AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN 1. JULI 2023 TIL 30. JUNI 2024 OM BESKRIVELSEN AF EASYIQ SAAS LØSNINGER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

EASYIQ A/S

Penneo dokumentnøgle: 1A4S3-QZVJ-CF468-8RM5S-5FSDL-48IK

BDO

INDHOLD

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN 1. JULI 2023 TIL 30. JUNI 2024 OM BESKRIVELSEN AF EASYIQ SAAS LØSNINGER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i EasyIQ A/S
EasyIQ A/S' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af EasyIQ A/S (databehandleren) for hele perioden fra 1. juli 2023 til 30. juni 2024 udarbejdede beskrivelse i sektion 3 af EasyIQ SaaS løsninger 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 og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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, implementere og effektivt udføre 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 og den operationelle effektivitet 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 og fungerer effektivt.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. 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 eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

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

Begrænsninger i kontroller hos en databehandler

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 EasyIQ SaaS løsninger, 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. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af EasyIQ SaaS løsninger 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 i hele perioden fra 1. juli 2023 til 30. 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 i hele perioden fra 1. juli 2023 til 30. juni 2024, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. juli 2023 til 30. juni 2024.

Beskrivelse af test af kontroller

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

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens EasyIQ SaaS løsninger, 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 1. juli 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Brian Bomholdt
Partner, CISA, CISM, CISSP

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

2. EASYIQ A/S' UDTALELSE

EasyIQ A/S varetager behandling af personoplysninger i forbindelse med EasyIQ SaaS løsninger 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 EasyIQ SaaS løsninger, 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.

EasyIQ A/S anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

EasyIQ A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af EasyIQ SaaS løsninger og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden fra 1. juli 2023 til 30. juni 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for EasyIQ SaaS løsninger, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger 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 kontroller, som vi med henvisning til afgrænsningen af EasyIQ SaaS løsninger har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

2. Indeholder relevante oplysninger om ændringer i EasyIQ SaaS løsninger og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden fra 1. juli 2023 til 30. juni 2024.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af EasyIQ SaaS løsninger 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 EasyIQ SaaS løsninger, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

EasyIQ A/S 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 og fungerede effektivt i hele perioden fra 1. juli 2023 til 30. 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.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden fra 1. juli 2023 til 30. juni 2024.

EasyIQ A/S bekræfter, at der er implementeret og opretholdt 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.

Skanderborg, den 1. juli 2024
EasyIQ A/S

Frank Nygaard
Direktør

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

3. EASYIQ A/S' BESKRIVELSE AF EASYIQ SAAS LØSNINGER

EASYIQ A/S

EasyIQ A/S i sin nuværende form blev etableret i 2014 og beskæftiger i dag ca. 12 medarbejdere. Fundamentet blev grundlagt med virksomheden Systemtech A/S tilbage i 2004. Grundlaget for succesen, dengang som nu, er agil udvikling af it-systemer i tæt samarbejde med brugerne, eksperter og udviklere med stor domæneviden. Vi har stor fokus på god og hurtig kundesupport. Dette er den filosofi, der stadig udgør grundstenen i EasyIQ A/S.

EasyIQ A/S leverer egenudviklede it-systemer som software as a service. Leverancen omfatter 100% drift, service og support, konsulentydelser samt uddannelse og kurser. Hertil løbende tilpasninger af funktionalitet således at systemerne lever op til gældende lovgivning og reguleringer. Alle vores systemer udvikles, drives og forvaltes af dygtige medarbejdere med base i Danmark.

EasyIQ A/S er kvalitetsbevidst og har fokus på at levere den aftalte løsning til tiden og til skolevenlige priser. Vi arbejder efter fastlagte procedurer, der sikrer ensartethed i vores arbejde og leverancer.

Formålet med nærværende beskrivelse er at levere information til EasyIQ A/S' kunder og deres revisorer vedrørende kravene i ISAE 3000, som er den internationale revisorstandard for andre erklæringsopgaver med sikkerhed end revision. Denne ISAE 3000-erklæring afdækker relevante områder fra databehandleraftalen, som afdækker de tekniske og organisatoriske sikringsforanstaltninger, som er implementeret i forbindelse med driften af EasyIQ SaaS løsninger.

Beskrivelse af EasyIQ A/S ydelser

Produktrammen for denne beskrivelse er følgende SaaS løsninger:

- EasyIQ SkolePortal – Læringsplatform med læringsforløb, opgaver, afleveringer, portfolio, skabeloner, Fælles Mål, Læringsmål samt Elevplan / Meddelelsesbog. Integreret med Microsoft 365 og Google Workspace.

- EasyIQ Dagtilbud – Læringsplatform med læringsforløb, opgaver, afleveringer, portfolio, skabeloner, Fælles Mål, Læringsmål samt Elevplan. Integreret med Office 365 og Google Apps.

- EasyIQ Microsoft 365 – Fælles dokument og kommunikationsplatform. Office-pakke, fællesdrev, klassedrev, fildeling, mail, kalender, grupper, OneNote, OneNote Cass Notebook, Teams, Classroom, Stream (Video portal), Forms, web- og videokonferencer og meget mere med ægte Unilogin inkl. support.

- EasyIQ Google Workspace - Fælles dokument og kommunikationsplatform baseret på Google Apps med adgang til dokumenter, fællesdrev, Google Classroom samarbejdsmuligheder m.m. adgang via Unilogin inkl. support.

- EasyIQ UniRadius - Redundant radius validering i forhold til UNI-Login.

- EasyIQ Lectio2Unilogin - Synkronisering fra Lectio til Unilogin – vi står for dagligt at synkronisere Lectio til Unilogin for elever og ansatte.

- EasyIQ IdP2Lectio – Synkronisering af password fra EasyIQ IdP til Lectio – Så elever og ansatte kan servicere sig selv via EasyIQ IdP.

- EasyIQ Widgets – Widget til Aula – Skolernes nye forældrekommunikation.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

- EasyIQ ASM - Med EasyIQ ASM (Apple School Manager) oprettes, vedligeholdes og nedlægges elever, ansatte og klasser i Apple School Manager helt automatisk på baggrund af data i jeres brugeradministration.

