



Juli 2023

Adeo Datacenter ApS

CVR-nr. 37 59 31 84

ISAE 3402 TYPE 2 ERKLÆRING

Revisors erklæring vedrørende de generelle it-kontroller
i tilknytning til driften af Adeo Datacenter's aktiviteter
for perioden 1. januar 2022 – 31. december 2022



Indhold

Kapitel 1: Ledelseserklæring.....	3
Kapitel 2: Adeo Datacenter ApS's beskrivelse af de generelle it-kontroller for driften af datacenter	4
Kapitel 3: Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet	10
Kapitel 4: Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf	13



Kapitel 1: Ledelseserklæring

Beskrivelsen af Adeo Datacenter's generelle it-kontroller i kapital 2 er udarbejdet til brug for kunder, der har anvendt eller påtænker at anvende Adeo Datacenter's datacenterydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber. Adeo Datacenter bekræfter hermed, at

- (A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af Adeo Datacenter datacenterydelsers generelle it-kontroller i hele perioden 1. januar 2022 – 31. december 2022. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:
- (i) Redegør for, hvordan kontrollerne var udformet og implementeret, herunder redegør for:
 - De typer af ydelser, der er levereret, når det er relevant
 - De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller
 - Relevante kontrolmål og kontroller udformet til at nå disse mål
 - Kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomhederne, og som, hvis det er nødvendigt for at nå de kontrolmål, som vi ikke selv kan nå
 - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har være relevante for de generelle it-kontroller
 - (ii) Indeholder relevante oplysninger om ændringer i Adeo Datacenter generelle it-kontroller foretaget i perioden 1. januar 2022 – 31. december 2022.
 - (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontroller, som den enkelte kunde måtte anse som vigtig efter deres særlige forhold.
- (B) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerende effektivt i hele perioden 1. januar 2022 – 31. december 2022. Kriterierne for dette udsagn er, at:
- (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
 - (ii) De identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer opnåelsen af de anførte kontrolmål og
 - (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. januar 2022 – 31. december 2022.

Albertslund, 7. juli 2023

Adeo Datacenter ApS

Mikkel Emmerik
Adm. Direktør



Kapitel 2: Adeo Datacenter ApS's beskrivelse af de generelle it-kontroller for driften af datacenter

Indledning

Formålet med nærværende beskrivelse er at levere information til Adeo Datacenter's kunder og deres revisorer vedrørende kravene i ISAE 3402-II, som er den internationale revisorstandard for erklæringsopgaver om kontroller for serviceleverandører, ISAE 3402-II.

Beskrivelsen giver herudover information om de kontroller, der er anvendt for driften i Adeo Datacenter's datacenter aktiviteter i perioden 1. januar 2022 – 31. december 2022.

Beskrivelse af Adeo Datacenter ApS

Adeo Datacenter er et danskejet datacenter, som blev etableret i 2016.

Adeo Datacenter leverer datacenterydelser i egne fysiske rammer beliggende i Albertslund.

Adeo Datacenters medarbejdere har mere end 50 års erfaring med at levere hosting og datacenterdrift til både små og store virksomheder. Med udgangspunkt i kundens ønsker og behov sammensættes den rette løsning, uanset om kunden ønsker at benytte eget udstyr, eller vil leje Adeo Datacenter's servere og hardware.

Adeo Datacenter sikrer den bedst mulige driftsstabilitet og sikkerhed i forbindelse med hele infrastrukturen, både på kort og på lang sigt. Med løsninger fra Adeo Datacenter fokuserer vi på fleksible og let skalerbare løsninger, til gavn for virksomhedens kunder, samt virksomheden og de ansatte, så de kan koncentrere sig om deres kerneforretning.

Vi beskæftiger os udelukkende med datacenterdrift for virksomheder og organisationer. Vores kundereferencer dækker både independent software vendors (ISV'er) samt partnere, dvs. virksomheder der leverer managed IT- services.

