AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. OKTOBER 2024 TIL 30. SEPTEMBER 2025 OM BESKRIVELSEN AF COMASYSTEM OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDS-FORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UD-FORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATA-BESKYTTELSESLOVEN

COMASYSTEM ApS

Denne dokumentnøgle: ADWD-UZJKO-PPQSX-A4SJ3-2QQ7K-WBEIJ

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING 2

2. COMASYSTEM APS UDTALELSE 5

3. COMASYSTEMS APS BESKRIVELSE AF COMASYSTEM 7

Indledning 7
Systembeskrivelse 7
Risikovurdering 8
Væsentlige ændringer i prioden 8
Tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige Kontroller 9
Komplementerende kontroller hos de dataansvarlige 15

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST 16

Risikovurdering 18
A.5: Informationssikkerhedspolitikker 19
A.7: Personalesikkerhed 20
A.8: Styring af aktiver 22
A.9: Adgangsstyring 23
A.10: Kryptografi 25
A.11: Fysisk sikring og miljøsikring 26
A.12: Driftssikkerhed 27
A.13: Kommunikationssikkerhed 30
A.14: Anskaffelse, udvikling og vedligeholdelse 31
A.15: Leverandørforhold 33
A.16: Styring af informationssikkerhedsbrud 36
A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring 38
A.18: Overensstemmelse 40

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. OKTOBER 2024 TIL 30. SEPTEMBER 2025 OM BESKRIVELSEN AF COMASYSTEM 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 COMAsystem ApS
COMAsystem ApS' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af COMAsystem ApS (databehandleren) for hele perioden fra 1. oktober 2024 til 30. september 2025 udarbejdede beskrivelse i sektion 3 af COMASYSTEM 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 Revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen 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: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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 COMASYSTEM 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 COMASYSTEM 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. oktober 2024 til 30. september 2025, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. oktober 2024 til 30. september 2025, 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. oktober 2024 til 30. september 2025.

Beskrivelse af test af kontroller

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

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens COMASYSTEM 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 10. november 2025

BDO Statsautoriseret Revisionspartnerselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

2. COMASYSTEM APS UDTALELSE

COMAsystem ApS varetager behandling af personoplysninger i forbindelse med COMASYSTEM 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 COMASYSTEM, 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.

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

COMAsystem ApS bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden fra 1. oktober 2024 til 30. september 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for COMASYSTEM, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer 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 COMASYSTEM 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.
2. Indeholder relevante oplysninger om ændringer i COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden fra 1. oktober 2024 til 30. september 2025.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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

COMAsystem ApS 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. oktober 2024 til 30. september 2025. Kriterierne anvendt for at give denne udtalelse var, at:

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

2. De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

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. oktober 2024 til 30. september 2025.

COMAsystem ApS 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.

København, den 10. november 2025

COMAsystem ApS

Christian Richter-Petersen
CEO

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

3. COMASYSTEM APS' BESKRIVELSE AF COMASYSTEM

INDLEDNING

Efterfølgende beskrivelse af COMAsystem er udfærdiget med det formål at kunne give retvisende oplysninger samt informationer til COMAsystem ApS' kunder og eksterne auditører.

Nedenstående forefindes en samlet beskrivelse af systemets anvendelse, formål og forhold i relation til systemets drift. Dernæst beskrives tilgangen og den løbende vedligeholdelse af risikovurderingen for systemet.

Beskrivelsen indeholder således også en gennemgang af de i organisationen implementerede kontroller for procedurer og dokumentation.

SYSTEMBESKRIVELSE

Generelt

COMASYSTEM er en Software as a Service (SaaS) webapplikation, der opbevarer og behandler kontraktdata for systemets brugere.

Anvendte kontrakttyper omfatter:

- Leverandørkontrakter
- Salgskontrakter
- Personalekontrakter
- Servicekontrakter

Systemet muliggør aktiv udnyttelse af relevante kontraktdata vha. notifikationer, der sendes til de ansvarlige brugere hos kunden.

Således sørger systemet for overholdelse af fornyelsesfrister, opsigelsesvarsler, overholdelse af forpligtelser i relation til personaler og styring af serviceaftaler.

Systemet er i den nuværende version udviklet med henblik på omfattende sikring af personhenførbare data iht. databeskyttelsesforordningens artikel 25 – "Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger".

Systemet anvendes dermed hos kunden til kontraktstyring, dokumentation ifm. compliance f.eks. ved behandling af persondata og økonomisk optimering.

Infrastruktur og drift

COMASYSTEM er hosted i Danmark, og backup opbevares ligeledes på forskellige lokationer i Danmark.

COMASYSTEM er placeret i Global Connect A/S' datacenter i Høje-Taastrup, Sjælland. Global Connect A/S varetager udelukkende housing-opgaver og optræder ikke som databehandler.

Den daglige drift af systemet, udviklingen og support gennemføres udelukkende af COMAsystem ApS.

COMAsystem er alene ansvarlig for udviklingen af applikationen.

Digital Signatur varetages af underleverandør ADDOsign twoday A/S, der fungerer som databehandler for kunder, som tilvælger digital underskrift.

Backup varetages af underleverandør Unit-IT ApS, der er databehandler.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Systemet overvåges 24/7 af COMAsystem ApS' egne medarbejdere. Derudover overvåges backuplokationer af Unit-IT ApS. Der anvendes en række eksterne systemer til overvågning og monitorering.

RISIKOVURDERING

Præmis for risikovurderingen
Risikovurderingen er udført under hensyntagen til de specifikke informationstyper som systemet behandler, mængden og følsomheden af de behandlede oplysninger.

Ligeledes vurderes systemets risiko under hensyntagen af den eller de trusler, der måtte være relevante for de brancher, som systemets kunder arbejder i.

Hændelser relateret til it eller persondatasikkerhed indgår i den løbende vurdering af risici.

Risikovurderingen er udført under antagelse af en hændelse i medfør af databeskyttelsesforordningens artikel 32, stk. 2.

Det antages i denne forbindelse, at systemet håndterer både almindelige og følsomme persondata.

Vurdering og opfølgning
Risikovurderingen er blevet foretaget systematisk igennem følgende hovedområder:

- Data (ind/ud)
- Brugere
- Hardware & Software
- Procedurer
- Generelle risici
- Underdatabehandlere
- Diverse hændelser af mere specifik karakter
    - Tiltag i fremtiden
    - DPIA
    - Opgavebestemte risikovurderinger knyttet til et specifikt projekt eller opgave

Risikovurderingen anvendes som et aktivt redskab og anses som en variabel, der skal revurderes løbende med hensyn til sikringen af, at COMASYSTEM drives og udvikles ift. det ønskede risikoniveau.