- EasyIQ Lightspeed - Med EasyIQ Lightspeed oprettes, vedligeholdes og nedlægges elever, ansatte og klasser i Lightspeed helt automatisk på baggrund af data i jeres brugeradministration.

- EasyIQ Kodeskift – website hvor brugerne kan skifte deres AD/EasyIQ password.

- EasyIQ IDP – Redundant Unilogin IDP-løsning tilkoblet Unilogin og MitID Erhverv (NemLog-in3).

- EasyIQ MitID Erhverv – Udstedelse og MitID Erhverv via Kodeskift inkl. opsætning af rettigheder i MitID Erhverv.

- EasyIQ 2Faktor – 2 faktorløsning til Unilogin, Aula og EasyIQ SkolePortal.

- EasyIQ Hosted Administration - Organisationens it-infrastruktur i skyen. EasyIQ står for drift af infrastruktur og applikationer på kundesystemer.

EASYIQ SAAS LØSNINGER OG BEHANDLING AF PERSONOPLYSNINGER

Som ejer og leverandør af softwaren behandler databehandleren ved generel drift, herunder hosting, at skabe adgang for brugerne til de ønskede løsninger herunder login og log ud, til visning, organisering, modtagelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, logning, support, fejlfinding og andre it-ydelser, de af den dataansvarlige tilføjede personoplysninger.

EasyIQ behandler personoplysninger i overensstemmelse med den enkelte kundes databehandleraftale, som bl.a. kan omfatte: Almindelige personoplysninger:

- Navn
- Adresse (inkl. by og postnr.)
- E-mail
- Telefonnummer
- Køn
- Fødselsdato

Særlige kategorier af personoplysninger samt personoplysninger vedrørende CPR-nummer, straffedomme og lovovertrædelser:

- CPR-nummer og oplysninger fra CPR-register

Listen er ikke udtømmende, da det afhænger af den databehandling, der foretages for den enkelte dataansvarlige.

STYRING AF PERSONDATASIKKERHED

EasyIQ 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 databehandler i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

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	Control activities	GDPR article
Risikovurdering	• Risikovurdering	• Artikel 28, stk. 3, litra c
A.5: Informationssikkerhedspolitikker	• Politik for Informationssikkerhed • Gennemgang af informationssikkerhedspolitik	• Artikel 28, stk. 1
A.6: Organisering af informationssikkerhed	• Roller og ansvarsområder • Politik for mobilt udstyr og Fjernarbejdspladser	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra c
A.7: Personalesikkerhed	• Rekruttering af medarbejdere • Uddannelse og awareness af medarbejdere • Awareness og oplysningskampagner for medarbejdere • Tavsheds- og fortrolighedsaftale med medarbejdere • Fratrædelse af medarbejdere	• Artikel 28, stk. 1 • 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 • Styring af privilegerede adgangsrettigheder • Gennemgang af brugeradgangsrettigheder • Procedure for sikkert log-on	• Artikel 28, stk. 3, litra c
A.10: Kryptografi	• Politik for anvendelse af kryptografi • Administration af nøgler	• Artikel 28, stk. 3, litra c
A.11: Fysisk sikring og miljøsikring	• Fysisk adgangskontrol • Fysisk sikkerhed • 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 • Overvågning • Sårbarhedsscanning	• 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	• 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	• Artikel 28, stk. 2 og 4

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

	• Oversigt over godkendte underdatabehandlere • Tilsyn med underdatabehandlere	
A.16: Styring af informationssikkerheds-brud	• Ansvar og procedurer • Underretning om brud på persondatasikkerheden • Registrering af brud på persondatasikkerheden	• Artikel 33, stk. 2
A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring	• Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse	• Artikel 28, stk. 3, litra c
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 persondata-sikkerheden og konsekvensanalyser • Revision og inspektion • Sletning af personoplysninger • Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger	• Artikel 28, stk. 3, litra a, c, e, f, g og h • Artikel 29 • Artikel 32, stk. 4 • Artikel 28, stk. 10

RISIKOVURDERING

Direktionen er ansvarlig for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som EasyIQ 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

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.

A.5: Informationssikkerhedspolitikker

EasyIQ A/S har indført politikker og procedurer, der sikrer, at kunden 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. EasyIQ har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af direktionen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres.

A.6: Organisering af informationssikkerhed

Roller og ansvarsområder

Direktionen hos EasyIQ A/S har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

Politik for mobilt udstyr og fjernarbejdspladser
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til anvendelsen er håndteret.

A.7: Personalesikkerhed

Rekruttering og fratrædelse af medarbejdere
Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere. HR-afdelingen arbejder med faste procedurer for bl.a. rekruttering og ansættelse og fratrædelser. Nye medarbejdere gennemgår et grundigt introduktionsforløb til virksomheden. Forløbet omfatter information i informationssikkerhed, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd, dataklassifikation og særligt fokus på EasyIQ A/S' rolle som databehandler.

Uddannelse og instruktion af medarbejdere, der behandler personoplysninger og Awareness og oplysningskampagner for medarbejdere
For at sikre en kontinuerlig tilgang til informationssikkerhedskulturen har EasyIQ A/S et årligt IT-Sikkerhedsinformationsmøde. Informationen revurderes årligt af informationssikkerhedsorganisationen.

Fortrolighed og lovbestemt tavshedspligt
Alle medarbejdere har en fortrolighedsklausul i deres ansættelseskontrakter. Som en del af vores fratrædelsesprocedure indgår en exit-samtale med nærmeste leder, hvor vi minder om, at fortrolighedsklausulen fortsat er gældende efter endt ansættelse.

A.8: Styring af aktiver

Fortegnelse over kategorier af behandlingsaktiviteter
EasyIQ A/S 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
Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.

