dokumenterer, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens persondatapolitik hvor det fremgår, at databehandler heri har opsat procedure for overførsel af personoplysninger til tredjeland, herunder, at der alene vil ske fremsendelse af personoplysninger til dets databehandlere, der befinder sig i et tredjeland, såfremt Kommissionen forinden har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, såfremt de fornødne eller passende garantier i øvrigt er garante-	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	ret ved eksempelvis bindende virksomhedsregler, der er samtykket til fremsendelsen, eller såfremt det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som organisationen er underlagt. Vi har inspiceret databehandlerens oversigt over underdatabehandlere hvor det fremgår, at databehandleren anvender underdatabehandlere, der er reguleret af amerikansk lovgivning, og at der derved kan ske en utilsigtet overførsel til tredjelande. Det drejer sig om underdatabehandleren Microsoft. Vi har inspiceret at databehandlerens udarbejdede TIA-analyser (Transfer Impact Assessment) for amerikanske underdatabehandlere i forbindelse med EDPB's (European Data Protection Board) hvor databehandlerens beskyttelsesniveau på overførsel af personoplysninger til tredjelande fremgår. Vi har inspiceret, at Microsoft har en aktiv certificering og dermed har databehandleren et gyldigt overførselsgrundlag for at overføre dataansvarliges personoplysninger til underbehandleren Microsoft.	
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurderer og evaluerer effektiviteten af, om de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedsbrudsprocedure hvor det fremgår at databehandleren på baggrund af erfaringsopsamlingen i forbindelse med hændelser vedrørende brud på persondatasikkerheden vil vurdere, hvorvidt det er nødvendigt med yderligere sikkerhedstiltag eller opdateringer/ændringer af politikker og procedurer. Oplæring af personale kan også blive relevant.	Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret databehandlerens procedure for afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger. Vi har inspiceret, at databehandleren har afprøvet, vurderet og evalueret af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. De data som varetages på vegne af dataansvarlig i november som stemmer overens med databehandlerens årshjul.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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

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

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-07-04 08:03:00 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner, chef for Risk Assurance, CISA, CRISC
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 62.66.xxx.xxx
2024-07-04 08:52:51 UTC

Palle Woss
Direktør
Serienummer: 2ca56959-4b28-4a3f-b6f3-fd13715b7c56
IP: 93.176.xxx.xxx
2024-07-05 12:50:10 UTC

Penneo dokumentnøgle: 571EM-PDXJF-OGH4L-B6CFH-OTGQO-EBWOU