AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 5. DECEMBER 2025 OM BESKRIVELSEN AF KOMMUNEPLATFORMEN OG PUBLICPLATFORMEN OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Cabana ApS

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING 2

2. CABANA APS' UDTALELSE 4

3. CABANAS BESKRIVELSE AF KOMMUNEPLATFORMEN OG PUBLICPLATFORMEN 6

Cabana aps 6

Kommuneplatformen og Publicplatformen og behandling af personoplysninger 6

Styring af persondatasikkerhed 6

Risikovurdering 8

Tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller 8

Komplementerende kontroller hos de dataansvarlige 12

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST 13

Kontrolområde A 15

Kontrolområde B 17

Kontrolområde C 24

Kontrolområde D 28

Kontrolområde E 30

Kontrolområde F 31

Kontrolområde H 34

Kontrolområde I 35

Kontrolområde J 37

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 5. DECEMBER 2025 OM BESKRIVELSEN AF KOMMUNEPLATFORMEN OG PUBLICPLATFORMEN OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Cabana ApS
Cabana ApS' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Cabana ApS (databehandleren) pr. 5. december 2025 udarbejdede beskrivelse i sektion 3 af Kommuneplatformen og Publicplatformen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

Databehandlerens ansvar

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

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for 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 af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

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

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

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

Begrænsninger i kontroller hos en databehandler

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

Konklusion

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

a. at beskrivelsen af Kommuneplatformen og Publicplatformen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 5. december 2025, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 5. december 2025.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt Kommuneplatformen og Publicplatformen, 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 9. december 2025

BDO Statsautoriseret revisionspartnerselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. CABANA APS' UDTALELSE

Cabana ApS varetager behandling af personoplysninger i forbindelse med Kommuneplatformen og Publicplatformen 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 Kommuneplatformen og Publicplatformen, 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.

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

Cabana bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af Kommuneplatformen og Publicplatformen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 5. december 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

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

cabana

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

Cabana 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 pr. 5. december 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.

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

Frederiksberg, den 9. december 2025

Cabana ApS

Thomas Vorgaard
Direktør

3. CABANAS BESKRIVELSE AF KOMMUNEPLATFORMEN OG PUBLICPLATFORMEN

CABANA APS

Cabana ApS er en danskejet virksomhed, der udvikler og driver en række online systemer til såvel kommuner som forskellige brancher på det private marked. Cabana har kontorer på Frederiksberg Allé 41B, 1820 Frederiksberg C.

Cabanas ca. 15 medarbejdere er specialiserede inden for systemudvikling, serverdrift, support og informationssikkerhed, og organiseret i en udviklingsafdeling, drift- og supportafdeling, økonomiafdeling og en administrationsafdeling.

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

KOMMUNEPLATFORMEN OG PUBLICPLATFORMEN OG BEHANDLING AF PERSONOPLYSNINGER

Cabana leverer Kommuneplatformen og PublicPlatform som en Software-as-a-Service (SaaS) løsning i henhold til indgået kontrakt med kommuner, offentlige organisationer og private virksomheder. Cabanas platform består af en CMS-system til styring af indhold.

Cabanas platforme udvikles i Danmark, og hostes via Cabanas underleverandør med hosting-center på dansk grund. Der benyttes pt. Ikke andre underdatabehandlere til udvikling eller afvikling af Cabanas platforme. Cabana har indgået databehandleraftaler med underdatabehandlere.

Cabana behandler personoplysninger på vegne af sine kunder, der er dataansvarlige, når disse anvender Cabanas platforme. Cabana har indgået databehandleraftaler med de dataansvarlige om denne behandling.