Til risikovurderingen anvendes materialer fra bl.a. Sikker Digital og andre relevante tilgængelige kilder, og der vurderes både på konsekvensen for virksomheden og for den eller de registrerede iht. databeskyttelsesforordningen.

Alle risici styres og holdes op imod processer og eller kontroller, hvor disse fremtræder i det af COMAsystem ApS' anvendte compliance system.

Der er gennemført risikovurderinger ift. både konsekvenser for virksomheden og den registrerede. Risikovurderingen bliver løbende revurderet, og der er processer på plads ifm. Udvikling og nye tiltag, som skal tilsikre at risikovurderingen ajourføres.

Der tages udgangspunkt i det nuværende trusselbillede, og risikovurderingen er en del af dokumentationen til den årlige ISAE 3000-revision. På baggrund af revisionens anbefalinger kan denne danne grundlag for nye projekter eller procedurer, der skal styrke sikkerheden for COMASYSTEM.

VÆSENTLIGE ÆNDRINGER I PRIODEN

Der er i perioden blevet udviklet og deployeret en feature der muliggør komplekse mappestrukturer til COMASYSTEM med et integreret modul til asset management.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

Generelt

Kontroller oprettes og gennemføres i Lexoforms iht. kontroller som vurderes relevante fra ISAE3000 katalog.

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
Risikovurdering	Risikovurdering	Artikel 28, stk. 3, litra c
A.5: Informationssikkerhedspolitikker	Politikker for informationssikkerhed og gennemgang af politikker for informationssikkerhed	Artikel 28, stk. 1
	Informationsikkerhedspolitikker i overensstemmelse med databehandleraftaler	Artikel 28, stk. 1
A.7: Personalesikkerhed	Rekruttering af medarbejdere - Screening	Artikel 28, stk. 1
	Rekruttering af medarbejdere - Tavsheds- og fortrolighedsaftale med medarbejdere	Artikel 28, stk. 1 og Artikel 28, stk. 3, litra b
	Awareness, uddannelse og træning vedrørende informationssikkerhed	Artikel 28, stk. 1
	Fratrædelse af medarbejdere - oplysning om fortrolighed og tavshedspligt	Artikel 28, stk. 1 og Artikel 28, stk. 3, litra b
	Fratrædelse af medarbejdere - inddragelse af adgangsrettigheder og aktiver	Artikel 28, stk. 1
A.8: Styring af aktiver	Fortegnelse over kategorier af behandlingsaktiviteter	Artikel 30, stk. 2, 3 og 4
	Reparation-, service- og destruktion af it-udstyr	Artikel 28, stk. 3, litra c
A.9: Adgangsstyring	Brugerregistrering og -afmelding og gennemgang af brugeradgangsrettigheder	Artikel 28, stk. 3, litra c
	Brug af hemmelig autentifikationsinformation	Artikel 28, stk. 3, litra c
	Procedure for sikkert log-on	Artikel 28, stk. 3, litra c
	Supporters adgang til personoplysninger	Artikel 28, stk. 1
A.10: Kryptografi	Kryptering ved transmission personoplysninger	Artikel 28, stk. 3, litra c
A.11: Fysisk sikring og miljøsikring	Fysisk adgangskontrol	Artikel 28, stk. 3, litra c
A.12: Driftssikkerhed	Vedligeholdelse af systemsoftware	Artikel 28, stk. 3, litra c
	Antivirusprogram	Artikel 28, stk. 3, litra c
	Sikkerhedskopiering og retablering af data	Artikel 28, stk. 3, litra c
	Logning	Artikel 28, stk. 3, litra c
	Overvågning af systemer og miljøer	Artikel 28, stk. 3, litra c
	Sårbarhedsscanning og penetrationstests	Artikel 28, stk. 3, litra c
A.13: Kommunikationssikkerhed	Netværkssikkerhed	Artikel 28, stk. 3, litra c
	Firewall	Artikel 28, stk. 3, litra c
	Fjernarbejdspladser og fjernadgang til systemer og data	Artikel 28, stk. 3, litra c
A.14: Anskaffelse, udvikling og vedligeholdelse	Ændringsstyring og privacy-by-design	Artikel 25
	Implementering af ændring i produktionsmiljøet	Artikel 25
	Adskillelse af udviklings-, test og produktionsmiljø	Artikel 25
	Adgang til kildekode	Artikel 25
	Anonymisering af personoplysninger i udviklingsopgaver	Artikel 25
A.15: Leverandørforhold	Underdatabehandleraftale og instruks	Artikel 28, stk. 2 og 4
	Godkendelse af underdatabehandlere	Artikel 28, stk. 2

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
	Ændringer i godkendte underdatabehandlere	Artikel 28, stk. 2
	Underdatabehandlerens forpligtelser	Artikel 28, stk. 2 og 4
	Oversigt over underdatabehandlere	Artikel 30, stk. 2
	Tilsyn med underdatabehandlere	Artikel 28, stk. 2 og 4
A.16: Styring af informationssikkerheds-brud	Underretning om brud på persondatasikkerheden	Artikel 33, stk. 2
	Rettidig underretning om brud på persondatasikkerhed	Artikel 33, stk. 2
	Identifikation af brud på persondatasikkerheden	Artikel 33, stk. 2
	Bistand til dataansvarlige ved brud på persondatasikkerhed	Artikel 33, stk. 2
A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring	Planlægning af informationssikkerhedskontinuitet	Artikel 28, stk. 3, litra c
	Implementering af informationssikkerhedskontinuitet	Artikel 28, stk. 3, litra c
	Verificering, gennemgang og evaluering af informationssikkerhedskontinuitet	Artikel 28, stk. 3, litra c
	Tilgængelighed af informationsbehandlingsfaciliteter	Artikel 28, stk. 3, litra c
A.18: OverensstemmelseA.15: Leverandørforhold	Procedure for behandling af personoplysninger	Artikel 28, stk. 3
	Efterlevelse af instruks for behandling af personoplysninger	Artikel 28, stk. 3. og Artikel 29 og Artikel 32, stk. 4
	Aftalte sikringsforanstaltninger	Artikel 28, stk. 3, litra c
	Underretning af den dataansvarlige ved ulovlig instruks	Artikel 28, stk. 3, litra h
	Procedure for opfyldelse af registreredes rettigheder	Artikel 28, stk. 3, litra e
	Tekniske foranstaltninger til opfyldelse af registreredes rettigheder	Artikel 28, stk. 3, litra e
	Sletning af oplysninger i overensstemmelse med dataansvarliges krav	Artikel 28, stk. 3, litra g
	Krav til opbevarings- og sletteperiode af oplysninger er i overensstemmelse med dataansvarliges krav	Artikel 28, stk. 3, litra g
	Sletning og tilbagelevering ved ophør af kundeforhold	Artikel 28, stk. 3, litra g
	Opbevaring af oplysninger er i overensstemmelse med dataansvarliges krav	Artikel 28, stk. 3, litra c
	Lokation for behandling og opbevaring af oplysninger	Artikel 28, stk. 3

Kontroller dokumenteres vha. aktiv stillingtagen fra den kontrollerende person og kan udføres når der er påført relevante kommentarer til gennemgangen.

