

**AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING
MED SIKKERHED PR. 1. JUNI 2025 OM BESKRIVELSE AF DATA-
BEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER I ADMI-
NISTRATIONEN AF DAGSINSTITUTIONER OG DE TILHØRENDE
TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALT-
NINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING,
RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOP-
LYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNIN-
GEN OG DATABESKYTTELSESLOVEN**

**Landsorganisationen Danske Dagin-
stitutioner**

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING	2
2. LANDSORGANISATIONEN DANSKE DAGINSTITUTIONERS UDTALELSE	5
3. LANDSORGANISATIONEN DANSKE DAGINSTITUTIONERS BESKRIVELSE AF BEHANDLING AF PERSONOPLYSNINGER I ADMINISTRATIONEN AF DAGINSTITUTIONER	7
Landsorganisationen Danske Daginstitutioner	7
Administrationen af daginstitutioner og behandling af personoplysninger.....	7
Styring af persondatasikkerhed.....	7
Risikovurdering.....	9
Tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller	9
4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST	14
Risikovurdering.....	16
A.5: Informationssikkerhedspolitikker.....	17
A.7: Personalesikkerhed	18
A.8: Styring af aktiver	20
A.9: Adgangsstyring.....	21
A.10: Kryptografi	23
A.11: Fysisk sikring og miljøsikring	24
A.12: Driftssikkerhed	25
A.13: Kommunikationssikkerhed.....	26
A.15: Leverandørforhold.....	27
A.16: Styring af informationssikkerhedsbrud.....	29
A.18: Overensstemmelse	32
5. SUPPLERENDE INFORMATION FRA LANDSORGANISATIONEN DANSKE DAGINSTITUTIONER	37

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 1. JUNI 2025 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 2025 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.

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 revisors 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 revisionspartnerselskab 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 2025, 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 2025.

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 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 15. august 2025

BDO Statsautoriseret revisionspartnerselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. LANDSORGANISATIONEN DANSKE DAGINSTITUTIONERS 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 i sektion 3 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 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for databehandlerens 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 vigtig 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 2025. 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 databehandleriskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Allerød, den 15. august 2025

Landsorganisationen Danske Daginstitutioner

Palle Woss
Direktør

3. LANDSORGANISATIONEN DANSKE DAGINSTITUTIONERS 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 private og 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. Der behandles personoplysninger, der henføres under databeskyttelsesforordningens artikel 9, herunder helbredsoplysning, samt CPR-nr, jf. DBL § 11 og strafbare forhold, jf. DBL § 8.

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	<ul style="list-style-type: none"> Risikovurdering 	<ul style="list-style-type: none"> Artikel 28, stk. 3, litra c
A.5: Informationssikkerhedspolitikker	<ul style="list-style-type: none"> Politikker for informationssikkerhed og databeskyttelse Gennemgang af persondatapolitik herunder tekniske sikkerhedsforanstaltninger 	<ul style="list-style-type: none"> Artikel 28, stk. 1
A.6: Organisering af informationssikkerhed	<ul style="list-style-type: none"> Roller og ansvarsområder Politik for mobilt udstyr Fjernarbejdspladser og fjernadgang til systemer og data 	<ul style="list-style-type: none"> Artikel 28, stk. 1 Artikel 28, stk. 3, litra c

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
A.7: Personalesikkerhed	<ul style="list-style-type: none"> • Rekruttering af medarbejdere • Uddannelse og instruktion af medarbejdere, der behandler personoplysninger • Tavsheds- og fortrolighedsaftale med medarbejdere og eksterne leverandører og konsulenter • Fratrædelse af medarbejdere 	<ul style="list-style-type: none"> • Artikel 28, stk. 1 • Artikel 28, stk. 3, litra b
A.8: Styring af aktiver	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Brugerregistrering og -afmelding • Tildeling af brugeradgange • Gennemgang af brugeradgangsrettigheder • Procedure for sikker log-on 	• Artikel 28, stk. 3, litra c
A.10: Kryptografi	<ul style="list-style-type: none"> • Politik for anvendelse af kryptografi 	• Artikel 28, stk. 3, litra c
A.11: Fysisk sikring og miljøsikring	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Vedligeholdelse af systemsoftware • Antivirusprogram 	• Artikel 28, stk. 3, litra c
A.13: Kommunikationssikkerhed	<ul style="list-style-type: none"> • Eksterne kommunikationsforbindelser 	• Artikel 28, stk. 3, litra c
A.14: Anskaffelse, udvikling og vedligeholdelse	<ul style="list-style-type: none"> • Analyse og specifikation af informationssikkerhedskrav 	• Artikel 25
A.15: Leverandørforhold	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 • Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger 	<ul style="list-style-type: none"> • 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