A.9: Adgangsstyring

EasyIQ A/S har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. 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, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

A.10: Kryptografi

EasyIQ A/S har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

EasyIQ A/S har indført procedurer, der sikrer, at data på personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, er krypteret ved ibrugtagning, således at adgang til data alene er mulig for autoriserede brugere. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

De algoritmer og niveauer for kryptering, der er anvendt til kryptering af enheder, servere og data, risikovurderes løbende i forhold til det aktuelle trusselsniveau.

A.11: Fysisk sikring og miljøsikring

Fysisk adgangskontrol

EasyIQ A/S har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne, og særlige sikkerhedsmæssige foranstaltninger er indført for områder, hvor der foretages behandling af personoplysninger. Kunder, leverandører og andre besøgende ledsages.

Fysisk sikkerhed

EasyIQ A/S har indført procedurer, der sikrer, at servere er beskyttet mod uautoriseret adgang, beskadigelse, driftsafbrydelser og lignende hændelser ved særlige sikkerhedsforanstaltninger. Servere er således opbevaret i et særligt indrettet serverrum med fysisk og elektronisk adgangskontrol og logning af adgange. Serverrummet er sikret mod miljømæssige trusler som brand, vandindtrængning, fugt, overophedning, strømudfald og overspænding. Systemer til miljømæssig sikring af driftsfaciliteter er serviceret og vedligeholdt løbende efter de respektive leverandørers forskrifter. Driftsmiljøet er overvåget.

Reparation og service samt bortskaffelse af it-udstyr

EasyIQ A/S har indført procedurer, der sikrer, at udstyr, som udleveres til tredjemand for service, reparation eller bortskaffelse, udleveres uden datadiske, og at brugte og kasserede datamedier og diske registreres og destrueres af certificeret leverandør.

A.12: Driftssikkerhed

Vedligeholdelse af systemsoftware

EasyIQ A/S har indført procedurer, der sikrer, 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

EasyIQ A/S har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselsniveau, og der er opsat en løbende overvågning af disse systemer, herunder periodisk test for funktionalitet.

Sikkerhedskopiering og retablering af data

EasyIQ A/S har indført procedurer, der sikrer, 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 sikkerheds-kopier ødelægges ved brand, vand, hærværk eller hændelig skade.

Logning i systemer, databaser og netværk

EasyIQ A/S har indført procedurer, der sikrer, 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.

Overvågning

EasyIQ A/S har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Sårbarhedsscanning og penetrationstests

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

EasyIQ A/S har indført procedurer, der sikrer, at systemer er indført med henblik på at identificere og imødegå tekniske sårbarheder i applikationer, services og infrastruktur, således at tab af fortrolighed, integritet og tilgængelighed af systemer og data undgås.

A.13: Kommunikationssikkerhed

Netværkssikkerhed
EasyIQ A/S 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
EasyIQ A/S har indført procedurer, der 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
EasyIQ A/S har indført procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med stærk kryptering, og at e-mail og anden kommunikation, der indeholder følsomme personoplysninger, er krypteret i forsendelsen ved anvendelse af TLS.

A.14: Anskaffelse, udvikling og vedligeholdelse

Udvikling og vedligeholdelse af systemer
EasyIQ A/S har indført politikker og procedurer for udvikling og vedligeholdelse af EasyIQ SaaS løsninger, der sikrer en styret ændringsproces. Der anvendes et Change Management system til styring af udviklings- og ændringsopgaver, og enhver opgave følger en ensartet proces, der indledes med risikovurdering i overensstemmelse med kravene om databeskyttelse gennem design og standardindstillinger.

Udviklings-, test- og produktionsmiljø er adskilte, og der er etableret funktionsadskillelse mellem medarbejdere i udviklingsafdelingen og i drifts- og supportafdelingen. Enhver udviklings- og ændringsopgave gennemløber et testforløb, og der anvendes anonymiserede produktionsdata som testdata. Der er indført procedurer for versionskontrol, logning og sikkerhedskopiering, således at det er muligt at geninstallere tidligere versioner.

A.15: Leverandørforhold

Underdatabehandleraftale og instruks
EasyIQ A/S har indført politikker og procedurer, der sikrer, at underdatabehandlere er blevet pålagt de samme databeskyttelsesforpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og EasyIQ, og at underdatabehandlerne kan give tilstrækkelige garantier til beskyttelse af personoplysninger. Procedurerne 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.

EasyIQ A/S vurderer underdatabehandleren og dennes garantier, forinden der indgås aftale, for at sikre, at underdatabehandleren kan overholde de forpligtelser, som er pålagt EasyIQ A/S. EasyIQ A/S 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

EasyIQ A/S har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at EasyIQ A/S 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.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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

Beredskabsplaner
EasyIQ A/S har udformet detaljerede beredskabsplaner og planer for retablering af systemer og data, der blandt andet sikrer personuafhængighed i forbindelse med aktivering af beredskabet og retableringen. Planerne er i kopi opbevaret sikret uden for EasyIQ A/S' it-systemer. Planerne afprøves og revideres løbende i forbindelse med ændringer i systemer mv.

A.18: Overensstemmelse

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

Instruks for behandling af personoplysninger
EasyIQ A/S har indført politikker og procedurer, der sikrer, at EasyIQ A/S 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, herunder hvem der hos den dataansvarlige kan give bindende instruks til EasyIQ A/S. Proceduren sikrer desuden, at EasyIQ A/S informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

Bistand til den dataansvarlige
EasyIQ A/S har indført politikker og procedurer, der sikrer, at EasyIQ A/S kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

EasyIQ A/S har indført politikker og procedurer, der sikrer, at EasyIQ A/S 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.

EasyIQ A/S har indført politikker og procedurer, der sikrer, at EasyIQ A/S kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlerne, til rådighed for den dataansvarlige.