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

STYRING AF PERSONDATASIKKERHED

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

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

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

KONTROLOMRÅDE	UNDERKONTROLOMRÅDE	GDPR-ARTIKEL
A - Behandling af personoplysninger på vegne af dataansvarliges instruks	A.1 - Procedure for behandling af personoplysninger	Artikel 28, stk. 3
	A.2 - Efterlevelse af instruks for behandling af personoplysninger	Artikel 28, stk. 3. og Artikel 29 og Artikel 32, stk. 4
	A.3 - Underretning af dataansvarlig ved ulovlig instruks	Artikel 28, stk. 3, litra h

KONTROLOMRÅDE	UNDERKONTROLOMRÅDE	GDPR-ARTIKEL
	A.4 - Fortegnelse over behandlingsaktiviteter	Artikel 30, stk. 2, 3 og 4
B - Tekniske foranstaltninger	B.1 - Aftalte sikringsforanstaltninger	Artikel 28, stk. 3, litra c
	B.2 - Risikovurdering	Artikel 28, stk. 3, litra c
	B.3 - Antivirus	Artikel 28, stk. 3, litra c
	B.6 - Adgangsstyring - adgang til personoplysninger	Artikel 28, stk. 3, litra c
	B.7 - Overvågning af systemer og miljøer	Artikel 28, stk. 3, litra c
	B.8 - Kryptering ved transmission personoplysninger	Artikel 28, stk. 3, litra c
	B.9 - Logning	Artikel 28, stk. 3, litra c
	B.10 - Anonymisering af personoplysninger i udviklingsopgaver	Artikel 28, stk. 3, litra c
	B.11 - Sårbarhedsscanninger og penetrationstests	Artikel 28, stk. 3, litra c
	B.12 - Vedligeholdelse af systemsoftware	Artikel 28, stk. 3, litra c
	B.13 - Adgangsstyring - procedure og periodisk gennemgang	Artikel 28, stk. 3, litra c
	B.14 - Logisk adgangskontrol	Artikel 28, stk. 3, litra c
	B.15 - Fysisk adgangskontrol	Artikel 28, stk. 3, litra c
	B.16 - Sikkerhedskopiering og reetablering	Artikel 28, stk. 3, litra c
	B.17 - Fjernarbejdspladser og fjernadgang til systemer og data	Artikel 28, stk. 3, litra c
C - Organisatoriske foranstaltninger	C.1 - Politikker for informationssikkerhed og gennemgang af politikker for informationssikkerhed	Artikel 28, stk. 1
	C.2 - Informationsikkerhedspolitikker i overensstemmelse med databehandleraftaler	Artikel 28, stk. 1
	C.3 - Rekruttering af medarbejdere - Screening	Artikel 28, stk. 1
	C.4 - Rekruttering af medarbejdere - Tavsheds- og fortrolighedsaftale med medarbejdere og introduktion til informationssikkerhed	Artikel 28, stk. 1 og Artikel 28, stk. 3, litra b
	C.5 - Fratrædelse af medarbejdere - inddragelse af adgangsrettigheder og aktiver	Artikel 28, stk. 1
	C.6 - Fratrædelse af medarbejdere - oplysning om fortrolighed og tavshedspligt	Artikel 28, stk. 1 og Artikel 28, stk. 3, litra b
	C.7 - Awareness, uddannelse og træning vedrørende informationssikkerhed	Artikel 28, stk. 1
	C.8 - Supporters adgang til personoplysninger	Artikel 28, stk. 1
	C.9 - Reparation-, service- og destruktion af it-udstyr	Artikel 28, stk. 3, litra c
D - Sletning af personoplysninger	D.1 - Sletning af oplysninger i overensstemmelse med dataansvarliges krav	Artikel 28, stk. 3, litra g
	D.2 - Krav til opbevarings- og sletteperiode af oplysninger er i overensstemmelse med dataansvarliges krav	Artikel 28, stk. 3, litra g
	D.3 - Sletning og tilbagelevering ved ophør af kundeforhold	Artikel 28, stk. 3, litra g
E - Opbevaring af personoplysninger	E.1 - Opbevaring af oplysninger er i overensstemmelse med dataansvarliges krav	Artikel 28, stk. 3, litra c
	E.2 - Lokation for behandling og opbevaring af oplysninger	Artikel 28, stk. 3
F - Underdatabehandlere	F.1 - Underdatabehandleraftale og instruks	Artikel 28, stk. 2 og 4
	F.2 - Godkendelse af underdatabehandlere	Artikel 28, stk. 2
	F.3 - Ændringer i godkendte underdatabehandlere	Artikel 28, stk. 2
	F.4 - Underdatabehandlerens forpligtelser	Artikel 28, stk. 2 og 4
	F.5 - Oversigt over underdatabehandlere	Artikel 30, stk. 2
	F.6 - Tilsyn med underdatabehandlere	Artikel 28, stk. 2 og 4