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 SystemConnect og Azets Perspektiv A/S, som underdatabehandlere, ligesom IT services herunder hosting, backup, patch management samt overvågning af virtuelle servere og firewall 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 på baggrund af stillingsopslag og modtagne ansøgninger 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 lpad, 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 er blandt andet oplæring af nyansatte og 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 destruktionsen 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 outsourcet sikkerhedskopiering og retablering af data til Advania Danmark A/S.

Logning i systemer, databaser og netværk

LDD har outsourcet netværkskonfiguration, overvågning af netværk og firewall samt logning på netværk til Advania

A.13: Kommunikationssikkerhed

Netværkssikkerhed

LDD har outsourcet netværkskonfiguration, overvågning af netværk og firewall til Advania Danmark A/S.

Firewall

LDD har indført procedurer, der via underdatabehandler Advania Danmark A/S 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. Advania Danmark A/S overvåger og konfigurerer firewallen.

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 Azets Perspektiv, Advania og SystemConnect

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 unødigt 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 udgangspunkt 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 Daginstitutioner 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 2025.

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 implementeret, 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. januar til 30. november 2024. 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 2023 til 31. maj 2024. Herudover anvendes Microsoft Office 365 i administrationen hvorfra vi har modtaget SOC 2 erklæring for perioden 1. oktober 2023 til 30. september 2024.

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 ► <i>At sikre, at databehandleren udfører en årlig risikovurdering i forhold til konsekvenserne for de registrerede, der danner grundlag for de tekniske og organisatoriske sikkerhedsforanstaltninger.</i>		
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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har foretaget en risikovurdering baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder. Vi har inspiceret, at den foretagne risikovurdering er opdateret og godkendt.	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 gennemgang af politikker for informationssikkerhed ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere. Vi har inspiceret, at procedurer er opdateret og godkendt.	Ingen afvigelser konstateret
Informationssikkerhedspolitikker i overensstemmelse med databehandleraftaler ▶ Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret ved en stikprøve på databehandleraftaler, at kravene i aftalerne ikke er modstridende med informationssikkerhedspolitikken.	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. ▶ At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar – GDPR, artikel 28, stk. 1. ▶ 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 - Screening ▶ Databehandleren udfører screening og baggrundstjek af alle 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, at der foreligger formaliserede procedurer, der sikrer udførelse af screening og baggrundstjek af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har for den seneste ansatte inspiceret, at databehandleren har udført efterprøvning af kandidaten, og at efterprøvningen har omfattet relevant dokumentation.	Ingen afvigelser konstateret.
Rekruttering af medarbejdere - Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Ved ansættelse underskriver medarbejdere en fortrolighedsaftale eller på anden måde har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for den seneste ansatte inspiceret, at den pågældende medarbejder har underskrevet krav til tavshedspligt i ansættelseskontrakten.	Ingen afvigelser konstateret.
Awareness, uddannelse og træning vedrørende informationsikkerhed ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. ▶ Databehandleren foretager løbende awareness, træning og uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger.	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. ▶ At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar – GDPR, artikel 28, stk. 1. ▶ 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
	Vi har inspiceret, at databehandleren foretager løbende awareness, træning og uddannelse af medarbejdere omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte uddannelse.	
Fratrædelse af medarbejdere - oplysning om fortrolighed og tavshedspligt ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for seneste fratrådte medarbejder inspiceret, at databehandleren har orienteret den fratrådte medarbejder om, at den pålagte tavshedspligt fortsat er gældende efter ansættelsesophør.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere - inddragelse af adgangsrettigheder og aktiver ▶ Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Vi har for den seneste fratrådte medarbejder inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget rettidigt.	Ingen afvigelser konstateret.