Sletning og tilbagelevering af personoplysninger
EasyIQ A/S 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
EasyIQ A/S har indført procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

ÆNDRINGER I PERIODEN 1. JULI 2023 TIL 30. JUNI 2024

EasyIQ A/S har ikke foretaget væsentlige ændringer i EasyIQ SaaS løsninger og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i perioden 1. juli 2023 til 30. juni 2024

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Den dataansvarlige er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed opfylde databeskyttelseslovgivningen:

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

- At sikre, at brugeroprettelser og brugersletning hos de dataansvarlige sker i deres eget studieadministrative system eller lønsystem, hvorefter der via en integration til Styrelsen for It og Læring sker adgangs- og rettighedstildeling i EasyIQ SaaS-løsninger. De dataansvarlige er derfor selv ansvarlige for, at deres brugere har de korrekte roller i deres studieadministrative system eller lønsystem.
- At sikre, at personoplysningerne er ajourførte og slettes behørigt, hvis det skal slettes tidligere end 90 dage efter brugerne er afmeldt.
- At sikre, at der er indgået en kontrakt og databehandleraftale med EasyIQ, der sikrer, at EasyIQ alene handler efter instruks fra den enkelte kunde, og at EasyIQ træffer alle nødvendige og tekniske foranstaltninger til behandling af personoplysninger.
- At sikre, at instruksen er hensigtsmæssig set i forhold til databehandleraftalen og hovedydelsen.
- At sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering.
- At sikre, at tilgang til terminaler, pc'ere, bærbare og andre enheder, der kan tilgå EasyIQ's Skoleportal og IT Platformen, alene sker for autoriserede brugere, herunder tildeling af rettigheder til autoriserede brugere.
- At sikre, at den dataansvarliges brugere er ajourførte.
- At sikre hensigtsmæssige kontroller for adgangsbrugeradministration og datamanagement, herunder sletning fra Windows Azure og Office 365 samt Googles G-suite.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 EasyIQ A/S' beskrivelse af EasyIQ SaaS løsninger samt for udformningen og den operationelle effektivitet 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 eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af EasyIQ A/S, 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 og har fungeret effektivt i hele perioden fra 1. juli 2023 til 30. juni 2024.

Udførte testhandlinger

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

Type	Beskrivelse
Forespørgsel	Forespørgsler hos EasyIQ A/S' 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.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som Microsoft Azure leverer inden for logning, har vi modtaget revisionserklæring for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. oktober 2022 til den 30. september 2023, samt tilhørende bridgeletters.

For de ydelser, som Fuzion A/S leverer inden for housing af systemerne, har vi modtaget revisionserklæring for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. juli 2022 til den 30. juni 2023.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

For de ydelser, som GlobalConnect leverer inden for housing af systemerne, har vi modtaget revisionserklæring for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. januar til den 31. december 2023.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i EasyIQ A/S' beskrivelse af EasyIQ SaaS løsninger og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos EasyIQ A/S, 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 og implementeret eller ikke har fungeret effektivt i perioden.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 én gang årligt en risikovurdering af it-miljøerne baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for risikovurdering, og observeret at den fastlægger at databehandlerens SaaS løsninger skal risikovurderes ud fra identificerede trusler og baseres på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder, samt at risici skal minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. Vi har inspiceret risikovurderingen af databehandlerens SaaS løsninger og observeret, at den er udarbejdet i overensstemmelse med proceduren. Vi har inspiceret dokumentation for, at databehandleren har foretaget den årlige gennemgang af risikovurderingen i erklæringsperioden. Vi har observeret, at der ikke er sket ændringer i den vurderede risiko i erklæringsperioden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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**
Politik for Informationssikkerhed ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at denne tager udgangspunkt i ISO 27001 standarden. Vi har inspiceret, at alle medarbejdere har underskrevet, at de har læst og accepteret informationssikkerhedspolitikken.	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum én gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at det er direktørens ansvar at gennemgå og opdatere informationssikkerhedspolitikken minimum én gang årligt. Vi har inspiceret, at direktøren har gennemgået informationssikkerhedspolitikken, og at denne er blevet godkendt af bestyrelsen i erklæringsperioden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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. ▶ Databehandleren har udpeget et kontaktpunkt for dataansvarlig med hensyn til behandling af persondata.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at direktøren har ansvaret for informationssikkerheden. Vi har inspiceret databehandlerens databehandlerskabelon og stikprøvevist udvalgt databehandleraftaler og observeret, at databehandleren har udpeget et kontaktpunkt for de dataansvarlige med hensyn til behandling af persondata.	Ingen afvigelser konstateret.
Politik for mobilt udstyr og fjernarbejdspladser ▶ Databehandleren har udarbejdet og implementeret en politik og understøttende sikkerhedsforanstaltninger til styring af risici for personoplysninger, der opstår ved anvendelse af mobilt udstyr. ▶ Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til anvendelsen er håndteret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at databehandleren har en politik for mobile enheder og fjernarbejdspladser, der fastlægger krav om anvendelse af Bitlocker, firewall og antivirus, Vi har stikprøvevist inspiceret dokumentation for, at databehandlerens medarbejdere efterlever de angivne sikkerhedsforanstaltninger for mobile enheder.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 udfører 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 databehandleren har en procedure for rekruttering af medarbejdere og observeret, at der skal gennemføres baggrundstjek ved ansættelse af nye medarbejdere. Vi har inspiceret dokumentation for, at der for alle nyansatte i erklæringsperioden er foretaget baggrundstjek i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Der udføres et introduktionsforløb for nye medarbejdere, herunder introduktion til informationssikkerhed, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd, dataklassifikation og særligt fokus på virksomhedens rolle som databehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for introduktionsforløb for nye medarbejdere og observeret, at der fastlægges krav til gennemførsel af specifikke kurser omhandlende it-sikkerhed og persondatabeskyttelse indenfor de første tre måneders ansættelse. Vi har inspiceret dokumentation for, at alle nyansatte i erklæringsperioden har deltaget i og gennemført specifikke kurser omhandlende it-sikkerhed og persondatabeskyttelse indenfor de første tre måneders ansættelse. Vi er på forespørgsel blevet oplyst, at introduktion til informationssikkerhedsorganisationen sker via sidemandsoplæring og læsning af informationssikkerhedshåndbogen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren afholder årligt et IT-sikkerhed informationsmøde for at sikre en kontinuerlig tilgang til informationssikkerhedskulturen. ▶ Databehandleren afholder årligt IT-sikkerhedstræning, som medarbejderne skal bestå.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at der skal afholdes et årligt møde til sikring af, at medarbejdere holdes ajour med sikkerhed og bevidstgøres om eventuelle nye trusler eller regler. Vi har inspiceret dokumentation for at afholdelse af det årlige IT-sikkerhed informationsmøde og observeret, at alle medarbejdere har deltaget. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at der løbende og minimum årligt skal afholdes IT-sikkerhedstræning af medarbejdere. Vi har inspiceret dokumentation for, at databehandleren har afholdt tests i GDPR og informationssikkerhed og observeret, at som alle medarbejdere har gennemført og bestået.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet en ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Alle medarbejdere har underskrevet informationssikkerhedshåndbogen, der indeholder en bestemmelse om tavshedspligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon til ansættelseskontrakter og observeret, at den indeholder bestemmelse om tavshedspligt. Vi har inspiceret dokumentation for, at alle nyansatte i erklæringsperioden har underskrevet en ansættelseskontrakt, der er baseret på skabelonen og indeholder bestemmelse om tavshedspligt.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
	Vi har inspiceret informationssikkerhedshåndbogen og observeret, at der indgår krav om tavshedspligt og fortrolighed i informationssikkerhedshåndbogen. Vi har inspiceret, at alle medarbejdere har underskrevet informationssikkerhedshåndbogen herunder krav om tavshedspligt og fortrolighed.	
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 databehandlerens informationssikkerhedshåndbog og observeret, at når en medarbejder skifter ansvarsområde eller stopper i virksomheden, gennemgår og justerer lederen medarbejderens rettigheder og systemadgange. Vi er på forespørgsel, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at der ikke været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