Der tages udgangspunkt i kundens behov for at skabe en skræddersyet løsning, som sammensættes af forskellige produkter med forskellige egenskaber lige fra virtuelle maskiner til fysiske rackskabe. Adeo Datacenter er kategoriseret som et professionelt datacenter. Det betyder, at virksomhederne får den optimale sikring af servere og data, idet Adeo Datacenter har elektronisk adgangskontrol, videoovervågning, temperaturalarmer, røg/brandsensorer, klimastyring, UPS og generatoranlæg. Datacenteret er opbygget i 5 separate datahaller, og i separate rows med egen switch-centric redundant netværksinfrastruktur. På den måde kan der hurtigt og fleksibelt tilføjes ekstra servere, CPU og storagekapacitet, så det præcis matcher kundens behov.

Hos Adeo Datacenter arbejder vi målrettet med IT-sikkerhed og EU's nye persondataforordning, som træder i kraft i maj 2018. Dét at vi er et dansk ejet datacenter beliggende på dansk jord, er i sig selv et meget stort skridt for vores kunder, hen mod at kunne imødekomme kravene i den nye forordning. Man ved nemlig hvor data ligger, i modsætning til virtuelle tjenester og konkurrenter med forbundne datacentre i mange lande.



Omfang for denne beskrivelse

Adeo Datacenter er leverandør af datacenterydelser, og kerneaktiviteten er datacenter drift. Overvågning af infrastruktur håndteres af Adeo Datacenter, mens kunderne selv overvåger og supporter eget eller lejet udstyr placeret i datacenteret.

Adeo Datacenter har ansvaret for at opsætte og overholde passende procedurer og kontroller med henblik på at finde og forebygge fejl. Overholdelsen af kontrollerne er essentiel for driften og danner grundlag for en ISAE3402-II certificering.

It-sikkerhedsstrategi

Adeo Datacenter's strategiske fokus for It-sikkerhed er, at forretningen skal have indbygget de nødvendige mekanismer, så selskabet og kunder ikke påføres uacceptable risici.

Vores sikkerhedspolitik er højt prioriteret af vores ledelse, og er dermed også afspejlet i vores daglige procedurer og forretningsgange.

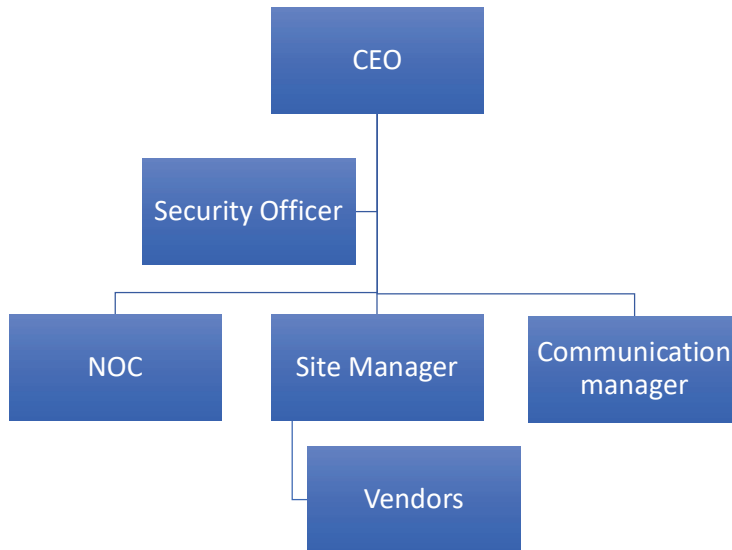
Adeo Datacenter's sikkerhedspolitik beskriver sikringsforanstaltninger indenfor følgende områder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved Nød-, beredskabs- og reetableringsstyring
- Overensstemmelse

Alle procedurer gennemgås løbende og revideres med henblik på at optimere og automatisere procedurer i organisationen. Formålet er at fjerne potentielle menneskelige fejl.

Organisation og organisering af it-sikkerheden

I Adeo Datacenter er CTO'en den overordnede ansvarlige for it-sikkerheden. Til at støtte op omkring sikkerheden er der lavet et IT-sikkerhedsudvalg, som løbende mødes og gennemgår virksomhedens sikkerhedsprocedurer.



Risikostyring

Adeo Datacenter har faste procedurer der sikrer, at de risici der er forbundet med datacenterets drift er minimeret. Kontrol foretages løbende som stikprøver, samt hver gang eksisterende systemer opdateres eller nye implementeres.