A.8: Styring af aktiver		
Kontrolmål ▶ <i>At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf – GDPR, artikel 30, stk. 2, 3 og 4.</i> ▶ <i>At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information og personoplysninger lagret på medier – GDPR, artikel 28, stk. 3, litra c.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Fortegnelse over kategorier af behandlingsaktiviteter <ul style="list-style-type: none"> ▶ Databehandleren har etableret en fortegnelse over kategorier af behandlingsaktiviteter som databehandler. Fortegnelsen skal indeholde: <ul style="list-style-type: none"> - navn og kontaktoplysninger for dataansvarlige, - de kategorier af behandling, der foretages på vegne af dataansvarlige, - navn og kontaktoplysninger for hver underdatabehandler, - angivelse af eventuel overførsel af personoplysninger til et tredjeland. ▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev. ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandlerens fortegnelse over kategorier af behandlingsaktiviteter som databehandler og observeret, at den, indeholder relevante oplysninger, samt at fortegnelsen bliver opbevaret elektronisk.</p> <p>Vi har inspiceret, at fortegnelsen er opdateret og/eller godkendt.</p> <p>Vi har på forespørgsel blevet oplyst, at Datatilsynet ikke har anmodet om udlevering af fortegnelsen.</p>	<p>Vi har konstateret, at Datatilsynet ikke ved erklæringstidspunktet har anmodet om udlevering af fortegnelsen. Vi har derfor ikke kunnet teste implementering af denne del af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>
Reparation-, service- og destruktion af it-udstyr <ul style="list-style-type: none"> ▶ Databehandleren har etableret en procedure for reparation-, service- og destruktion af it-udstyr, der sikrer sikker håndtering af it-udstyr indeholdende personoplysninger. ▶ Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger. ▶ Databehandleren bortskaffer it-udstyr ved fysisk destruktion af databærende medier eller foretager sikker sletning af data på databærende medier. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har formaliserede procedurer for reparation-, service- og destruktion af it-udstyr.</p> <p>Vi har på forespørgsel fået oplyst, at der ikke har været sendt it-udstyr til reparation-, service- eller destruktion.</p>	<p>Vi har konstateret, at databehandleren ikke har sendt it-udstyr til reparation-, service- eller destruktion. Vi har derfor ikke kunnet teste implementering af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

A.9: Adgangsstyring		
<p>Kontrolmål</p> <ul style="list-style-type: none"> ▶ <i>At begrænse adgangen til information og personoplysninger, herunder informations- og databehandlingsfaciliteter – GDPR, artikel 28, stk. 3, litra c.</i> ▶ <i>At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester – GDPR, artikel, 28, stk. 3, litra c.</i> ▶ <i>At gøre brugere ansvarlige for at sikre deres autentifikationsinformation – GDPR, artikel 28, stk. 3, litra c.</i> ▶ <i>At forhindre uautoriseret adgang til systemer og applikationer – GDPR, artikel 28, stk. 3, litra c.</i> 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Brugerregistrering og -afmelding og gennemgang af adgangsrettigheder</p> <ul style="list-style-type: none"> ▶ Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret og sker ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildelles til systemer og enheder ud fra arbejdsbetinget behov. ▶ Brugerens adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for tildelelse og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Vi har for seneste ansatte medarbejder inspiceret, at medarbejderens adgang til systemer, hvor der behandles personoplysninger, er godkendt, og at medarbejderen har et arbejdsbetinget behov for adgangen.</p> <p>Vi har for seneste fratrådte medarbejder inspiceret, at den fratrådtes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.</p> <p>Vi har inspiceret databehandlerens årshjul / procedure for brugerstyring, og observeret, at databehandleren regelmæssigt skal vurdere og godkende tildelte brugeradgange.</p> <p>Vi har inspiceret, at databehandleren har foretaget vurdering og godkendelse af brugeradgange.</p>	<p>Vi har på forespørgsel fået oplyst, at der ikke er blevet tildelt privilegerede adgangsrettigheder siden afgivelse af sidste erklæring. Vi har derfor ikke kunnet teste implementering af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>
<p>Brug af hemmelig autentifikationsinformation</p> <ul style="list-style-type: none"> ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger sker gennem adgangskoder, der afspejler risikoen ved behandlingsaktiviteten.</p>	<p>Ingen afvigelser konstateret.</p>