KONTROLOMRÅDE	UNDERKONTROLOMRÅDE	GDPR-ARTIKEL
H - De registreredes rettigheder	H.1 - Procedure for opfyldelse af registreredes rettigheder	Artikel 28, stk. 3, litra e
	H.2 - Tekniske foranstaltninger til opfyldelse af registreredes rettigheder	Artikel 28, stk. 3, litra e
I - Sikkerhedsbrud	I.1 - Underretning om brud på persondatasikkerhed	Artikel 33, stk. 2
	I.2 - Identifikation af brud på persondatasikkerhed	Artikel 33, stk. 2
	I.3 - Rettidig underretning om brud på persondatasikkerhed	Artikel 33, stk. 2
	I.4 - Bistand til dataansvarlige ved brud på persondatasikkerhed	Artikel 28, stk. 3, litra f
J - Databeskyttelse gennem design og standardindstillinger	J.1 - Ændringsstyring og privacy-by-design	Artikel 25
	J.2 - Implementering af ændring i produktionsmiljøet	Artikel 25
	J.3 - Adskillelse af udviklings-, test- og produktionsmiljøet	Artikel 25
	J.4 - Adgang til kildekode	Artikel 25

Ovenstående kontroller er formuleret med afsæt i FSR – Danske Revisorers forslag til kontroller, der kan indgå i ISAE 3000 GDPR-erklæring. Det skal bemærkes at B.4 vedrørende firewall, B.5 vedrørende netværkssikkerhed ikke er medtaget i erklæringen idet, at databehandleren ikke selv opbevarer personoplysninger på egne netværk, G.1, G.2 og G.3 vedrørende overførsel af personoplysninger til tredjeland ikke er medtaget i erklæringen idet, at databehandleren ikke overfører personoplysninger til tredjelande.
Kontrollen vedrørende databeskyttelsesrådgiver er ligeledes ikke medtaget i erklæringen idet, at databehandleren ikke opfylder betingelserne for krav om DPO-funktionen.

RISIKOVURDERING

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

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

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

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

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

Behandling af personoplysninger på vegne af dataansvarliges instruks (kontrolmål A)

Databehandleraftale

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

Instruks for behandling af personoplysninger
Cabana har indført politikker og procedurer, der sikrer, at Cabana handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske, herunder hvem der hos den dataansvarlige kan give bindende instruks til Cabana. Proceduren sikrer desuden, at Cabana informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

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

Tekniske foranstaltninger (kontrolmål B)

Aftalte sikringsforanstaltninger
Cabana har indført procedurer, der sikrer, at der er etableret aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Risikovurdering
Cabana har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom.

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

Logisk adgangssikkerhed og adgangsstyring
Cabana har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Overvågning
Cabana har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

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

Kryptering af personoplysninger

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

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

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

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

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

Vedligeholdelse af systemsoftware
Cabana har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og software installeret på servere og arbejdsstationer.

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

Cabana har indført procedurer, der sikrer, at adgang til serverrum er tildelt ud fra et arbejdsbetinget behov. Serviceleverandører, der har behov for adgang for at varetage opsyn eller vagt, er godkendt af ledelsen. Tildelte adgange til serverrum gennemgås og revideres ved ændringer og mindst én gang årligt.

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

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

Fjernarbejdspladser og fjernadgang til systemer og data
Cabana har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for Cabanas lokaler og fjernadgang til systemer og data sker via whitelistede IP-adresser.

Organisatoriske foranstaltninger (kontrolmål C)

Databehandlerens garantier

Cabana har indført politikker og procedurer, der sikrer, at Cabana kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. Cabana har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres. Cabana har sikret at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler. Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for uddannelse og instruktion af medarbejdere, der behandler personoplysninger, herunder gennemførelse af awareness og oplysningskampagner.