Det er på denne måde hensigtens at skabe en ensartet og kontinuerlig oversigt samt historik over COMAsystem ApS' kontrolregime.

COMAsystem ApS har en aktiv holdning til det løbende kontrolregime og tilpasser kontroller løbende til ændrede processer eller funktioner samt tilføjer nye eller arkiverer unødvendige kontroller.

COMAsystem er opmærksom på den manglende funktionsadskillelse mellem den udførende og den kontrollerende part.

A.5 Informationssikkerhedspolitikker

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Der er implementeret en Informationssikkerhedspolitik i virksomheden, og den tages årligt til revision.

Iht. informationssikkerhedspolitikken står bestyrelsen med det overordnede ansvar for organiseringen af informationssikkerheden, og COMAsystem ApS' ledelse har defineret en informationssikkerhedsstrategi. Informationssikkerheden er udbredt i hele organisationen, og COMAsystem ApS stiller de samme krav til eksterne samarbejdspartnere.

A.7 Personalesikkerhed

Det tilsikres under ansættelsen af COMAsystem ApS' medarbejdere, at disse kan arbejde med fortroligt forhold og vurderes til at være i stand til at varetage driften og behandlingen af fortrolige samt følsomme data. Der er ligeledes procedurer, som tilsikrer en nedlukning af ophørte medarbejdere.

A.8 Styring af aktiver

IT-chefen er udpeget som virksomhedens systemejer og driftsansvarlige. Der er taget stilling til klassificeringen af systemer, og hvilke data der behandles. Der foreligger processer for beskyttelse af mobilt IT-udstyr samt server. På arbejdsstationer (mobilt udstyr) er der etableret diskkryptering. Databærende medier destrueres iht. godkendt procedure.

A.9 Adgangsstyring

I COMAsystem ApS er der indført procedurer for adgangsstyring på arbejdsstationer, systemer og netværk. Adgang til systemer og data baseres på den individuelle medarbejders funktion og mindst mulige niveau.

Adgang til kritiske drifts- og backend-systemer er beskyttet af firewall samt VPN, som er termineret i firewall.

For VPN-brugerne er der planlagt rotation af password iht. IT politikkens minimumskrav.

Bruger, der ikke længere har et funktionsmæssigt behov eller grundet samarbejdets ophør, fratages rettigheder og/eller adgang til dele af eller alle systemer.

Der er implementeret kontroller for at overvåge, at kun personer med funktionsmæssige behov har adgang til specifikke systemer.

Der forefindes ikke fælles brugerkonti og der udleveres personlige brugernavne plus koder. Hemmelige koder styres og opbevares krypteret.
Adgang til persondatabærende enheder og/eller kritiske systemer sker efter vurdering og ifm. arbejdsbetingede behov.

Der arbejdes med transmissionskryptering ved alle loginfunktioner.

A.10 Kryptografi

Der arbejdes målrettet med kryptografering ved både transmission af data og i visse tilfælde ved opbevaring af data.

For e-mail kommunikation er der opsat krav om TLS-kommunikation.

For adgang til webbaserede tjenester bliver TLS-kryptering påtvunget til minimum TLS 1.2.

Backup transmitteres krypteret og opbevares krypteret. Unit-IT har ikke adgang til krypteringsnøglen for COMAsystems backup data.

Kundernes filer er krypteret at rest.

A.11 Fysisk sikring og miljøsikring

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Der anvendes ekstern housing-løsning til COMAsystem ApS' datacenter, hvor der arbejdes med 24/7 overvågning og adgangsstyring.

Det er kun specifikke af COMAsystem ApS' medarbejdere med funktionsrelaterede behov, som har adgang til det fysiske materiel i datacentret. Det fysiske materiel omfatter server, switche, firewall etc. og er ejet af COMAsystem ApS.

Der forefindes procedure for sikker bortskaffelse og destruktion af databærende medier.

Hos COMAsystem ApS forefindes der alarmanlæg med alarmering. Der er processer på plads, således arbejdsstationer automatisk låser.

A.12 Driftssikkerhed

Der anvendes compliance-software til styring af processer, kontroller og tilhørende risikovurderinger. Der registreres hændelser efter bestemte processer og COMAsystem ApS gennemgår årligt alle registrerede hændelser ifm. procesoptimering.

Der er opsat proces og registrering for patch management for både arbejdsstationer og server.

Der anvendes drifts- / kapacitetsovervågning og alarmering på server.

På både arbejdsstationer og server anvendes centraliseret software til imødegåelse af vira og malware.

Der er taget stilling til backup ift. type, og hvilke data der skal tages backup af. Derudover er der også blevet vurderet, hvor ofte det er nødvendigt at gennemføre backup. Backup verificeres iht. løbende kontrol og ved anvendelse af systemets egne verifikationsindstillinger.

Logning er opsat på alle driftsenheder og opsamles centralt. Adgangen til logdata er begrænset til specifikke medarbejdere.

Change management registreres i hændelseslog, og det er udelukkende IT-chefen, der har beføjelse til installation og eller ændringer af nuværende software på driftsmaskiner. Medarbejdere, kan efter IT-chefens skøn, få tilladelse til installation af software på udleverede PCer og få tildelt lokale admin rettigheder.

COMAsystem ApS holder sig løbende ajour i åbne medier og professionelle netværk vedr. sårbarheder.

A.13 Kommunikationssikkerhed

Der er udfærdiget politikker til kommunikationssikkerhed. Det er udelukkende medarbejdere med arbejdsbetinget behov, som kan foretage rettelser i netværksudstyr.

Driftskritisk netværk kan kun tilgås via VPN.

Der eksponeres kun relevante og ønskede services til det åbne net.