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
<p>Procedure for sikkert log-on</p> <ul style="list-style-type: none"> ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder anvendelsen to-faktor autentifikation.</p>	<p>Vi har konstateret, at databehandleren ikke har en tidssvarende passwordpolitik.</p> <p>Ingen yderligere afvigelser konstateret</p>

A.10: Kryptografi		
Kontrolmål ► <i>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.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Kryptering ved transmission personoplysninger ► Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring		
Kontrolmål ► <i>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.</i>		
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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til databehandlerens lokaler. Vi har inspiceret dokumentation for, at kun autoriserede personer har fysisk adgang til lokaler, hvori der opbevares og behandles personoplysninger.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed		
<p>Kontrolmål</p> <ul style="list-style-type: none"> ▶ <i>At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter – GDPR, artikel 28, stk. 3, litra c.</i> ▶ <i>At sikre, at information og personoplysninger, herunder informations- og databehandlingsfaciliteter er beskyttet mod malware – GDPR, artikel 28, stk. 3, litra c.</i> ▶ <i>At beskytte mod tab af data – GDPR, artikel 28, stk. 3, litra c.</i> ▶ <i>At registrere hændelser og tilvejebringe bevis – GDPR, artikel 28, stk. 3, litra c.</i> ▶ <i>At sikre integriteten af driftssystemer – GDPR, artikel 28, stk. 3, litra c.</i> ▶ <i>At forhindre, at tekniske sårbarheder udnyttes – GDPR, artikel 28, stk. 3, litra c.</i> 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Vedligeholdelse af systemsoftware</p> <ul style="list-style-type: none"> ▶ Ændringer til systemer, arbejdsstationer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret ved udtræk, at databaser og netværk er opdateret med relevante opdateringer og sikkerhedspatches.</p> <p>Vi har stikprøvevis inspiceret, at en arbejdsstation er opdateret med nyeste systemopdatering.</p>	<p>Ingen afvigelser konstateret.</p>
<p>Antivirusprogram</p> <ul style="list-style-type: none"> ▶ Der er for de arbejdsstationer og systemer, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har for én tilfældig udvalgt pc, der anvendes til behandling af personoplysninger, inspiceret, at der er installeret antivirus, som er opdateret.</p>	<p>Ingen afvigelser konstateret.</p>

A.13: Kommunikationssikkerhed		
Kontrolmål ▶ At sikre beskyttelse af informationer og personoplysninger i netværk og af understøttende informationsbehandlingsfaciliteter – GDPR, artikel 28, stk. 3, litra c.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Netværkssikkerhed ▶ Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværkstopologi og observeret, at netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Vi har inspiceret dokumentation for, at databehandlerens netværk er opsat i overensstemmelse med netværkstopologien.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall korrekt efter best-practice standard. ▶ Databehandler anvender kun services/porte, som de har behov for.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem firewall. Vi har inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen afvigelser konstateret.
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og brug af Awingo.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværkstopologi og observeret, at der kun kan opnås fjernadgang til systemer og data via Awingo, samt at firewall kun tillader trafik på specifikke porte. Vi har inspiceret dokumentation for, at databehandlerens netværk er opsat i overensstemmelse med netværkstopologien. Vi har observeret at, fjernadgang til systemer og data sker via tofaktor autentifikation.	Ingen afvigelser konstateret.

A.15: Leverandørforhold		
Kontrolmål		
<ul style="list-style-type: none"> ▶ At sikre beskyttelse af organisationens aktiver og personoplysninger, som leverandører har adgang til – GDPR, artikel 28, stk. 2 og 4. ▶ At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne – GDPR, artikel 28, stk. 2 og 4. 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks <ul style="list-style-type: none"> ▶ Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Vi har inspiceret, at procedurerne er opdateret og godkendt.</p>	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere <ul style="list-style-type: none"> ▶ Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere.</p> <p>Vi har inspiceret ved en stikprøve på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af seneste indgåede databehandleraftale med en dataansvarlig.</p>	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere <ul style="list-style-type: none"> ▶ Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.</p>	<p>Vi har konstateret, at der ikke er sket ændringer af underdatabehandlere. Vi har derfor ikke kunnet teste kontrollens implementering.</p> <p>Ingen afvigelser konstateret.</p>