CEO har ansvaret for en løbende risikovurdering, som godkendes og forankres i ledelsen.

Håndtering af it-sikkerhed

Det daglige ansvar for IT-sikkerheden håndteres af medlemmerne i IT-sikkerhedsudvalget. Dermed sikres det, at krav og rammer overholdes. Sikkerhedsudvalget arbejder ud fra gældende sikkerhedspolitikker.

Adeo Datacenter ønsker at levere en stabil og sikker datacenterløsning til kunderne, og det er ud fra denne målsætning, at så mange procedure som muligt bliver automatiseret, og der er udarbejdet tjeklister for manuelle processer. Formålet er at sikre en ensartet leverance overfor kunder og partnere.

Sikkerhedspolitikken gælder for alle medarbejdere og leverancere.

Skulle der ske fejl i driftsmiljøet, udbedres fejlen straks. IT-sikkerhedsudvalget gennemgår herefter fejlen med henblik på at undgå, at den opstår igen. Der laves en incidentrapport, som har til formål at informere kunder og danne basis for vidensdeling til medarbejdere. Alle netværksenheder er registreret i Adeo Datacenter's DCIM system (Data Center Information Management), og alle systemændringer registreres heri. Konfigurationsfiler til netværksenheder (firewall, routere, switches osv.) ligger i Adeo Datacenter's dokumentationssystem.

Adeo Datacenter foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.



HR, medarbejdere og uddannelse

Ansættelse af medarbejdere og etablering af samarbejdsaftaler med eksterne sker ud fra faste procedurer, så vi sikrer, at vi ansætter den rette person i forhold til baggrund og kompetencer. Alle får en specifik rolle- og ansvarsbeskrivelse, så man er bekendt med sit ansvar.

Generelle ansættelsesvilkår, herunder fortrolighedsforhold omkring kunder og Adeo Datacenter er beskrevet i hver medarbejders ansættelseskontrakt. I kontrakten er ligeledes indeholdt medarbejderens forpligtelse til at overholde de gældende politikker og procedurer.

Medarbejdere er et uhyre vigtigt aktiv i et datacenter, og derfor arbejder Adeo Datacenter målrettet med at sikre, at alle medarbejdere har de rette kvalifikationer, certificeringer og uddannelse. Og medarbejdernes viden og kompetencer vedligeholdes løbende igennem kurser mm. i ind- og udland. Tilsvarende orienteres medarbejders også, når interne sikkerhedsprocedurer/politikker ændres, så alle altid er ajour.

Forhold omkring ophør af ansættelse er beskrevet i hver medarbejders ansættelseskontrakt. Og de gældende fratrædelseskontroller (adgang til systemer, lokaler mm.) og processer ligger hos den ansattes leder.

Styring af aktiver

Hos Adeo Datacenter er alt udstyr; servere, racks, netværksudstyr mm. individuelt registreret, for at få et let udstyrsoverblik. Da vi har et stort og ekstrem redundant netværk, hvor der er tilkoblet mange systemer og mange kunder, har vi udarbejdet en særlig navnestandard for at sikre en nem forståelse af placering og brug i netværket.

Brugerstyring/adgangssikkerhed

Som en del af IT-politikken, har Adeo Datacenter klare procedurer for adgangstildeling til det fysiske datacenter og til netværket. Kun autoriserede brugere har adgang til haller og systemer.

Kunder som har adgang til Adeo Datacenter's haller får udleveret en pinkode og en individuel adgangsbrik.

For at en adgangsbrik kan udstedes, skal personen fremvise gyldigt pas eller kørekort.

Adeo Datacenter's egne medarbejdere oprettes alene med autorisation fra CTO.

Medarbejdere og kunder som ikke skal have adgang mere, skal meldes til Adeo Datacenter NOC, som sikrer at adgange straks lukkes for brugeren, og at konti nedlægges.