Udover tvungen TLS på alt e-mail, så anvendes der en intern mailtjeneste for comasystem.dk, som kun benyttes af applikationen comasystem.dk.

A.14 Udvikling og vedligeholdelse af systemer

Der er fastlagte processer for igangsættelse af udvikling og retningslinjer for sikkerhedskrav til udvikling, anskaffelse og vedligeholdelse.

Der arbejdes med processer til overvågning og kontrol af underleverandører.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Iht. blandet andet databeskyttelsesforordningen revurderes evt. risici løbende, og også kravet om DPIA bliver løbende revurderet.

Der anvendes en ensartet Pipeline til udvikling, og nye systemfeatures dokumenteres.

Produktion og udvikling er adskilt, og der udvikles ikke på produktionsdata.

Der er fastlagt processer for opdatering og opgradering af virtuelle maskiner samt hypervisor og baremetal.

A.15 Leverandørforhold

Der er indgået databehandleraftaler med underleverandører og der er indhentet revisionserklæringer.

Der er ligeledes etableret fysisk kontrol af datacenters sikkerhed og omgivende forhold.

Der udføres tilsyn med primære leverandører på følgende måde:

GlobalConnect A/S (ikke databehandler):
Leverance: Datacenter housing

- Fysisk kontrol
- Årlig revurdering af revisionserklæring med særlig fokus på fysisk sikkerhed

Unit-IT ApS:
Leverance: Backup

- Funktionskontroller (særskilt under backup)
- Årlig revurdering af revisionserklæring med fokus på afvigelser ift. forhold, som gælder backup i transmission og under opbevaring

ADDOsign twoDay A/S:
Leverance: Digital signatur

- Årlig revurdering af revisionserklæring med fokus på afvigelser ift. forhold, som gælder backup i transmission og under opbevaring

A.16 Styring af informationssikkerhedsbrud

Grundlæggende anvendes forebyggende og opdagende kontroller, således brud på persondatasikkerheden kan afværges eller håndteres uden unødvendige ophold.

Der forefindes procedurer for håndtering af informationssikkerhedsbrud. Håndteringen omfatter registrering, risikovurdering, kommunikation og mitigering.

Medarbejdere og leverandører gøres løbende opmærksomme på hvordan informationssikkerhedsbrud skal håndteres.

Alle sikkerhedsbrud behandles også som hændelser under databeskyttelsesforordningen ifm. registrering, orientering og anmeldelse.

I langt til fleste tilfælde optræder COMAsystem ApS som databehandler på vegne af systemets kunder. Brud på persondatasikkerheden meddeles derfor straks til den eller de pågældende dataansvarlige.

Det præciseres herved, at COMAsystem ApS' kunder er selvstændige dataansvarlige ift. COMAsystem ApS og har ansvaret for egen risikovurdering af hændelser og anmeldelse til myndigheder samt underretninger af de registrerede.

A.17 Beredskabsplan

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

COMAsystem ApS har procedurer på plads, der har til opgave at tilsikre en opstart af mitigerende foranstaltninger uden unødige ophold i tilfælde af systemnedbrud eller anden hændelse, som gør COMASYSTEM utilgængeligt for brugere / kunder og COMAsystem ApS' medarbejdere, eller nedsætter systemets funktionsevne eller sikkerhed.

Derudover opfattes alle hændelser også som hændelser under databeskyttelsesforordningen og risikovurderes iht. denne.

CEO er som udgangspunkt den ansvarlige ift. alle hændelser og sørger for registrering, kommunikation, risikovurdering samt mitigering.

CCO overtager denne rolle i CEO´ens fravær.

Alle hændelser håndteres centralt i COMAsystem ApS' OPS board.

A.18 Overensstemmelse

Privatlivspolitik – er udarbejdet og vedligeholdes løbende igennem opsat kontrol. Politikken er tilgængelig for alle COMAsystem ApS' kunder og gæster på comasystem.dk/privatlivspolitik.

I forhold til awareness træning opererer COMAsystem ApS med en meget flad organisation, og der er opsat kontroller, som bidrager til gentagne diskussioner og vurderinger af virksomhedens forhold ift. persondata, og hvordan medarbejdere samt leverandører for COMAsystem ApS skal håndtere disse.

Databehandleraftaler med kunder bliver indgået ved indgåelse af aftale/kontrakt om leverance af COMASYSTEM software og skal underskrives inden, der gives adgang.
Databehandleraftalen er altid tilgængelig på https://comasystem.dk/dpa.

Databehandlerfortegnelse, opbevaring og vedligeholdelse heraf sker i COMAsystem samt filbaserede systemer. Fortegnelse, kontroller og risikovurdering dokumenteres og danner grundlag for den løbende dokumentation af de opstillede kontroller.

Efterlevelse af instrukser og underretning, hvis disse er i strid med lovgivningen, fastholdes ligeledes i OPS board, og der gennemføres løbende vurderinger igennem planlagte kontroller, så organisationen kan tilrettes.

Elektronisk opbevaring af databehandleraftaler for leverandører sker i COMAsystem og sammenholdes med de indhentede revisionserklæringer.

Sikring af, at underdatabehandlere lever op til kravene fra de dataansvarlige, sker gennem en ensartet databehandleraftale med COMAsystem ApS' kunder og et leverandørvalg, som understøtter den udarbejdede instruks omkring sikringsniveau og fysisk placering. Derudover risikovurderes databehandlerne ift. de funktioner, som disse udfører på vegne af COMAsystem ApS.

Konsekvensanalyse (DPIA) vurderes umiddelbart ikke nødvendigt at gennemføre pga. fravær af høj risiko for behandlingen, og idet behandlingen kun i mindre grad omfatter følsomme data. Der er opsat kontrol af, at behov for en DPIA for COMASYSTEM løbende revurderes.

Sletning af data sker både automatiseret i COMAsystem ApS' backup samt i automatiseret processer i applikationen, som den dataansvarlige selv har indflydelse på. Kundedata bliver slettet ved endt kundeforhold og er fastholdt i sletningsprocesserne. COMAsystem ApS opbevarer derudover kun data, som falder under anden lovgivning, som f.eks. bogføringsloven.

De registreredes rettigheder er beskrevet i procedurer for COMAsystem ApS. Det er dog sådan, at den enkelte kunde som dataansvarlige selv skal udtrække, rette eller slette egne data ift. anmodning efter databeskyttelsesforordningens artikel 15 – 20 samt artikel 7 vedr. samtykke. COMAsystem ApS vil i alle tilfælde assistere den dataansvarlige efter anmodning, og disse anmodninger vil blive registreret i hændelsesloggen for COMAsystem ApS.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Revision og inspektion udføres årligt og på egen foranledning af COMAsystem ApS. COMAsystem ApS ønsker via en ekstern revision af typen ISAE 3000 at synliggøre virksomhedens fokus på og evner til at kunne arbejde sikkert og på en professionel måde med kundernes data.