A.8: Styring af aktiver

Kontrolmål

- *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 én gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. Vi har observeret, at fortegnelsen er opdateret i erklæringsperioden.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk	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 på forespørgsel fået oplyst, at databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet. Vi har på forespørgsel fået oplyst, at der ikke har været anmodninger fra Datatilsynet i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at der ikke har været anmodninger fra Datatilsynet i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet. Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

A.8: Styring af aktiver

Kontrolmål

- *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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedshåndbogen og observeret, at databehandleren har en procedure, som skal sikre, at medier/udstyr destrueres korrekt, således at data på medierne ikke kan genskabes. Vi har observeret, at der ikke har været medier eller udstyr, der er destrueret eller bortskaffet i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at der ikke har været medier eller udstyr, der er destrueret eller bortskaffet i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet. Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

A.9: Adgangsstyring

Kontrolmål

- *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 autoriseret. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for brugeradministration, som fastlægger, at brugeroprettelser og -nedlæggelser følger skal følge en styret proces, og at alle brugeroprettelser skal være autoriseret, og brugerrettigheder skal tildeles ud fra et arbejdsbetinget behov. Vi har inspiceret dokumentation for, at alle brugeroprettelser i erklæringsperioden er sket i overensstemmelse med proceduren, og er autoriseret og at adgange er tildelt ud fra den ansattes arbejdsbetingede behov. Vi har inspiceret dokumentation for, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste for procedurens implementering og effektivitet vedrørende nedlæggelser. Vi har inspiceret, at kundens brugere automatisk oprettes og slettes gennem en integration til STIL, som trækker data fra kundens eget studieadministrative system. Kunderne er derfor selv ansvarlige for, at deres brugere har de korrekte roller i deres administrative system.	Vi har konstateret, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste denne del af kontrollens implementering og effektivitet. Ingen afvigelser konstateret.
Styring af privilegerede adgangsrettigheder ▶ 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 databehandlerens procedure for brugeradministration, som fastlægger, at brugerrettighedsstyring skal følge en	Vi har konstateret, at der ikke er tildelt privilegerede rettigheder til egne medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