Fysisk sikkerhed

Hardware

Hardware (racks, servere mm) i Adeo Datacenter er leveret fra markedets bedste og mest anerkendte producenter, herunder Brocade, HP, MikroTIK og Fortigate. Adeo Datacenter følger leverandørers anvisninger for vedligeholdelse af udstyret. Alt udstyr i datacenteret er ejet af Adeo Datacenter, og det



giver os fuld kontrol. Internet forbindelser er redundante for at kunne opretholde en stabil drift for vores kunder.

Adgangsforhold

Alle adgange til datacenteret er sikret med RFID kort, og alle adgange logges i separat adgangssystem (i 5 år). Centret er opbygget i 5 separate haller, og har desuden separate områder til nødstrømsanlæg, lager og brandslukningsudstyr. Al adgang er kameraovervåget 24/7/365.

Strømsikring

Strømforsyningen i datacenteret er sikret ved et UPS nødstrømsanlæg, som ved længere tids udfald overtages af dieselgenerator, således at drift kan fortsætte, hvis bystrøm skulle forsvinde.

Transientbeskyttede strømtavler i datacenteret beskytter mod udefrakommende strømbelastninger, f.eks. lynnedslag.

Brandsikring

Hvis der konstateres røg i en hal, affyres Fire-eater systemet automatisk og omgående. Brandslukningen alarmerer den lovpligtige kontrolcentral, og vagt tilkaldes automatisk.

Køling

Der er etableret et N+1 redundant kølesystem i datacenteret. Hvis det primære system går ned, så tager det ekstra system over. Det redundante system er et klassisk frikølingsanlæg bestående af tre (3) køletårne.

Placering

Med henblik på oversvømmelse, er datacenteret placeret et sted med gode afvandringsforhold, med blandt andet en afledningskanal på tilstødende arealer, hvor overfladevand kan ledes hen og bort.

Afledningskanaler er blevet vedligeholdt af kommunen for at sikre frit løb. Iflg. Geodatastyrelsens vandafledningskort er datacenteret ikke i risiko ved maksimalregn, og der har til vores kendskab aldrig været konstateret oversvømmelse på matriklen.

Logning og overvågning

Adeo Datacenter overvåger alle centrale systemer og logger trafik, samt mønstre til brug for fejlfinding i systemerne.

Patch management / ændringshåndtering

Adeo Datacenter vil patche infrastrukturen og sikre at sikkerhedshuller bliver lukket med det samme. Ændringer bliver dokumenteret og logget i dokumentationssystemet. De systemer som tilbydes kunderne bliver håndteret på samme måde som resten af infrastrukturen. Normale opdateringer bliver først testet i vores laboratorie-setup, inden det implementeres på produktionssystemer.



Styring af it-sikkerhedshændelser

Konstateres fejl eller svagheder i Adeo Datacenter's systemer korrigeres disse hurtigst muligt, så kunder ikke belastes unødigt. Derudover meldes fejl og svagheder løbende til ledelsen, så nødvendige ændringer kan iværksættes, og lignende fremtidige sager dermed kan undgås.

Leverandørforhold

Hvis leverandører tildeles adgang til datacenter eller systemer, foreligger der en underskrevet NDA. IT-sikkerhedsudvalget vedligeholder en leverandøroversigt indeholdende adgangsplysninger.

Beredskabsstyring

I Adeo Datacenters beredskabsplan fremgår, hvordan et nedbrud skal håndteres, herunder hvilke systemer og i hvilken rækkefølge driften skal genskabes. Ved alvorlige fejl eller nedbrud orienteres alle nøglemedarbejdere om problemet, samt om hvordan det er håndteret og løst.

Ved totalskade på et eller flere serverrum er der udarbejdet en plan for, hvordan reetablering skal ske, og hvordan backup kan gendannes.

Væsentlige ændringer i forhold til it-sikkerhed

For erklæringsperioden er der ikke væsentlige ændringer.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Indeværende beskrivelse dækker over standardaftaler og dækker ikke over den enkelte kundes særftaler.

Kunden er ansvarlig for de systemer, de driver via Adeo Datacenter's faciliteter, og skal selv tilse de nødvendige kontroller i forbindelse med driften.

Kunden er ansvarlig for at sikre, at adgang givet til datacenteret og til de omkringliggende systemer, til enhver tid er fuldt opdaterede.