Fortrolighed og lovbestemt tavshedspligt

Cabana har indført politikker og procedurer, der sikrer fortrolighed ved behandlingen af personoplysninger. Alle medarbejdere i Cabana har forpligtet sig til fortrolighed ved at underskrive en ansættelseskontrakt, der indeholder vilkår om tavshed og fortrolighed.

Reparation og service samt bortskaffelse af it-udstyr

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

Supporters adgang til personoplysninger

Cabana har indført procedurer 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.

Sletning af personoplysninger (kontrolmål D)

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

Opbevaring af personoplysninger (kontrolmål E)

Opbevaring af personoplysninger

Cabana har indført procedurer, der sikrer, at opbevaring af personoplysninger alene foretages i overensstemmelse med kontrakten med den dataansvarlige og listen over lokationer i den tilhørende databehandleraftale.

Underdatabehandlere (kontrolmål F)

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

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

Cabana har etableret en oversigt over underdatabehandlere med angivelse af underdatabehandlerens navn, CVR-nr., adresse og beskrivelse af behandlingen. Herunder findes en oversigt over Cabanas anvendte underdatabehandlere samt deres formål:

Underdatabehandler	Adresse	Lokation for databehandling	Formål
ITM8 27001092	Dalgas Plads 7B, 1. 2 7400 Herning	Dalgas Plads 7B, 1. 2 7400 Herning	Hostingleverandør

	Danmark		
Curanet 29412006	Højvangen 4 8660 Skanderborg Danmark	Højvangen 4 8660 Skanderborg	Hostingleverandør

De registreredes rettigheder (kontrolmål H)

Bistand til den dataansvarlige i forhold til den registreredes rettigheder

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

Sikkerhedsbrud (kontrolmål I)

Underretning om brud på persondatasikkerheden

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

Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden

Cabana har indført politikker og procedurer, der sikrer, at Cabana kan bistå den dataansvarlige med artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden.

Databeskyttelse gennem design og standardindstillinger (kontrolmål J)

Cabana har indført politikker og procedurer for udvikling og vedligeholdelse af Cabanas platforme, der sikrer en styret ændringsproces. Der anvendes et Change Management system til styring af udviklings- og ændringsopgaver, og enhver opgave følger en ensartet proces, der indledes med risikovurdering i overensstemmelse med kravene om databeskyttelse gennem design og standardindstillinger.

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

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

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

- Den dataansvarlige har ansvaret for at sikre, at administratorernes brug af Cabanas platforme og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen.
- Den dataansvarlige styrer brugerrettighederne i Cabanas platforme, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.
- Den dataansvarlige må ikke anvende Cabanas platforme til behandling, herunder opbevaring af følsomme personoplysninger, og det er den dataansvarliges ansvar at sikre, at der ikke indtastes eller uploades sådanne personoplysninger i Cabanas platforme.

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 Cabanas beskrivelse af Kommuneplatformen og Publicplatformen samt for udformningen af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risicierne for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

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

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 5. december 2025.

Udførte testhandlinger

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

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

For de ydelser, som ITM8 leverer inden for hosting, har vi modtaget Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden 1. januar 2024 til 31. december 2024 i henhold til databehandleraftale med dataansvarlige for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Curanet leverer inden for hosting, har vi modtaget Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden 1. januar 2024 til 31. december 2024 i henhold til databehandleraftale med dataansvarlige for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Disse underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Cabanas beskrivelse af Kommuneplatformen og Publicplatformen og de tilhørende tekniske og organisatoriske sikkerhedsforanstalt-

ninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos Cabana, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

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

En afvigelse foreligger, når:

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

Kontrolområde A			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
A.1	**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, at der foreligger en formaliseret procedure, der skal sikre, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at proceduren indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Vi har inspiceret, at proceduren er opdateret og ledelsesgodkendt.	Ingen afvigelser konstateret.
A.2	**Efterlevelse af instruks for behandling af personoplysninger** ▶ 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 den seneste indgåede databehandleraftale med en dataansvarlig og observeret, at aftalen indeholder instrukser fra dataansvarlig. Vi har inspiceret databehandlerens fortegnelse over behandlingsaktiviteter og ved en stikprøve inspiceret, at behandlingen foregår i overensstemmelse med instruks fra dataansvarlig.	Ingen afvigelser konstateret.
A.3	**Underretning af dataansvarlig ved ulovlig instruks** ▶ Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon til indgåelse af databehandleraftaler med dataansvarlig og den seneste indgåede databehandleraftale med en dataansvarlig og observeret, at databehandleren er forpligtet til at underrette den dataansvarlige i	Vi har konstateret, at der ikke har været tilfælde, hvor instruks har været vurderet i strid med lovgivning ved erklæringstidspunktet. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.