A.9: Adgangsstyring		
Kontrolmål ▶ *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**
	styret proces, og at brugerrettigheder skal tildeles ud fra et arbejdsbetinget behov. Vi har på forespørgsel fået oplyst, at der ikke er tildelt privilegerede rettigheder til egne medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste for procedurens implementering og effektivitet. Vi har inspiceret, at ved kundeoprettelse opretter databehandleren den første privilegerede bruger til systemerne, som herefter kan tildele yderligere privilegerede rettigheder i deres organisation.	
Gennemgang af brugeradgangsrettigheder ▶ Der foretages årligt gennemgang af brugere og brugerrettigheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at der minimum én gang årligt skal foretages periodisk gennemgang af brugere og tilhørende rettigheder. Vi har inspiceret, at databehandleren har gennemgået brugere og tilhørende rettigheder i erklæringsperioden.	Ingen afvigelser konstateret.
Procedure for sikkert log-on ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, som skal følges af alle medarbejdere	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret passwordpolitikken til databehandlerens SaaS løsninger samt medarbejdernes arbejdscomputere og observeret, at databehandleren har etableret tilstrækkelig logisk adgangskontrol til systemer og arbejdscomputere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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. ▶ EasyIQ A/S har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier. Genopprettelsesnøgler og certifikater opbevares på forsvarlig vis. ▶ Bærbare medier med personoplysninger er krypteret. ▶ 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 databehandlerens procedure for kryptografi og observeret at den fastlægger krav til kryptering af persondata, anvendelse af bestemte protokoller samt anvendelse af certifikater. Vi har inspiceret dokumentation for, at databehandleren følger deres procedure for kryptografi. Vi har inspiceret dokumentation for, at databaser, der indeholder personoplysninger er krypteret og at certifikater opbevares på forsvarlig vis. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at alle bærbare medier med personoplysninger skal være krypteret. Vi har stikprøvevist inspiceret, at medarbejdernes bærbare medier med personoplysninger er krypteret. Vi har inspiceret, at databehandleren har en sikker mail funktion til brug for fremsendelse af personoplysninger.	Ingen afvigelser konstateret.
Administration af nøgler ▶ Krypteringsnøgler opbevares på en lokation, der er forskellig fra, hvor krypteret data er lagret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at krypteringsnøgler opbevares på en lokation, der er forskellig fra, hvor krypteret data er lagret.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 én gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har fysisk inspiceret, at databehandleren har opsat logisk adgangskontrol ved indgangen til kontorfællesskabet. Vi har inspiceret oversigt over adgang til virksomhedens kontor og observeret, at adgange er tildelt til databehandlerens medarbejdere. Vi har inspiceret, at adgange til kontorfællesskabet registreres og logges. Vi har inspiceret, at databehandlerens direktør har gennemgået loggen og sammenholdt den med tildelte adgange.	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 krav til serverrum.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret revisionserklæringer fra anvendte housing-leverandører og observeret, at der ikke har været konstateret svagheder i forhold til den fysiske sikkerhed.	Ingen afvigelser konstateret.
Sikring af udstyr og aktiver for organisationen ▶ Adgang til organisationens server fra fjernarbejdspladser tilgås via RDP-løsning med 2-faktor autentifikation.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
	Vi har inspiceret informationssikkerhedshåndbogen og observeret, at adgang til servere fra fjernarbejdspladser skal ske via 2-faktor autentifikation. Vi har stikprøvevist inspiceret, at databehandlerens medarbejdere kun kan opnå adgang til servere med anvendelse af 2-faktor autentifikation.	
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 inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at den fastlægger, at når it-udstyr skal sendes til reparation og service skal det ske uden indhold af personoplysninger, samt at ved bortskaffelse skal it-udstyr destrueres. Vi har inspiceret, at der ikke har været medier, der er sendt til reparation, destrueret eller bortskaffet i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at der ikke har været nogle medier, der er sendt til reparation, destrueret eller bortskaffet i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.
Politik for ryddeligt skrivebord og skærmlås - Skærmlås aktiveres automatisk. - Medarbejdere skal aktivere skærmlås, når klienten forlades.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at den fastlægger at arbejdsstationer automatisk skal skærmlåses og at medarbejdere skal aktivere skærmlås når klienten forlades. Vi har stikprøvevist inspiceret dokumentation for, at medarbejdere har opsat automatisk pauseskærm efter 15 minutter.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
	Vi er på forespørgsel blevet oplyst, at medarbejdere aktiverer skærmlås, når klienter forlades.	

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandlerens medarbejdere selv er ansvarlige for at opdatere deres arbejdscomputere. Vi har stikprøvevist inspiceret dokumentation for, at databehandlerens medarbejdere har opdateret deres operativsystem-software. Vi har inspiceret databehandlerens procedure for vedligeholdelse af servere og observeret, at opdatering af servernes operativsystem skal ske løbende og minimum hvert kvartal. Vi har stikprøvevist inspiceret, at serveres operativsystem-software er opdateret.	Ingen afvigelser konstateret.
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende til seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at den fastlægger at servere og arbejdsstationer skal have installeret opdateret antivirus. Vi har stikprøvevist inspiceret, at databehandlerens medarbejdere har installeret og opdateret antivirus på deres arbejdscomputere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
	Vi har stikprøvevist inspiceret, at servere har installeret og opdateret antivirus.	
Sikkerhedskopiering og retablering af data ▶ Generel OS Backup – foretages 1 gang pr. uge og gemmes i 4 uger ▶ Kritiske OS Backup - backup hver dag og gemmes i 4 uger ▶ SQL Backup – Backup hver dag og gemmes i 14 dage ▶ Der udføres restore-tests én gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for backup og observeret, at der skal foretages general OS backup 1 gang pr. uge, som gemmes i 4 uger, at der for kritiske OS-backup skal foretages daglig backup, som gemmes i 4 uger og at der skal foretages SQL backup dagligt, som gemmes i 14 dage. Vi har inspiceret, at databehandleren foretager backup i overensstemmelse med databehandlerens procedure. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at der er beskrevet krav om restore-test minimum én gang årligt. Vi har inspiceret, at der er gennemført restore-test i erklæringsperioden.	Ingen afvigelser konstateret.
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Der anvendes et centralt overvågningsværktøj, der afgiver alarmer, hvis kendte fejl opstår. ▶ Alle succesfulde adgange og mislykkede adgangsforsøg til databehandlerens systemer og data logges.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
▶ Alle brugerændringer i system og databaser logges. ▶ Loggen slettes efter den fastsatte retentionperiode. ▶ Databehandleren monitorerer og logger netværkstrafik.	Vi har inspiceret databehandlerens overvågningsværktøj og observeret, at der overvåges for fejl og udsendes alarmer herom. Vi har stikprøvevist inspiceret hændelseslog for dataansvarliges adgang til databehandlerens systemer og data og observeret at alle succesfulde adgange og mislykkede adgangsforsøg, samt brugerændringer, logges. Vi har inspiceret dokumentation for, at logs ikke opbevares i længere tid end den fastsatte retentionperiode. Vi har inspiceret dokumentation for, at databehandleren monitorerer og logger netværkstrafik.	
Overvågning ▶ Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. ▶ Databehandleren notificeres om identificerede alarmer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. Vi har inspiceret, at databehandleren notificeres om identificerede alarmer.	Ingen afvigelser konstateret.
Sårbarhedsscanning ▶ Der foretages løbende sårbarhedsscanning af databehandlerens netværk. Resultatet dokumenteres i en rapport.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
▶ Databehandleren gennemgår rapporten og følger op på konstaterede svagheder. ▶ Databehandleren håndterer/mitigerer eventuelle sårbarheder ud fra en risikovurdering. ▶ Databehandleren har dokumenteret deres håndtering/mitigering af fundne sårbarheder.	Vi har inspiceret procedure for gennemførsel af løbende sårbarhedsscanninger og observeret, at databehandlerens direktør hver måned modtager en rapport på baggrund af seneste måneds scanninger. Vi har inspiceret dokumentation for gennemførte sårbarhedsscanninger og observeret, at der ikke er konstateret nogle svagheder af høj risiko. Vi er på forespørgsel blevet oplyst, at der ikke har været nødvendigt at implementere mitigerende foranstaltninger på baggrund af udførte sårbarhedsscanninger i erklæringsperioden.	