Kunden er ansvarlig for, at egne forbindelser er funktionelle og sikrede på et ansvarligt niveau.

Adeo Datacenter har en generel beredskabsplan, som dækker specifikke aktiviteter involveret i at genskabe datacenteret og ydelser. Såfremt den enkelte kunde har et udvidet behov, kan der udarbejdes en særskilt plan.



Kapitel 3: Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til kunder / brugere af Adeo Datacenter ApS' datacenteraktiviteter og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Adeo Datacenter ApS' beskrivelse, som er gengivet i kapitel 2. Beskrivelsen, som i kapitel 1 er bekræftet af Adeo Datacenter ApS' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens datacenter-plattform i perioden 1. januar 2022 – 31. december 2022 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Adeo Datacenter ApS' ansvar

Adeo Datacenter ApS' er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i kapitel 2 og tilhørende udtalelse (kapitel 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetance og fornøden omhu, fortrolighed samt professionel adfærd.

Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Adeo Datacenter ApS' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402-II, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB. Denne standard kræver, at vi overholder etiske krav samt 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollerens udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens 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 funktionaliteten 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 nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i kapitel 2.

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

Begrænsninger i kontroller hos Adeo Datacenter ApS'

Adeo Datacenter ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør 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 kapitel 1 i ledelsens erklæring. Det er vores opfattelse:

- a) at beskrivelsen af de af Adeo Datacenter ApS' generelle it-kontroller i tilknytning til datacenteraktiviteter, således som det var udformet og implementeret i hele perioden fra 1. januar 2022 – 31. december 2022, i alle væsentlige henseender er retvisende, og
- b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2022 – 31. december 2022, og
- c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2022 – 31. december 2022.

Vi skal bemærke, at der for de enkelte kunder kan være specifikke forhold, som gør, at den generelle konklusion ikke er dækkende. Hvis det er aftalt mellem kunden og Adeo Datacenter ApS', at der udarbejdes en specifik erklæring vedrørende kunden kontrakt, vil forholdene fremgå heraf.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår på kapitel 4.



Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapitel 4 er udelukkende tiltænkt kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Roskilde, 7. juli 2022

Algade Revision

Registreret revisionsanpartsselskab

CVR-nr. 35 66 39 16

Mick Andersen

Registreret revisor, FSR – danske revisorer

MNE: mne41282



Kapitel 4: Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Adeo Datacenter ApS har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i perioden 1. januar 2022 – 31. december 2022.

Vi har således ikke nødvendigvis testet alle kontroller, som Adeo Datacenter ApS har nævnt i sin beskrivelse af kapitel 2.

Kontroller udført hos Adeo Datacenter ApS' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Vi har udført vores tests af kontroller hos Adeo Datacenter ApS via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingstagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv udført - eller observeret - en genudførelse af kontroller med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores test ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.



Overvågning			
Nr.	Kontrolmål	Revisionstest	Resultat af test
1.1	Adeo DC's overvåger datacenterløsninger ved hjælp af fjernovervågning, som bl.a. monitorerer alarmer vedrørende temperatur, brand, vand, adgangsforhold m.v..	Vi har forespurgt til procedure vedrørende overvågning og fejlhåndtering, herunder registrering af oplysninger. Vi har observeret, at Adeo DC overvåger kabler, housing-faciliteter og kredsløb ved hjælp af fjernovervågning.	Ingen væsentlige afvigelser konstateret.

Adgangskontrol			
Nr.	Kontrolmål	Revisionstest	Resultat af test
1.2	Datacenterløsningers faciliteter er forsynet med adgangskontrolanlæg til sikring af, at kun autoriserede og godkendte medarbejdere og kunders udpegede personer har adgang til disse faciliteter. Godkendelse, udstedelse og nedlæggelse af adgangsmedier følger Adeo DC's kvalitetsproces herfor.	Vi har inspiceret procedure vedrørende adgangskontrol i datacentrene. Stikprøvevis observeret, at der kræves adgangskort for at få adgang til datacentre. Vi har observeret, at adgangsaktiviteter registreres og overvåges. Vi har inspiceret, at der foretages en løbende gennemgang af både interne og eksterne brugeradgange.	Ingen væsentlige afvigelser konstateret.