Kontrolområde A			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		tilfælde, hvor en instruks vurderes at være i strid med lovgivning. Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde, hvor instruks har været vurderet i strid med lovgivning ved erklæringstidspunktet.	
A.4	**Fortegnelse over 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 og stilles til rådighed for tilsynsmyndigheden efter anmodning.	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 inspiceret, at fortegnelsen er opdateret. Vi har på forespørgsel blevet oplyst, at Datatilsynet ikke har anmodet om udlevering af fortegnelsen ved erklæringstidspunktet.	Vi har konstateret, at Datatilsynet ikke ved erklæringstidspunktet har anmodet om udlevering af fortegnelsen ved erklæringstidspunktet. Vi har derfor ikke kunnet teste implementering af denne del af kontrollen. Ingen afvigelser konstateret.

Kontrolområde B			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
B.1	**Aftalte sikringsforanstaltninger** ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Vi har inspiceret, at procedurer er opdateret og ledelsesgodkendt.	Ingen afvigelser konstateret.
B.2	**Risikovurdering** ▶ Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. VI har inspiceret, at databehandleren har foretaget en risikovurdering baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder. Vi har inspiceret, at den foretagne risikovurdering er opdateret og godkendt. Vi har stikprøvevist inspiceret, at databehandler har implementeret tekniske foranstaltninger på baggrund af risikovurderingen, herunder foranstaltninger der er aftalt med dataansvarlige.	Ingen afvigelser konstateret.
B.3	**Antivirus** ▶ Der er for de arbejdsstationer, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for én tilfældig udvalgt pc, der anvendes til behandling af personoplysninger, inspiceret, at der er installeret antivirus, som er opdateret.	Ingen afvigelser konstateret.

Kontrolområde B			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		Vi er på forespørgsel blevet oplyst, at databehandlerens personoplysninger bliver opbevaret hos underdatabehandlere Curanets og ITM8's datacentre. Vi har inspiceret underdatabehandlernes ISAE 3000 revisionserklæringer og observeret, at erklæringerne er uden forbehold og, at erklæringerne ikke indeholder forhold om antivirus, som har krævet yderligere handlinger fra databehandleren.	
B.6	**Adgangsstyring - adgang til personoplysninger** ▶ Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Vi har inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Vi har inspiceret ved en stikprøve på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.
B.7	**Overvågning af systemer og miljøer** ▶ Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: ○ Oppetid ○ Nedetid ○ Svartider	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi er på forespørgsel blevet oplyst, at databehandlerens personoplysninger bliver opbevaret hos underdatabehandlere Curanets og ITM8's datacentre. Vi har inspiceret underdatabehandlernes ISAE 3000 revisionserklæringer og observeret, at	Ingen afvigelser konstateret.

Kontrolområde B			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		erklæringerne er uden forbehold og, at erklæringerne ikke indeholder forhold om overvågning, som har krævet yderligere handlinger fra databehandleren. Vi har for en stikprøve inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	
B.8	**Kryptering ved transmission personoplysninger** ▶ Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med 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.
B.9	**Logning** ▶ Der er etableret logning i systemer, databaser og netværk af følgende forhold: ○ Aktiviteter, der udføres af brugere ○ Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder ○ Sikkerhedshændelser omfattende: ▪ Ændringer i systemrettigheder til brugere ▪ Fejlede forsøg på log-on til systemer, databaser og netværk ▶ Logoplysninger er beskyttet mod manipulation og tekniske fejl.	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 inspiceret ved en stikprøve på én dags logning, at logfiler har det forventede indhold i forhold til opsætning. Vi har inspiceret ved en stikprøve på én dags logning, at logfiler med systemadministratorer og andre med særlige rettigheders aktiviteter har det forventede indhold i forhold til opsætning.	Ingen afvigelser konstateret.