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværkstypologi og observeret, at al kundetrafik køres gennem Cloudflare for filtrering og DDOS-beskyttelse, hvilket sikrer at servere, som driver applikationer, ikke kan nås direkte fra internettet. Vi har inspiceret, at netværksfirewall er opsat, således at servere, som driver applikationer, ikke kan nås direkte fra internettet.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall efter minimumsprincippet. ▶ Arbejdsstationer benytter firewall.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for håndtering af netværkssikkerhed og observeret, at alene godkendt netværkstrafik må komme gennem firewallen. Vi har stikprøvevist inspiceret opsætning af firewall på servere og observeret, at alene godkendt netværkstrafik kan komme gennem firewallen. Vi har inspiceret databehandlerens informationssikkerhedshåndbog og observeret, at alle serverer og arbejdsstationer skal benytte firewall. Vi har stikprøvevist inspiceret dokumentation for, at firewall er aktiveret på arbejdsstationer og servere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 ▶ Udveksling af personoplysninger via e-mail sker vha. en sikker mailløsning.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for elektroniske meddelelser og observeret, at personfølsomme oplysninger og andre informationer, der kræver særlige sikkerhedsforanstaltninger, altid sendes via sikker mail. Vi har på forespørgsel fået oplyst, at det sker meget sjældent, at databehandleren skal fremsende personoplysninger over mail. Hvis dette er tilfældet, har databehandleren opsat en sikker mail funktion. Vi har inspiceret, at databehandleren har en sikker mail til brug for fremsendelse af personoplysninger.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
Udvikling og vedligeholdelse af systemer ▶ Databehandleren arbejder ud fra Privacy by Design og Privacy by Default principper i udviklings- og vedligeholdelsesopgaver. ▶ Risikovurdering af systemændringer er udført for at sikre databeskyttelse gennem Privacy by Design og Privacy by Default. ▶ Databehandleren har tilrettet systemudvikling og vedligeholdelsesaktiviteter baseret på en egenudviklet projektmodel. ▶ Alle ændringer, som skal idriftsættes i produktionsmiljøet, skal være godkendt før udrulning. ▶ Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at databehandleren har forholdt sig til Privacy by Design og Privacy by Default principperne. Vi har inspiceret, at databehandleren har designet løsningen til at gemme mindst mulig information omkring brugerne. Vi har inspiceret, at der er lavet tiltag til at fremsøge og slette brugere i forbindelse med en indsigtsbegæring og i forbindelse med retten til at blive glemt. Vi har inspiceret, at de dataansvarliges brugerne automatisk slettes i AD 60 dage, efter de er stoppet hos de dataansvarlige. Vi har inspiceret, at de dataansvarliges brugerne automatisk slettes i SQL 90 dage, efter de er stoppet hos de dataansvarlige.Vi har inspiceret databehandlerens procedure for ændringsstyring og observeret, at: ▶ Alle ændringer drøftes, prioriteres og godkendes af ansvarshavende ▶ Alle ændringer testes ▶ Alle ændringer godkendes før idriftsættelse Vi er på forespørgsel blevet oplyst at principperne indgår i den løbende udviklingsproces. Vi har stikprøvevis inspiceret, dokumentation at databehandleren har fulgt processen for udvikling og vedligeholdelse af systemer. Vi har inspiceret, at ændringer godkendes af databehandlerens direktør.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode.	
Informationssikkerhed i udvikling og ændringer ▶ Rollback-plan er implementeret i tilfælde af fejl i produktionsmiljøet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er implementeret mulighed for Rollback i tilfælde af fejl i produktionsmiljøet.	Ingen afvigelser konstateret.
Adskillelse af udviklings-, test- og produktionsmiljø ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har fået fremvist og inspiceret, at udvikling og test udføres i miljøer, som er adskilt fra produktionsmiljøet.	Ingen afvigelser konstateret.
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes fiktive testdata i udviklings- og testmiljø.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at der ikke anvendes persondata i udviklings- og testmiljøet.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databehandlerskabelon og stikprøvevist udvalgt databehandleraftaler og observeret, at databehandleren har anført underdatabehandlere. Vi har inspiceret indgået underdatabehandleraftale med Microsoft Azure og observeret, at databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt, at aftalen opbevares elektronisk og at aftalen indeholder information om brugen af underdatabehandlere. Vi har foretaget inspektion af, at databehandleren anvender en underdatabehandler, Microsoft Azure, der er reguleret af amerikansk lovgivning, og at der derved kan ske en utilsigtet overførsel til tredjelande via underdatabehandlerne. Vi har inspiceret dokumentation for, at der pr. 10. juli 2023 er etableret et gyldigt overførselsgrundlag, idet at vi har inspiceret, at Microsoft har tiltrådt EU-U.S Data Privacy Framework, der trådte i kraft 10. juli 2023. Vi har inspiceret databehandleraftalen med Microsoft om Azure og observeret, at der ifølge aftalen udelukkende må anvendes datacentrer i EU til opbevaring af data.	Vi har konstateret, at Microsoft Azure har tiltrådt det nye overførselsgrundlag EU-U.S. Data Privacy Framework, som trådte i kraft den 10. juli 2023. Databehandleren har redegjort for, at der i perioden før den 10. juli 2023, ikke skete overførsel af personoplysninger til usikre tredjeland, og at de har konfigureret samt implementeret sikringsforanstaltninger til beskyttelse af personoplysninger ved brug af Microsoft Azure som underdatabehandler. Ingen øvrige afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevist inspicere dokumentation for, at der kun anvendes godkendte underdatabehandlere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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. ▶ 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 inspiceret databehandlerskabelonen og stikprøvevist indgåede databehandleraftaler og observeret, at ved ændringer af underdatabehandlere skal databehandleren underrette og have skriftlig godkendelse før en ny underdatabehandler må tages i brug. Vi har på forespørgsel fået oplyst, at der ikke er sket ændringer i brugen af underdatabehandlere i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at der ikke er sket ændringer i brugen af underdatabehandlere i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet lokation for behandling samt hvilken type af behandling og kategori af personoplysninger, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databehandlerskabelon og stikprøvevist indgåede databehandleraftaler og observeret, at der fremgår en oversigt over godkendte underdatabehandlere, herunder lokation for behandling, type af behandling og kategori af personoplysninger som underdatabehandler foretager.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
	Vi har inspiceret revisionserklæringer, som databehandleren har lagt til grund for deres tilsyn med deres underdatabehandlere. Vi har inspiceret seneste 3402 erklæring fra Fuzion for perioden 1. juli 2022 til 30. juni 2023. Vi har inspiceret seneste 3402 erklæring fra GlobalConnect for perioden 1. januar til 31. december 2023 Vi har inspiceret modtagen SOC 2 erklæring fra Microsoft Azure for perioden 1. oktober, 2022 – 30. september 2023 og tilhørende bridge letters. Vi har inspiceret, at databehandleren har gennemgået revisions-erklæringerne og observeret, at de er vurderet tilstrækkelige og tilfredsstillende.	