Bistand til den dataansvarlige ydes til den dataansvarlige, og de nærmere forhold fremgår af databehandleraftalen.

Der er opsat kontroller, som varetager sikringen og dokumentationen af forandringer, fjernelse eller tilføjelse af forretningsprocesserne i COMAsystem ApS. Kontrollen bliver gennemført under hensyntagen til risikovurderingen, som tager udgangspunkt i konsekvensen for de registrerede.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Det henstilles til de dataansvarlige, som COMAsystem ApS er databehandler for, at overholde følgende:

- Tilsikre egne processer til sikring af de registreredes rettigheder for de persondata, som lægges i COMASYSTEM.
- Tilsikre en tilstrækkelig vurdering af den afgivne instruks i databehandleraftalen.
- Udarbejde egne risikovurderinger for indhentning, anvendelse og opbevaring af persondata.
- Benyt de i COMASYSTEM udlagte funktioner til sletning af persondata uden formål eller manglende lovhjemmel.
- Tilsikre en brugeradministration af egne brugere i COMAsystem, så fratrådte og opsagte medarbejder ikke længere har adgang til systemet.
- Tilsikre i brugeradministrationen, at der drages omhyggeligt omsorg med tildelingen af rettigheder i COMASYSTEM.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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 COMAsystem ApS' beskrivelse af COMASYSTEM 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 COMAsystem ApS, 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. oktober 2024 til 30 september 2025.

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

For de ydelser, der leveres af Global Connect A/S som serviceunderleverandør inden for housing af it-udstyr, har vi fra uafhængig revisor modtaget en ISAE 3402 type 2-erklæring for perioden fra 1. januar til 31. december 2024 om beskrivelsen af kontroller, deres udformning og funktionalitet i tilknytning til datacenterløsning.

Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i databehandlerens beskrivelse af COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene vurderet erklæringen og testet de kontroller hos databehandleren, der overvåger funktionaliteten af serviceunderleverandørens kontroller.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

For de ydelser, der leveres af Unit IT A/S som underdatabehandler inden for drift af it, har vi fra uafhængig revisor modtaget en ISAE 3402 og ISAE 3000 type 2-erklæring for perioden fra 1. januar 2024 til 31. december 2024 vedrørende afdækning af de tekniske og organisatoriske sikringsforanstaltninger i tilknytning til driften af Cloud backup-ydelser.

For de ydelser, der leveres af Twoday A/S som underdatabehandler inden for digital underskrift, har vi fra uafhængig revisor modtaget en ISAE 3402 og ISAE 3000 type 2-erklæring for perioden fra 1. april 2024 til 31. marts 2025 om overensstemmelse med databeskyttelseslovgivningen som databehandler.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i COMAsystem ApS beskrivelse af COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos COMAsystem ApS, 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: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Risikovurdering		
Kontrolmål ▶ *At sikre, at databehandleren udfører en årlig risikovurdering i forhold til konsekvenserne for de registrerede, der danner grundlag for de tekniske og organisatoriske sikkerhedsforanstaltninger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret databehandlerens system for risikostyring og politikker for risikostyring. Vi har observeret, at risikovurderingen er udarbejdet med afsæt i fortrolighed, integritet og tilgængelighed for den registrerede. Vi er ved forespørgsel blevet oplyst, at risikovurdering opdateres løbende og mindst én gang årligt. Vi har observeret, at risikovurderingen er opdateret i revisionsperioden. Vi har observeret, at identificerede risici registreres og opdateres i databehandlerens risikolog.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.5: Informationssikkerhedspolitikker

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politikker for informationssikkerhed og gennemgang af politikker for informationssikkerhed - Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. - Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at ansvars- og gyldighedsområde er defineret. Vi har observeret, at politikker omfatter behandling af persondata. Vi har observeret, at informationssikkerhedspolitikken er opdateret og godkendt af ledelsen den 29. september 2025.	Ingen afvigelser konstateret
Informationsikkerhedspolitikker i overensstemmelse med databehandleraftaler - Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevist inspiceret i databehandleraftaler, at kravene i aftalerne ikke er modstridende med informationssikkerhedspolitikken.	Ingen afvigelser konstateret

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.7: Personalesikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Rekruttering af medarbejdere - Screening ▶ Databehandleren udfører screening og baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer udførsel af screening og baggrundstjek af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har stikprøvevist inspiceret, at databehandleren har udført efterprøvning af kandidater inden ansættelse, og at efterprøvningerne har omfattet relevant dokumentation.	Ingen afvigelser konstateret.
Rekruttering af medarbejdere - Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Ved ansættelse underskriver medarbejdere en fortrolighedsaftale eller på anden måde har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevist for ansatte i erklæringsperioden inspiceret, at de pågældende medarbejdere har underskrevet krav til tavshedspligt i ansættelseskontrakten.	Ingen afvigelser konstateret.
Awareness, uddannelse og træning vedrørende informationssikkerhed ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. ▶ Databehandleren foretager løbende awareness, træning og uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren afholder introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. Vi har inspiceret, at databehandleren foretager løbende awareness, træning og uddannelse af medarbejdere omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.7: Personalesikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fratrædelse af medarbejdere - oplysning om fortrolighed og tavshedspligt ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevist for fratrådte medarbejder i erklæringsperioden inspiceret, at databehandleren har orienteret de fratrådte medarbejdere om, at den pålagte tavshedspligt fortsat er gældende efter ansættelsesophør.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere - inddragelse af adgangsrettigheder og aktiver ▶ Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker for personalesikkerhed ved fratrædelse, herunder retningslinjer for tilbagelevering af informationsaktiver og fjernelse af rettigheder i systemer. Vi har stikprøvevist inspiceret for fratrådte medarbejdere i erklæringsperioden inspiceret dokumentation for tilbagelevering af informationsaktiver, nedlukning af adgange er foretaget for den pågældende medarbejder.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.8: Styring af aktiver

