AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 31. AUGUST 2024 OM BESKRIVELSEN AF KONSULENTFORRETNING VED BRUG AF MICROSOFT PRODUKTER 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

JCD A/S

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 31. AUGUST 2024 OM BESKRIVELSEN AF KONSULENTFORRETNING VED BRUG AF MICROSOFT PRODUKTER 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 JCD A/S
JCD A/S kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af JCD A/S (databehandleren) pr. 31. august 2024 udarbejdede beskrivelse i sektion 3 af konsulentforretning ved brug af Microsoft produkter 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 revisionsaktieselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen 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 konsulentforretning ved brug af Microsoft produkter, 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 konsulentforretning ved brug af Microsoft produkter 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. 31. august 2024, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 31. august 2024.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens konsulentforretning ved brug af Microsoft produkter, 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 16. september 2024

BDO Statsautoriseret revisionsaktieselskab

Claus Bonde Hansen
Partner, Statsautoriseret revisor

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

2. JCD A/S UDTALELSE

JCD A/S varetager behandling af personoplysninger i forbindelse med konsulentforretning ved brug af Microsoft produkter 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 konsulentforretning ved brug af Microsoft produkter, 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.

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

JCD A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af konsulentforretning ved brug af Microsoft produkter og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 31. august 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for konsulentforretning ved brug af Microsoft produkter, 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 konsulentforretning ved brug af Microsoft produkter har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af konsulentforretning ved brug af Microsoft produkter og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved konsulentforretning ved brug af Microsoft produkter, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

JCD A/S bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 31. august 2024. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

JCD A/S 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 databehandler i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Aalborg, den 16. september 2024

JCD A/S

Per Kristoffersen
Adm. direktør

3. JCD BESKRIVELSE AF KONSULENTFORRETNING VED BRUG AF MICROSOFT PRODUKTER

JCD A/S

JCD er en dansk- og medarbejderejet virksomhed med Microsoft partnerskab, der udbyder konsulentydelser med udgangspunkt i primært Microsoft Dynamics Business Central/NAV, Azure, Power platformen og IT-Infrastruktur løsninger til forskellige brancher på det private og offentlige marked, hvor personoplysningerne er placeret hos den dataansvarlige eller en anden leverandør, som den dataansvarlige anvender som databehandler.
JCD har hovedkontor i Aalborg og en afdeling i Glostrup. JCD's ca. 70 medarbejdere er specialiserede inden for implementering af Microsoft produkter, systemudvikling, serverdrift, support samt salg. JCD er organiseret i følgende afdelinger:

- Dynamics - Udviklings-, drifts-, og supportopgaver af Business Central/NAV
- It-Infrastruktur - Opsætning, tilpasning, opdatering og support
- Modern Workplace - Udviklings- drifts- og supportopgaver
- WEB - Udvikling, integrationer og supportopgaver
- Udvikling - Udvikling, systemopbygning og support
- Salg - Opsøgende salg af JCD produktporteføljen
- Brand & Kommunikation - Leadgenerering, brand awareness og online marketing
- Administration - Bogholderi, HR, Jura, m.v.

Nærværende systembeskrivelse vedrører udelukkende vores konsulentforretning, dermed de konsulentydelser der leveres af vores Dynamics- og IT-infrastrukturafdeling. Ydelserne omfatter:

- Konfigurationer eller tilpasning af systemer
- Systemudvikling
- Implementering af standard systemer
- Tilpasning af netværk
- Tilpasning af pc'er og servere
- Support

JCD's ledelse og den GDPR-ansvarlige har ansvaret for JCD's persondatasikkerhed i forhold til den behandling, som JCD 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, sikkerhedsforanstaltninger og procedurer.

JCD A/S OG BEHANDLING AF PERSONOPLYSNINGER

JCD's konsulentforretning leverer konsulentydelser i form af udvikling, konfiguration/tilpasning, implementering, drift eller support med udgangspunkt i Microsoft Dynamics Business Central/NAV, Power Platformen eller It-Infrastruktur løsninger i henhold til indgåede aftaler med dataansvarlige og altid på dennes instruks. I forbindelse med leverancen kan JCD i kortere eller længere perioder behandle personoplysninger på vegne af dataansvarlige.