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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, at databehandleren har en procedure for håndtering af persondatabrud og observeret, at der er fastlagt ledelsesansvar og roller i forbindelse med brud på persondatasikkerheden. Vi er på forespørgsel blevet oplyst, at der ikke er konstateret brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at der ikke har været brud på persondatasikkerhed i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. 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 dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en procedure for håndtering af persondatabrud og observeret, at der skal ske underretning til de dataansvarlige. Vi er på forespørgsel blevet oplyst, at der ikke er konstateret brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at der ikke har været brud på persondatasikkerhed i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.
Registrering af brud på persondatasikkerheden ▶ Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en procedure for håndtering af persondatabrud og observeret, at der skal ske registrering af bruddet.	Vi har konstateret, at der ikke har været brud på persondatasikkerhed i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 er på forespørgsel blevet oplyst, at der ikke er konstateret brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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

Kontrolmål

- *Informationssikkerheds- og databeskyttelseskontinuiteten skal være forankret I organisationens ledelsessystemer for nød-, beredskabs- og retableringsstyring - GDPR-artikel 28, stk. 3, litra c.*
- *At sikre tilgængelighed af informations- og databehandlingsfaciliteter - GDPR-artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidig at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en beredskabsplan for at sikre hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. Vi har inspiceret, at databehandleren har gennemført test af beredskabsplanen i erklæringsperioden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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. ▶ 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 databehandleraftaleskabelon for indgåelse af databehandleraftaler Vi har stikprøvevist inspiceret indgåede databehandleraftaler i erklæringsperioden og observeret, at databehandleraftaler underskrives og opbevares elektronisk samt indeholder informationer om brugen af underdatabehandlere.	Ingen afvigelser konstateret.
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ 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 stikprøvevist inspiceret, at indgåede databehandleraftaler indeholder instruks for behandling af personoplysninger fra de dataansvarlige.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har forholdt sig til, at de udelukkende udfører behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig 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 procedure for underretning af dataansvarlige ved ulovlig instruks og observeret, at databehandler i tilfælde af ulovlig instruks underretter dataansvarlig herom. Vi har på forespørgsel fået oplyst, at der ikke er sket sådanne hændelser i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at databehandleren ikke har modtaget instruks stridende mod databeskyttelsesforordningen i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.
De registreredes rettigheder ▶ Databehandler har udarbejdet en procedure for bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for bistand ved opfyldelse af de registreredes rettigheder og observeret, at databehandleren vil og er i stand til at yde bistand til dataansvarlig i relation hertil. Vi har på forespørgsel fået oplyst, at databehandleren ikke har modtaget forespørgsel på sådan bistand i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Vi har konstateret, at databehandleren ikke har modtaget forespørgsel på bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Vi har konstateret, at databehandleren ikke har modtaget forespørgsel på bistand til dataansvarlig ved opfyldelse af bistand i forhold til artikel 32-36 i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 bistand til den dataansvarlige ved opfyldelse af artikel 32-36 og observeret, at databehandleren vil og er i stand til at yde bistand i relation hertil. Vi har på forespørgsel fået oplyst, at databehandleren ikke har modtaget forespørgsel på sådan bistand i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.	Ingen afvigelser konstateret.
Revision og inspektion ▶ Databehandleren er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon til databehandleraftaler og stikprøvevist indgåede databehandleraftaler og observeret, at databehandler er forpligtet til at få udarbejdet en årlig ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. Vi har observeret at databehandler årligt får udarbejdet en ISAE 3000 erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger.	Ingen afvigelser konstateret.
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 procedure for ophør af aftaler og observeret, at databehandleren skal slette dataansvarliges personoplysninger straks efter ophørt af hovedaftalen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

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 inspiceret oversigt over ophørte databehandleraftaler i erklæringsperioden. Vi har stikprøvevist inspiceret dokumentation for at, at databehandleren har slettet dataansvarliges personoplysninger straks efter ophør af hovedaftaler i erklæringsperioden.	
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger - Databehandler afprøver, vurderer og evaluerer, hvorvidt effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har gennemgået og godkendt deres risikovurdering informationssikkerhedspolitik, og derigennem forholdt til om effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af dataansvarlig. Vi har på forespørgsel fået oplyst, at databehandlerens direktør har vurderet, at de organisatoriske og tekniske foranstaltninger stadig er tilfredsstillende.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

BDO Statsautoriseret revisionsaktieselskab, 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 1.700 medarbejdere, mens det verdensomspændende BDO-netværk har over 115.000 medarbejdere i 166 lande.

Copyright - BDO Statsautoriseret revisionsaktieselskab, cvr.nr. 20 22 26 70.

Penneo dokumentnøgle: 1A45G-3CZJJ-GEH68-8BM5B-DF6D5-I480K