A.15: Leverandørforhold		
Kontrolmål ► At sikre beskyttelse af organisationens aktiver og personoplysninger, som leverandører har adgang til – GDPR, artikel 28, stk. 2 og 4. ► At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne – GDPR, artikel 28, stk. 2 og 4.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlere i overensstemmelse med indgåede databehandleraftaler. Vi har på forespørgsel fået oplyst, at der ikke er sket ændringer af underdatabehandlere.	
Underdatabehandlerens forpligtelser ► Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er indgået databehandleraftaler med anvendte underdatabehandlere, Vi har inspiceret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
Oversigt over underdatabehandlere ► Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: <ul style="list-style-type: none"> ○ Navn ○ CVR-nr. ○ Adresse ○ Beskrivelse af behandlingen. 	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Vi har inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ► Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.	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 og 4. ► At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne – GDPR, artikel 28, stk. 2 og 4.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at databehandleren har udført tilsyn, herunder indhentet og gennemgået underdatabehandlers revisorerklæringer, certificeringer og lignende. Vi har inspiceret, at databehandlerens tilsyn af underdatabehandlere ikke har givet anledning til yderligere handlinger.	

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
Underretning om brud på persondatasikkerheden ► Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. ► Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret og godkendt. Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.	Ingen afvigelser konstateret.
Rettidig underretning om brud på persondatasikkerhed ► Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødigt forsinkelse.	Vi har udført forespørgsel hos passende personale hos databehandleren.	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, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødigt forsinkelse og senest 15 minutter efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	
Identifikation af brud på persondatasikkerheden ► Databehandleren har opsat foranstaltninger til at identificere brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
Bistand til dataansvarlige ved brud på persondatasikkerhed ► Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: <ul style="list-style-type: none"> ○ Karakteren af bruddet på persondatasikkerheden ○ Sandsynlige konsekvenser af bruddet på persondatasikkerheden ○ Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: <ul style="list-style-type: none"> • Kontaktoplysningerne for organisationens responshold, hvor yderligere oplysninger kan hentes. • Beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden. • Beskrivelse af foranstaltninger, som responsholdet på vegne af LDD har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden. 	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 dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	

A.18: Overensstemmelse		
Kontrolmål		
▶ <i>At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Procedure for behandling af personoplysninger <ul style="list-style-type: none"> ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger en formaliseret procedure, der skal sikre, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Vi blevet oplyst, at der minimum årlig foretages vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Vi har inspiceret, at proceduren er opdateret og ledelsesgodkendt.</p>	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger <ul style="list-style-type: none"> ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret den seneste indgåede databehandleraftale med en dataansvarlig og observeret, at aftalen indeholder instrukser fra dataansvarlig.</p> <p>Vi har inspiceret databehandlerens fortegnelse over behandlingsaktiviteter og ved en stikprøve inspiceret, at behandlingen foregår i overensstemmelse med instruks fra dataansvarlig.</p>	Ingen afvigelser konstateret.
Aftalte sikringsforanstaltninger <ul style="list-style-type: none"> ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Vi har inspiceret, at procedurer er opdateret og godkendt.</p>	Ingen afvigelser konstateret.

A.18: Overensstemmelse		
Kontrolmål ▶ At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivning.	Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde, hvor instruks har været vurderet i strid med lovgivning.	Vi har konstateret, at der ikke har været tilfælde, hvor instruks har været vurderet i strid med lovgivning. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.
Procedure for opfyldelse af registreredes rettigheder ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdateret og godkendt.	Ingen afvigelser konstateret.
Tekniske foranstaltninger til opfyldelse af registreredes rettigheder ▶ Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: <ul style="list-style-type: none"> • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har inspiceret dokumentation for, at de anvendte systemer understøtter gennemførelsen af de nævnte detaljerede procedurer. Vi har på forespørgsel fået oplyst, at der ikke er sket anmodning om bistand i forhold til de registreredes rettigheder.	Vi har konstateret, at der ikke er sket anmodning om bistand i forhold til de registreredes rettigheder. Vi har derfor ikke kunne teste kontrollens implementering Ingen afvigelser konstateret.