Kontrolmål

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf – GDPR, artikel 30, stk. 2, 3 og 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 kategorier af behandlingsaktiviteter som databehandler. Fortegnelsen skal indeholde: • navn og kontaktoplysninger for dataansvarlige, • de kategorier af behandling, der foretages på vegne af dataansvarlige, • navn og kontaktoplysninger for hver underdatabehandler, • angivelse af eventuel overførsel af personoplysninger til et tredjeland. ▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev. ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandlerens fortegnelse over kategorier af behandlingsaktiviteter som databehandler og observeret, at den, indeholder relevante oplysninger, samt at fortegnelsen bliver opbevaret elektronisk. Vi har på forespørgsel blevet oplyst, at Datatilsynet ikke har anmodet om udlevering af fortegnelsen.	Vi har konstateret, at Datatilsynet ikke ved erklæringstidspunktet har anmodet om udlevering af fortegnelsen. Vi har derfor ikke kunnet teste implementering af denne del af kontrollen. Ingen afvigelser konstateret.
Reparation-, service- og destruktion af it-udstyr ▶ Databehandleren har etableret en procedure for reparation-, service- og destruktion af it-udstyr, der sikrer sikker håndtering af it-udstyr indeholdende personoplysninger. ▶ Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger. ▶ Databehandleren bortskaffer it-udstyr ved fysisk destruktion af databærende medier eller foretager sikker sletning af data på databærende medier.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har formaliserede procedurer for reparation-, service- og destruktion af it-udstyr. Vi har på forespørgsel fået oplyst, at der ikke har været sendt it-udstyr til reparation-, service- eller destruktion i erklæringsperioden.	Vi har konstateret, at databehandleren ikke har sendt it-udstyr til reparation-, service- eller destruktion. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.9: Adgangsstyring

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Brugerregistrering og -afmelding og gennemgang af brugeradgangsrettigheder ▶ Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret og sker ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. ▶ Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker for adgangsstyring. Vi har ved forespørgsel fået bekræftet, at oprettelse af brugere sker ved indgåelse af kontrakt med medarbejder. Vi har observeret, at privilegerede adgange til systemer og adgange tildeles ud fra et arbejdsbetinget behov. Vi har inspiceret procedure for gennemgang af brugerrettigheder. Vi har observeret, at der sker gennemgang af rettigheder for kritiske driftssystemer og adgang til personoplysninger. Vi har observeret, at kontrollen er gennemført den 29. november og 29. december 2024.	Ingen afvigelser konstateret.
Brug af hemmelig autentifikationsinformation ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger sker gennem VPN og adgangskoder, der afspejler risikoen ved behandlingsaktiviteten.	Ingen afvigelser konstateret.
Procedure for sikkert log-on ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.9: Adgangsstyring

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder anvendelsen VPN med privat certifikat og adgangskode.	
Supporters adgang til personoplysninger ▶ Databehandleren har etableret procedure for supporters adgang til personoplysninger, der sikrer, at supporters adgange og håndtering af personoplysninger ved supportopgaver sker ud fra support tickets og supporterens arbejdsbetingede behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at der er etableret procedurer, der sikrer, at supporters adgange og håndtering af personoplysninger ved supportopgaver sker ud fra support tickets og supporterens arbejdsbetingede behov. Vi har stikprøvevist inspiceret supportsager og observeret, at disse følger proceduren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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
Kryptering ved transmission personoplysninger ▶ Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til databehandlerens datacentre. Vi har inspiceret adgangsliste for personer med adgang til databehandlerens udstyr i datacenter. Alene CEO og senior developer er tildelt adgang. Vi har observeret, at ledelsen har foretaget gennemgang af adgangsloggen, hvor den seneste gennemgang var den 13. juli 2025. Vi er på forespørgsel blevet oplyst, at databehandlerens personoplysninger bliver opbevaret hos hostingleverandør Global Connect. Vi har inspiceret hostingleverandør Global Connect's revisionserklæring og observeret, at erklæringen er uden forbehold og, at erklæringen ikke indeholder forhold omkring fysisk adgangssikkerhed, som har krævet yderligere handlinger fra databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter – GDPR, 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 28, stk. 3, litra c*
- *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.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Vedligeholdelse af systemsoftware ▶ Ændringer til systemer, arbejdsstationer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at der er udformet procedure for opdatering af operativsystemer og databaser. Vi har for en stikprøve inspiceret dokumentation for opdatering. Vi har observeret, at der er gennemført opdatering af driftssystemer.	Ingen afvigelser konstateret.
Antivirusprogram ▶ Der er for de arbejdsstationer og systemer, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for en stikprøve inspiceret arbejdsstationer. Vi har observeret, at der er installeret antivirus-software. Vi har ligeledes observeret, at software er opdateret.	Ingen afvigelser konstateret.
Sikkerhedskopiering og retablering af data ▶ Databehandleren har etableret en procedure for sikkerhedskopiering og reetablering af data og systemer, der sikrer, at relevante systemer og data sikkerhedskopieres og opbevares på anden fysisk lokation, samt at systemer og data kan reetableres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der skal sikre sikkerhedskopiering og reetablering af relevante data og systemer, og at sikkerhedskopier opbevares på anden fysisk lokation. Vi har inspiceret systemkonfiguration for sikkerhedskopiering. Vi har observeret, at der foretages sikkerhedskopiering af driftskritiske systemer og servere. Vi har observeret, at der foretages sikkerhedskopiering hver time.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter – GDPR, 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 28, stk. 3, litra c*
- *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.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret system for dokumentation af kontroller. Vi har for en stikprøve observeret, at der foretages ugentlig kontrol af korrekt sikkerhedskopiering. Vi har observeret, at der sendes notifikation til driftsansvarlig ved afvigelser i sikkerhedskopiering. Vi har inspiceret, at sikkerhedskopier har været genetableret.	
Logning ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges. ▶ Databehandler monitorerer og logger netværkstrafik. ▶ Sikkerhedshændelser omfattende: • Ændringer i logopsætninger, herunder deaktivering af logning • Ændringer i systemrettigheder til brugere • Fejlede forsøg på log-on til systemer, databaser og netværk • Bruteforce ▶ Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Vi har for en stikprøve inspiceret, at der løbende foretages gennemgang af logs og overvågning. Vi har inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen afvigelser konstateret.
Overvågning af systemer og miljøer	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter – GDPR, 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 28, stk. 3, litra c*
- *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.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • CPU-load • Ram-brug • Uptime/ downtime	Vi har inspiceret system for kapacitetsovervågning. Vi har for en stikprøve observeret, at der foretages overvågning af servere og systemer for kapacitets overvågning. Vi har inspiceret dokumentation for at beskeder med alarmer modtages, og at der sker opfølgning herpå.	
Sårbarhedsscanning og penetrationstests ▶ De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests. ▶ Databehandleren gennemgår rapporten og håndterer konstaterede svagheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren modtager ugentlige rapportere fra Sophos med information om trusselsdetektioner og hændelser. Vi har observeret, at databehandleren har foretaget pentest. Vi har foretaget inspektion af rapporten og konstateret at der kun er fundet mindre sårbarheder som ikke vurderes nødvendige at håndtere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.13: Kommunikationssikkerhed