Kontrolområde B			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
B.10	**Anonymisering af personoplysninger i udviklingsopgaver** ▶ Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret ved en stikprøve på udviklingsmiljøet, at personoplysninger heri er anonymiseret.	Ingen afvigelser konstateret.
B.11	**Sårbarhedsscanninger og penetrationstests** ▶ De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger. Vi har inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Vi har inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret eller accepteret.	Ingen afvigelser konstateret.
B.12	**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 inspiceret ved udtræk, at databaser og netværk er opdateret med relevante opdateringer og sikkerhedspatches. Vi er på forespørgsel blevet oplyst, at databehandlerens personoplysninger bliver opbevaret hos underdatabehandlere Curanets og ITM8's datacentre. Vi har inspiceret underdatabehandlernes ISAE 3000 og ISAE 3402 revisionserklæringer og observeret, at erklæringerne er uden forbehold og, at erklærin-	Ingen afvigelser konstateret.

Kontrolområde B			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		gerne ikke indeholder forhold om vedligeholdelse af systemsoftware, som har krævet yderligere handlinger fra databehandleren.	
B.13	**Adgangsstyring - procedure og periodisk gennemgang** ▶ Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har for seneste ansatte medarbejder inspiceret, at medarbejderens adgang til systemer, hvor der behandles personoplysninger, er godkendt, og at medarbejderen har et arbejdsbetinget behov for adgangene. Vi har for seneste fratrådte medarbejder inspiceret, at den fratrådtes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Vi har inspiceret databehandlerens årshjul og observeret, at databehandleren regelmæssigt skal vurdere og godkende tildelte brugeradgange. Vi har inspiceret, at databehandleren har foretaget vurdering og godkendelse af brugeradgange.	Ingen afvigelser konstateret.
B.14	**Logisk adgangskontrol** ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle med adgang til personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger sker gennem adgangskoder, der afspejler risikoen ved behandlingsaktiviteten.	Ingen afvigelser konstateret.

Kontrolområde B			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
B.15	**Fysisk adgangskontrol** ▶ Der er etableret fysisk adgangssikkerhed således, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at kun autoriserede personer har fysisk adgang til lokaler, hvori der behandles personoplysninger. Vi er på forespørgsel blevet oplyst, at databehandlerens personoplysninger bliver opbevaret hos underdatabehandler Curanet og ITM8. Vi har inspiceret Curanets og ITM8s 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.
B.16	**Sikkerhedskopiering og reetablering** ▶ 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, at der foretages sikkerhedskopiering af relevante systemer og data i overensstemmelse med proceduren. Vi har inspiceret, at sikkerhedskopier har været genetableret.	Ingen afvigelser konstateret.
B.17	**Fjernarbejdspladser og fjernadgang til systemer og data** ▶ Fjernadgang til databehandlerens systemer og data sker via Whitelistede IP-adresser.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens gruppe over brugere underlagt login igennem whitelistede IP-adresser.	Ingen afvigelser konstateret.

Kontrolområde B			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		Vi har for en stikprøve inspiceret dokumentation for, at adgang til databehandlerens systemer kun kan ske igennem whitelistede IP-adresser.	

Kontrolområde C			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
C.1	**Politikker for informationssikkerhed og gennemgang af politikker for informationssikkerhed** ▶ Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere. Vi har inspiceret, at procedurer er opdateret og ledelsesgodkendt.	Ingen afvigelser konstateret.
C.2	**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 inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Vi har inspiceret ved en stikprøve på databehandleraftaler, at kravene i aftalerne ikke er modstridende med informationssikkerhedspolitikken.	Ingen afvigelser konstateret.
C.3	**Rekruttering af medarbejdere – Screening** ▶ Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: o Referencer fra tidligere ansættelser o Straffeattest o Uddannelsesbevis	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Ingen afvigelser konstateret.