A.18: Overensstemmelse		
Kontrolmål		
<p>▶ At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.</p>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Sletning af oplysninger i overensstemmelse med dataansvarliges krav</p> <ul style="list-style-type: none"> ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Vi har inspiceret, at procedurerne er opdateret og godkendt.</p>	<p>Ingen afvigelser konstateret.</p>
<p>Sletning og tilbagelevering ved ophør af kundeforhold</p> <ul style="list-style-type: none"> ▶ Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: <ul style="list-style-type: none"> ○ Tilbageleveret til den dataansvarlige og/eller ○ Slettet, hvor det ikke er i modstrid med anden lovgivning. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for tilbagelevering og/eller sletning af den dataansvarliges data ved ophør af behandling af personoplysninger.</p> <p>Vi har på forespørgsel fået oplyst, at der individuelt aftales med kunden, hvordan behandlingen afvikles.</p> <p>Vi har for seneste ophørte databehandling inspiceret, at den aftalte sletning eller tilbagelevering af data er udført rettidigt.</p>	<p>Ingen afvigelser konstateret.</p>
<p>Opbevaring af oplysninger er i overensstemmelse med dataansvarliges krav</p> <ul style="list-style-type: none"> ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Vi har inspiceret, at procedurerne er opdateret og godkendt.</p>	<p>Ingen afvigelser konstateret.</p>

A.18: Overensstemmelse		
Kontrolmål		
<p>▶ At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.</p>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Lokation for behandling og opbevaring af oplysninger</p> <p>▶ Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.</p>	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder for behandling og opbevaring af personoplysninger.</p> <p>Vi har inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.</p>	<p>Ingen afvigelser konstateret.</p>
<p>Procedure ved overførsel af personoplysninger til tredjeland</p> <p>▶ Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelands eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.</p> <p>▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelands eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.</p> <p>Vi har inspiceret, at procedurerne er opdateret og godkendt.</p>	<p>Ingen afvigelser konstateret.</p>
<p>Instruks til overførsel af personoplysninger til tredjeland</p> <p>▶ Databehandleren må kun overføre personoplysninger til tredjelands eller internationale organisationer efter instruks fra den dataansvarlige.</p>	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelands eller internationale organisationer.</p> <p>Vi har inspiceret ved en stikprøve på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for,</p>	<p>Ingen afvigelser konstateret.</p>

A.18: Overensstemmelse		
Kontrolmål ► At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	at overførslen er aftalt med den dataansvarlige i databehandleraftalen.	
Gyldigt overførselsgrundlag ► Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer.	Ingen afvigelser konstateret.

5. SUPPLERENDE INFORMATION FRA LANDSORGANISATIONEN DANSKE DAGINSTITUTIONER

På baggrund af BDO's konstaterede afvigelse i ISAE 3000-erklæringen har Landsorganisationen Danske Daginstitutioner følgende supplerende information:

Passwordpolitik

Det er i forbindelse med udskiftning af servere i forsommeren 2025 muliggjort, at LDD's password lever op til anbefalinger fra Center for Cybersikkerhed. Tidssvarende passwordpolitik vil blive implementeret medio september 2025.

**BDO STATSATORISERET
REVISIONSPARTNERSELSKAB**

**VESTRE RINGGADE 28
8000 AARHUS C**

www.bdo.dk

BDO Statsautoriseret Revisionspartnerselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlems-firmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.800 medarbejdere, mens det verdensomspændende BDO-netværk har ca. 120.000 medarbejdere i mere end 166 lande.

*Copyright - BDO Statsautoriseret revisionspartnerselskab,
cvr.nr. 45719375.*



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

**BDO Holding VII, statsautoriseret revisionsaktieselskab CVR:
20222670**

Statsautoriseret revisor

På vegne af: BDO

Serienummer: 375cad19-f0ea-4e39-8646-d3d882b8ce8e

IP: 86.52.xxx.xxx

2025-08-17 08:50:24 UTC



Mikkel Jon Larsen

**BDO Holding VII, statsautoriseret revisionsaktieselskab CVR:
20222670**

Partner, chef for Risk Assurance, CISA, CRISC

På vegne af: BDO

Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff

IP: 77.215.xxx.xxx

2025-08-18 07:09:18 UTC



Palle Woss

Direktør

På vegne af: LDD

Serienummer: 2ca56959-4b28-4a3f-b6f3-fd13715b7c56

IP: 93.176.xxx.xxx

2025-08-18 15:08:01 UTC



Dette dokument er underskrevet digitalt via [Penneo.com](https://penneo.com). De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.