Da JCD's konsulentforretning i høj grad anvender Microsoft produkter i sine leverancer, og i visse tilfælde opbevarer kundens personoplysninger ved Microsoft, benyttes Microsoft som underdatabehandler. Andre underdatabehandlere benyttes i visse tilfælde, hvilket altid vil fremgå af gældende databehandleraftale med dataansvarlige. JCD har indgået databehandleraftaler med disse underdatabehandlere.

JCD behandler personoplysninger på vegne af sine kunder, der er dataansvarlige, når disse tilkøber konsulentydelser af JCD. Disse personoplysninger er i alle tilfælde undtagen ét placeret hos den dataansvarlige eller en anden leverandør, som den dataansvarlige anvender som databehandler. Der vil kun kortvarigt og efter specifik instruks fra den dataansvarlige ske kortvarig lagring af personoplysninger hos databehandleren, fx i

forbindelse med konverteringsopgaver. JCD har indgået databehandleraftaler med de dataansvarlige om denne behandling.

De personoplysninger, der behandles, henhører under databeskyttelsesforordningens artikel 6 om almindelige personoplysninger og artikel 9 om fortrolige og/eller følsomme personoplysninger. Dataansvarlig vælger selv, hvilke personoplysninger der behandles. Disse omfatter blandt andet, men er ikke nødvendigvis begrænset til; loginoplysninger, navn, adresse, e-mailadresse, fødselsdato, telefonnummer, CPR-nummer, køn, job titler, arbejdsgiver, ansættelsesdato, løninformationer, arbejdstider, fravær, sygedage (men ikke årsag), kontaktoplysninger, ID-data, forbindelsesdata, lokaliseringsdata, skatteoplysninger, kontonummer, skat og gæld, billede, tv-overvågning eller video af personer samt ansøgninger.

STYRING AF PERSONDATASIKKERHED

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

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:

DATABEHANDLERAFTALEN	KONTROLOMRÅDE	Artikel
Kontrolmål A Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.	• Databehandleraftale med den dataansvarlige • Instruks for behandling af personoplysninger	• Artikel 28, stk. 3 • Artikel 28, stk. 3, litra a • Artikel 29 • Artikel 32, stk. 4 • Artikel 28, stk. 10 • Artikel 28, stk. 3, litra h
Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Tekniske og organisatoriske sikkerhedsforanstaltninger • Databeskyttelse gennem design og standardindstillinger	• Artikel 28, stk. 3, litra c • Artikel 25
Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Databehandlerens garantier • Fortrolighed og lovbestemt tavshedspligt. • Bistand til den dataansvarlige vedrørende behandlingssikkerhed og konsekvensanalyser • Bistand til den dataansvarlige vedrørende revision og inspektion.	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra b • Artikel 28, stk. 3, litra f • Artikel 28, stk. 3, litra h • Artikel 30, stk. 2, 3 og 4

DATABEHANDLERAFTALEN	KONTROLOMRÅDE	Artikel
	• Fortegnelse over kategorier af behandlingsaktiviteter	
Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.	• Sletning og tilbagelevering af personoplysninger	• Artikel 28, stk. 3, litra g
Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	• Opbevaring af personoplysninger	• Artikel 28, stk. 3, litra c
Kontrolmål F 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.	• Underdatabehandleraftaler og instruks	• Artikel 28, stk. 2 og 4
Kontrolmål G Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.	• Overførsel af personoplysninger til tredjelande	• Artikel 44 - 49
Kontrolmål H 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.	• Bistand til den dataansvarlige i forhold til de registreredes rettigheder	• Artikel 28, stk. 3, litra e
Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.	• Underretning om brud på persondatasikkerheden • Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden	• Artikel 33, stk. 2 • Artikel 28, stk. 3, litra f

RISIKOVURDERING

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

Generelt vurderes risikoen for de registreredes rettigheder som lav for så vidt angår den behandling JCD foretager henset til, at data i næsten alle tilfælde opbevares hos den dataansvarlige eller dennes øvrige databehandler og at persondatabehandlingen i al væsentlighed er sekundær i forhold til de primære ydelser. Hertil kommer, at der primært er tale om behandling af almindelige personoplysninger.