Kontrolmål

- *At sikre beskyttelse af informationer og personoplysninger i netværk og af understøttende informationsbehandlingsfaciliteter – GDPR, artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Netværkssikkerhed ▶ Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret systemkonfiguration for firewall. Vi har observeret, at der er implementeret trafikfiltrering for adgang til servere.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall korrekt efter best-practice standard. ▶ Databehandler anvender kun services/porte, som de har behov for.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem firewall. Vi har inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen afvigelser konstateret.
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker via VPN-forbindelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at der kun kan opnås fjernadgang til systemer og data via VPN. Vi har observeret, at der er konfigureret kryptering af VPN-forbindelse. Vi har observeret, at VPN-klient autentificeres vha. certifikat samt unik bruger-id og password.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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
Ændringsstyring og privacy-by-design ▶ Databehandleren har etableret en procedure for udviklings- og ændringsopgaver, der sikrer overholdelse af privacy-by-design-principperne, samt at alle udviklings- og ændringsopgaver følger en formaliseret proces, der sikrer test og krav om godkendelse inden implementering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret politikker og procedurebeskrivelser. Vi har observeret, at der er opsat krav til overholdelse af privacy by default og privacy by design. Vi har endvidere observeret, at der ved opstart af projekter foretages vurdering af projektets påvirkning i forhold til persondata. Vi har stikprøvevis observeret, at der gennemføres automatiseret test af kildekode før installation i driftsmiljø.	Ingen afvigelser konstateret.
Implementering af ændring i produktionsmiljøet ▶ Databehandleren har etableret en procedure for implementering af ændringer i produktionsmiljøet, der sikrer funktionsadskillelse i implementeringsprocessen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der ikke er opsat logistik funktionsadskillelse. Vi har dog konstateret, at der er defineret interne retningslinjer vedrørende implementering af ændringer i driftsmiljø. Vi har endvidere konstateret, at CEO bliver notificeret, når der sendes ny kildekode til driftsmiljø, før dette bliver deployet.	Ingen afvigelser konstateret.
Adskillelse af udviklings-, test og produktionsmiljø ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionsmiljøer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret produktions- og testmiljø. Vi har observeret, at der er adskillelse mellem test- og produktionsmiljø. Vi har observeret, at test og udvikling sker på separate servere.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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
Adgang til kildekode ▶ Kildekode er beskyttet mod uautoriseret ændring og sletning.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at det kun er databehandlerens udviklere og CEO, der har adgang til kildekode. Vi har inspiceret dokumentation for, at kildekoden er beskyttet mod uautoriseret ændring og sletning.	Ingen afvigelser konstateret.
Anonymisering af personoplysninger i udviklingsopgaver ▶ Der anvendes anonymiseret testdata i udviklings- og testmiljø.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databaser i udviklings- og testmiljø. Vi har observeret, at data i tabeller er anonymiseret.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.15: Leverandørforhold		
Kontrolmål ▶ *At sikre beskyttelse af organisationens aktiver og personoplysninger, som leverandører har adgang til – GDPR, artikel 28, stk. 2 og 4.* ▶ *At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne – GDPR, artikel 28, stk. 2 og 4.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at procedurerne er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har stikprøvevist inspiceret på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerenes databehandling fremgår af indgåede databehandleraftaler med en dataansvarlige.	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere ▶ Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Vi har inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i overensstemmelse med indgåede databehandleraftaler.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.15: Leverandørforhold

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandlerens forpligtelser ▶ Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er indgået databehandleraftaler med anvendte underdatabehandlere, Vi har stikprøvevist inspiceret på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
Oversigt over underdatabehandlere ▶ Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Vi har inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ▶ Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. ▶ Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Vi har inspiceret, at databehandleren har udført tilsyn, herunder indhentet og gennemgået underdatabehandlers revisorerklæringer, certificeringer og lignende.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.15: Leverandørforhold

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at databehandlerens tilsyn af underdatabehandlere ikke har givet anledning til yderligere handlinger, hvorfor de dataansvarlige ikke er blevet orienteret om opfølgningen.	

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.16: Styring af informationssikkerhedsbrud

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underretning om brud på persondatasikkerheden ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret og godkendt i erklæringsperioden. Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har inspiceret dokumentation for hændelser. Vi har observeret, at der i perioden er indrapporteret informationssikkerhedshændelser, men ikke brud på persondatasikkerheden. Vi har ligeledes observeret, at hændelserne er mitigeret.	Ingen afvigelser konstateret.
Rettidig underretning om brud på persondatasikkerhed ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at der ikke har været konstateret hændelser, som har medført brud på persondatasikkerheden i erklæringsperioden.	Vi har konstateret, at der ikke har været konstateret hændelser, som har medført brud på persondatasikkerheden. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har opsat foranstaltninger til at identificere brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Vi har inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer mv.	Ingen afvigelser konstateret.
Bistand til dataansvarlige ved brud på persondatasikkerhed ▶ Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Vi har observeret, at der ikke har været konstateret hændelser, som har medført brud på persondatasikkerheden i erklæringsperioden.	Vi har konstateret, at der ikke har været konstateret hændelser, som har medført brud på persondatasikkerheden. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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**
Planlægning af informationssikkerhedskontinuitet ▶ Der er på baggrund af risikovurdering etableret en plan for informationssikkerhedskontinuitet.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret beredskabsplan. Vi har observeret, at der er udformet og implementeret beredskabsplan ud fra en risikovurdering for drift af informationsaktiver. Vi har observeret, at beredskabsplanen er revideret i september 2025.	Ingen afvigelser konstateret.
Implementering af informationssikkerhedskontinuitet ▶ Organisations- og ledelsesstruktur under nødberedskab er specificeret i procedure for nød-, beredskabs- og reetableringsstyring. ▶ Der er udarbejdet en overordnet beredskabsplan, der beskriver den overordnede procedure for iværksættelse af beredskab og organisering af beredskab. ▶ Roller og ansvar i forbindelse med aktivering af beredskab er kommunikeret til relevante personer; herunder information om placering af nødvendige beskrivelser og information. ▶ Der er udarbejdet procedure og arbejdsbeskrivelser for reetablering af driftskritiske systemer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret beredskabsplaner. Vi har observeret, at ledelsesstruktur er specificeret i beredskabsplan. Vi har observeret, at der er udarbejdet en overordnet beredskabsplan med procedure for iværksættelse og organisering af beredskab. Vi har ligeledes observeret, at roller og ansvar i forbindelse med beredskab er fastlagt og kommunikeret til relevante medarbejdere. Vi har observeret, at der er udarbejdet en arbejdsbeskrivelse for trinvis reetablering af driftssystemer.	Ingen afvigelser konstateret.
Verificering, gennemgang og evaluering af informationssikkerhedskontinuitet ▶ Beredskabsplaner revideres en gang årligt ved implementering af nye systemer eller ændringer i risikovurderingen. ▶ Beredskabsplaner afprøves efter en fastlagt rotationsplan. Afprøvning af beredskabsplaner er planlagt i årshjul.	Vi har udført forespørgsler hos passende personale. Vi har observeret, at der er udformet og implementeret beredskabsplan ud fra en risikovurdering for drift af informationsaktiver.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