Forebyggende vedligehold			
Nr.	Kontrolmål	Revisionstest	Resultat af test
1.3	Adeo DC foretager ugentligt tilsyn af datacenterfaciliteter. Resultatet af disse tilsyn dokumenteres i udfyldte skemaer.	Vi har forespurgt til procedurer for forebyggende tilsyn. Vi har stikprøvevis inspiceret, at der bliver foretaget ugentlige kontroller inden for strøm, klima, brand og almindelig vedligehold, og at dette er dokumenteret i udfyldte skemaer	Ingen væsentlige afvigelser konstateret.

Fysisk sikkerhed			
Nr.	Kontrolmål	Revisionstest	Resultat af test
1.4	Adeo DC overholder specificerede krav til fysisk sikkerhed for datacenterløsninger omfattende følgende forhold; Bygning, gulve, klima, strøm, adgang, alarmmonitoring, automatisk brandslukning, kabling.	Vi har forespurgt til procedurer for overholdelse af krav til fysisk sikkerhed. Stikprøvevis observeret, at datacentret lever op til kravene.	Ingen væsentlige afvigelser konstateret.



Beredskabsplan			
Nr.	Kontrolmål	Revisionstest	Resultat af test
1.5	Adeo DC beredskabsplan bliver løbende afprøvet. Resultatet af afprøvninger dokumenteres.	Vi har forespurgt til procedurer vedrørende beredskabsplaner samt afprøvning af disse. Vi har inspiceret, at beredskabsøvelser er gennemført som planlagt og dokumenteret.	Ingen væsentlige afvigelser konstateret.

Human Security			
Nr.	Kontrolmål	Revisionstest	Resultat af test
1.6	Adeo DC identificere alle kunder via pas eller kørekort, samt underskrivelse af udleveret relevant materiale. Adeo DC har processer for tilbagelevering af ADEO DC's ejendele, samt lukning af alle accesser ved fratrædelser.	Vi har inspiceret, at Adeo DC foretager kontrol på kunder, samt procedurer for nedlukning af adgang mv.	Ingen væsentlige afvigelser konstateret.



Overensstemmelse			
Nr.	Kontrolmål	Revisionstest	Resultat af test
Review af informationssikkerheden			
1.7	Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.	Vi har forespurgt til periodisk uafhængig evaluering af it-sikkerheden og kontrol med overholdelsen af politikker samt tekniske konfigurationer.	Der har i perioden ikke været en formel procedure og kontrol for efterlevelse af politikker og procedurer. Der er efterfølgende udarbejdet en procedure og kontrol til formålet. Ingen væsentlige afvigelser i øvrigt.

Dette dokument er underskrevet af nedenstående parter, der med deres underskrift har bekræftet dokumentets indhold samt alle datoer i dokumentet.

This document is signed by the following parties with their signatures confirming the documents content and all dates in the document.

Mikkel Emmerik

Navnet returneret af dansk MitID var:

Mikkel Emmerik

Direktør

ID: 0d5d53a0-973b-4ec0-9e11-55f81eeef4a0

Tidspunkt for underskrift: 08-07-2023 kl.: 10:24:56

Underskrevet med MitID



Mick Andersen

Navnet returneret af dansk NemID var:

Mick Andersen

Revisor

ID: 74879815

CVR-match med dansk NemID

Tidspunkt for underskrift: 08-07-2023 kl.: 10:30:51

Underskrevet med NemID

NEM ID

This document has esignatur Agreement-ID: fb3309SsXIP250411376

This document is signed with esignatur. Embedded in the document is the original agreement document and a signed data object for each signatory. The signed data object contains a mathematical hash value calculated from the original agreement document, which secures that the signatures is related to precisely this document only. Prove for the originality and validity of signatures can always be lifted as legal evidence.

The document is locked for changes and all cryptographic signature certificates are embedded in this PDF. The signatures therefore comply with all public recommendations and laws for digital signatures. With esignatur's solution, it is ensured that all European laws are respected in relation to sensitive information and valid digital signatures. If you would like more information about digital documents signed with esignatur, please visit our website at www.esignatur.dk.