Kontrolområde C			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		Vi har for den seneste ansatte inspiceret, at databehandleren har udført efterprøvning af kandidaten, og at efterprøvningen har omfattet relevant dokumentation.	
C.4	**Rekruttering af medarbejdere - Tavsheds- og fortrolighedsaftale med medarbejdere og introduktion til informationssikkerhed** ▶ Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for den seneste ansatte inspiceret, at den pågældende medarbejder har underskrevet krav til tavshedspligt i ansættelseskontrakten. Vi har for den seneste ansatte inspiceret, at den pågældende medarbejder er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information.	Ingen afvigelser konstateret.
C.5	**Fratrædelse af medarbejdere - inddragelse af adgangsrettigheder og aktiver** ▶ Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Vi har for den seneste fratrådte medarbejder inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget rettidigt.	Ingen afvigelser konstateret.

Kontrolområde C			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
C.6	**Fratrædelse af medarbejdere - oplysning om fortrolighed og tavshedspligt** ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for seneste fratrådte medarbejder inspiceret, at databehandleren har orienteret den fratrådte medarbejder om, at den pålagte tavshedspligt fortsat er gældende efter ansættelsesophør.	Ingen afvigelser konstateret.
C.7	**Awareness, uddannelse og træning vedrørende informationssikkerhed** ▶ Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen afvigelser konstateret.
C.8	**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 inspiceret, at der foreligger formaliserede procedurer, der sikrer, at supporters adgange og håndtering af personoplysninger ved supportopgaver sker ud fra support tickets og supporterens arbejdsbetingede behov. Vi har ved en stikprøve inspiceret en supportsag og observeret, at denne følger proceduren.	Ingen afvigelser konstateret.

Kontrolområde C			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
C.9	**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.	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 ved erklæringstidspunktet.	Vi har konstateret, at databehandleren ikke har sendt it-udstyr til reparation-, service- eller destruktion ved erklæringstidspunktet. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.

Kontrolområde D			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
D.1	**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 ledelsesgodkendt.	Ingen afvigelser konstateret.
D.2	**Krav til opbevarings- og sletteperiode af oplysninger er i overensstemmelse med dataansvarliges krav** ▶ Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: ○ personoplysninger opbevares så længe der er et aktivt kundeforhold ○ Ved ophør af tjenesten, sletter eller tilbageleverer databehandleren personoplysningerne.	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. Vi har inspiceret ved en stikprøve på databehandlinger fra databehandlerens fortegnelse over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Vi har inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen afvigelser konstateret.

Kontrolområde D			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
D.3	**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, at der foreligger formaliserede procedurer for tilbagelevering og/eller sletning af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har på forespørgsel fået oplyst, at der individuelt aftales med kunden, hvordan behandlingen afvikles. Vi har på forespørgsel fået oplyst, at der ikke har været ophør af databehandleraftaler ved erklæringstidspunktet.	Vi har konstateret, at der ikke har været ophør af databehandleraftaler ved erklæringstidspunktet. Vi har derfor ikke kunnet teste kontrollens implementering. Ingen afvigelser konstateret

Kontrolområde E			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
E.1	**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 ved en stikprøve på opbevaring af personoplysninger, at personoplysninger kun opbevares i den periode, som er aftalt med den dataansvarlige. Vi har inspiceret, at procedurerne er opdateret og ledelsesgodkendt.	Ingen afvigelser konstateret.
E.2	**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. 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 inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolområde F			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
F.1	**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 ledelsesgodkendt.	Ingen afvigelser konstateret.
F.2	**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 inspiceret ved en stikprøve på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af seneste indgåede databehandleraftale med en dataansvarlig.	Ingen afvigelser konstateret.
F.3	**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.	Ingen afvigelser konstateret.

Kontrolområde F			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		Vi har inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i overensstemmelse med indgåede databehandleraftaler.	
F.4	**Underdatabehandlerens forpligtelser** ▶ Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er indgået databehandleraftaler med anvendte underdatabehandlere, Vi har inspiceret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
F.5	**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.
F.6	**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.	Ingen afvigelser konstateret.

Kontrolområde F			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
		Vi har inspiceret, at databehandleren har udført tilsyn, herunder indhentet og gennemgået underdatabehandlers revisorerklæringer, certificeringer og lignende. Vi har inspiceret, at databehandlerens tilsyn af underdatabehandlere ikke har givet anledning til yderligere handlinger.	