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
	Vi har observeret, at beredskabsplanen er revideret i september 2025. Vi har inspiceret dokumentation for afprøvning af beredskabsplan ved en konkret situation og observeret, at beredskabsplanen har været fulgt den 18. juli 2025.	
Tilgængelighed af informationsbehandlingsfaciliteter ▶ Driftskritiske systemer er virtualiseret, når muligt. ▶ Beredskabsplaner opbevares på flere fysiske lokationer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret oversigt over virtualiserede servere. Vi har observeret, at databehandlerens systemer er virtualiseret, når muligt. Vi har inspiceret system for opbevaring af dokumentation. Vi har observeret, at beredskabsplaner er opbevaret i filsystem. Vi har ligeledes observeret, at beredskabsplanen opbevares i fysisk udskrift på kontoret.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Procedure for behandling af personoplysninger ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandleraftale og politikker. Vi har observeret, at der er udformet procedure, der skal sikre, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at proceduren er opdateret og ledelsesgodkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon til indgåelse af databehandleraftaler med dataansvarlig og stikprøvevist udvalgt indgåede databehandleraftale med en dataansvarlige og observeret, at databehandleraftalen indeholder instruks Vi har inspiceret databehandlerens fortegnelse over behandlingsaktiviteter og stikprøvevist inspiceret, at behandlingen foregår i overensstemmelse med instruks fra dataansvarlig.	Ingen afvigelser konstateret.
Aftalte sikringsforanstaltninger ▶ Databehandleren har implementerer de aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for en stikprøve observeret, at databehandleren har implementeret de aftalte sikkerhedsforanstaltninger. Vi har inspiceret, at procedurer er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivning.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon til indgåelse af databehandleraftaler med dataansvarlig og stikprøvevist udvalgt indgåede databehandleraftale med en dataansvarlige og observeret, at databehandleren er forpligtet til at underrette den dataansvarlige i tilfælde, hvor en instruks vurderes at være i strid med lovgivning. Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde i erklæringsperioden, hvor instruks har været vurderet i strid med lovgivning.	Vi har konstateret, at der ikke har været tilfælde, hvor instruks har været vurderet i strid med lovgivning. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.
Procedure for opfyldelse af registreredes rettigheder ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandleraftale og politikker. Vi har observeret, at der er udformet procedurer for bistand til den dataansvarlige i relation til den registreredes rettigheder. Vi har inspiceret, at procedurerne er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Tekniske foranstaltninger til opfyldelse af registreredes rettigheder ▶ Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger	Vi har konstateret, at der ikke er sket anmodning om bistand i forhold til de registreredes rettigheder. Vi har derfor ikke kunne teste kontrollens implementering Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.18: Overensstemmelse		
Kontrolmål ▶ *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	• Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har på forespørgsel fået oplyst, at der ikke er sket anmodning om bistand i forhold til de registreredes rettigheder i erklæringsperioden.	
Sletning af oplysninger i overensstemmelse med dataansvarliges krav ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Krav til opbevarings- og sletteperiode af oplysninger er i overensstemmelse med dataansvarliges krav ▶ Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Backup opbevares i 180 dage	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning af personoplysninger indeholder specifikke krav til databehandlerens opbevaringsperioder og sletterutiner, samt observeret at databehandleren foretager ugentlige kontrol for sletning af data. Vi har observeret, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Vi har stikprøvevist inspiceret at databehandleren har kontrolleret at data slettes i overensstemmelse med de aftalte opbevaringsperioder.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sletning og tilbagelevering ved ophør af kundeforhold ▶ Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure og politikker for sletning og tilbagelevering af data til dataansvarlige. Vi har observeret, at der er udarbejdet procedure for sletning af data ved ophør af kundeforhold. Vi er blevet oplyst at der er foretaget tilbagelevering af data til dataansvarlig. Vi har observeret at tilbagelevering blev afviklet med dataansvarlige i overensstemmelse med proceduren. Vi har på forespørgsel fået oplyst, at der ikke har været ophør af databehandleraftaler i erklæringsperioden.	Ingen afvigelser konstateret.
Opbevaring af oplysninger er i overensstemmelse med dataansvarliges krav ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret log for sletning og foretaget inspektion af databaser for registrering af personoplysninger. Vi har observeret, at der er foretaget sletning af personoplysninger i henhold til procedure. Vi har inspiceret, at procedurerne er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Lokation for behandling og opbevaring af oplysninger ▶ Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav – GDPR, artikel 28, stk. 3, artikel 28, stk. 3, litra a og g og artikel 44 - 49.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder for behandling og opbevaring af personoplysninger. Vi har stikprøvevist inspiceret på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingerne, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

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

Copyright - BDO Statsautoriseret Revisionspartnerselskab, cvr.nr. 45719375.

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

PENNEO

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

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

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 77.243.xxx.xxx
2025-11-10 11:22:28 UTC

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner, Chef for Risk Assurance
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 77.243.xxx.xxx
2025-11-10 11:56:46 UTC

Christian Richter-Pedersen
CEO
På vegne af: COMAsystem
Serienummer: 4328a6a0-06b4-412e-a452-4a418642d03e
IP: 87.116.xxx.xxx
2025-11-10 18:36:13 UTC

Penneo dokumentnøgle: ADMDI-UZPIQ-RDZ3X-P5JT3-Q57KQ-M5CBJ

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptofrafiske beviser er indlejret i denne PDF for validering i fremtiden.

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

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

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