Kontrolområde H			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
H.1	**Procedure for opfyldelse af registreredes rettigheder** ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdateret og ledelsesgodkendt.	Ingen afvigelser konstateret.
H.2	**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 • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har inspiceret dokumentation for, at de anvendte systemer understøtter gennemførelsen af de nævnte detaljerede procedurer. Vi har på forespørgsel fået oplyst, at der ikke er sket anmodning om bistand i forhold til de registreredes rettigheder ved erklæringstidspunktet.	Vi har konstateret, at der ikke er sket anmodning om bistand i forhold til de registreredes rettigheder ved erklæringstidspunktet. Vi har derfor ikke kunne teste kontrollens implementering Ingen afvigelser konstateret.

Kontrolområde I			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
I.1	**Underretning om brud på persondatasikkerhed** ▶ 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.	Ingen afvigelser konstateret.
I.2	**Identifikation af brud på persondatasikkerhed** ▶ Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: o Awareness hos medarbejdere o Overvågning af netværkstrafik o Opfølgning på logning af tilgang til personoplysninger	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 af underdatabehandler og af Cabanas eget setup. Vi har inspiceret Curanets og ITM8s revisionserklæringer og observeret, at erklæringerne er uden forbehold og, at erklæringerne ikke indeholder forhold omkring overvågning, som har krævet yderligere handlinger fra databehandleren. Vi har inspiceret, at databehandleren modtager notifikationer om serveres tilgængelighed. Vi har inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen afvigelser konstateret.

Kontrolområde I			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
I.3	**Rettidig underretning om brud på persondatasikkerhed** ▶ Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 48 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har observeret, at der ikke har været konstateret hændelser, som har medført brud på persondatasikkerheden.	Vi har konstateret, at der ikke har været konstateret hændelser ved erklæringstidspunktet, som har medført brud på persondatasikkerheden. Vi har derfor ikke kunnet teste implementering af kontrollen. Ingen afvigelser konstateret.
I.4	**Bistand til dataansvarlige ved brud på persondatasikkerhed** ▶ Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: o Karakteren af bruddet på persondatasikkerheden o Sandsynlige konsekvenser af bruddet på persondatasikkerheden o 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.	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.

Kontrolområde J			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer informationssikkerhed og databeskyttelse tilrettelægges og implementeres i databehandlerens udviklings- og ændringsproces.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
J.1	**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, at 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 for seneste implementerede ændring/udvikling inspiceret, at der i udviklings-/ændringsopgaven er sikret overholdelse af privacy-by-design-principperne. Vi har endvidere inspiceret, at opgaven har fulgt den formaliserede proces, og at der er udført test, og at ændringen/udviklingen er godkendt inden implementering.	Ingen afvigelser konstateret.
J.2	**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 er opsat funktionsadskillelse således, at udviklere ikke må implementere ændringer direkte i produktionsmiljøet. Vi har for en stikprøve inspiceret, at udviklere ikke selv tester og implementerer deres ændringer i produktionsmiljøet.	Ingen afvigelser konstateret.
J.3	**Adskillelse af udviklings-, test- og produktionsmiljøet** ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionsmiljøer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at udviklings-, test- og produktionsmiljøet er adskilt.	Ingen afvigelser konstateret.

Kontrolområde J			
Kontrolmål *Der efterleves procedurer og kontroller, som sikrer informationssikkerhed og databeskyttelse tilrettelægges og implementeres i databehandlerens udviklings- og ændringsproces.*			
Nr.	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
J.4	**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, der har adgang til kildekode. Vi har inspiceret dokumentation for, at kildekoden er beskyttet mod uautoriseret ændring og sletning.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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

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

Thomas Vorgaard Andersen
Direktør
På vegne af: Cabana ApS
Serienummer: bbda2021-c97b-429d-aa36-70405dc614a1
IP: 104.28.xxx.xxx
2025-12-09 14:13:03 UTC

Mit ID

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner, Statsautoriseret revisor
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 77.243.xxx.xxx
2025-12-09 14:24:33 UTC

Mit ID

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner, chef for Risk Assurance, CISA, CRISC
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 37.96.xxx.xxx
2025-12-09 15:02:34 UTC

Mit ID