JCD styrer risici i forbindelse med behandling af personoplysninger ud fra følgende risikostyringsproces:

1. Identifikation af potentielle risici, som behandlingen medfører.
2. Vurdering af de identificerede potentielle risici, væsentlighed, sandsynlighed og konsekvenser for behandlingen.
3. Vurdering af, hvad der er passende tekniske og organisatoriske sikkerhedsforanstaltninger til reduktion af sandsynligheden for at risici indtræder.

I risikovurderingen 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. I vurderingen indgår kortlægning af alle kendte risici, behandlingen medfører, og en kategorisering heraf, samt tiltag til minimering af kortlagte risici.

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.

DATABEHANDLERAFTALE

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

INSTRUKS FOR BEHANDLING AF PERSONOPLYSNINGER

JCD har indført politikker og procedurer, der sikrer, at JCD handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der sikrer at medarbejderne udelukkende behandler personoplysninger ud fra instruks, herunder hvem der hos den dataansvarlige kan give bindende instruks til JCD. JCD har desuden en procedure der sikrer, at JCD informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

Risikovurdering

JCD 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.

Beredskabsplaner

JCD har etableret en beredskabsplan, så JCD rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. JCD har etableret et kriseberedskab, der træder i kraft i disse tilfælde. Organisering af kriseberedskabsgruppe er etableret, og der indført retningslinjer for aktivering af kriseberedskabet.

Fysisk adgangskontrol

JCD 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.

JCD og JCD's hostingleverandør 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. Fysiske adgange til JCD's kontorer og faciliteter gennemgås løbende og mindst én gang årligt.

Fysisk sikkerhed

JCD 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.

JCD finder anvendelse af underdatabehandlere vedr. leverance af konsulentydelser. Der føres årligt tilsyn og bliver indhentet relevante certificeringer fra underdatabehandlerne, hvis fundet nødvendigt på baggrund af risikovurdering.

Logisk adgangssikkerhed

JCD 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.

Fjernarbejdspladser og fjernadgang til systemer og data

JCD har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for JCD's lokaler og fjernadgang til systemer og data sker via krypteret VPN-forbindelser med to-faktor autentifikation.

Eksterne kommunikationsforbindelser

JCD's eksterne kommunikationsforbindelser er sikret med stærk kryptering, og e-mail og anden kommunikation, der indeholder følsomme personoplysninger, er krypteret i forsendelsen ved anvendelse af TLS.

Kryptering af personoplysninger

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

JCD har indført procedurer, der sikrer, at data på personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, er krypteret ved ibrugtagning, så 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.

Firewall

JCD har indført procedurer, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Netværkssikkerhed

JCD har indført procedurer, der sikrer, at netværk i forhold til anvendelse og sikkerhed er opdelt i et antal virtuelle netværk (VLAN), hvor trafik mellem de enkelte virtuelle netværk kontrolleres af firewall. Servere med indbygget firewall benytter denne til at sikre, at der kun gives adgang til nødvendige services.

Antivirusprogram

JCD 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.

Sårbarhedsscanning og penetrationstests

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

Sikkerhedskopiering og retablering af data

JCD har indført procedure, der sikrer, at systemer og data, der indeholder personoplysninger, sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alter-

nativ lokation. Sikkerhedskopier er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde, eller at sikkerheds-kopier ødelægges ved brand, vand, hærværk eller hændelig skade.

Vedligeholdelse af systemsoftware

JCD 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.

Logning i systemer, databaser og netværk

JCD har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret mod tab og sletning.

Overvågning?

JCD har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger, hvis kunden ønsker det.

Reparation og service samt bortskaffelse af it-udstyr

JCD 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.

Afprøvning, vurdering og evaluering

JCD har indført procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

DATABESKYTTELSE GENNEM DESIGN OG STANDARDINDSTILLINGER

JCD har indført politikker og procedurer for udvikling og vedligeholdelse af JCD udviklede Business Central tilpasninger og Modern Workplace løsninger, der sikrer en styret ændringsproces. Der anvendes et Change Management system til styring af udviklings- og ændringsopgaver, og enhver opgave følger en ensartet proces, der indledes med risikovurdering i overensstemmelse med kravene om databeskyttelse gennem design og standardindstillinger.

Udviklings-, test- og produktionsmiljø er adskilte, og der er etableret funktionsadskillelse mellem medarbejdere i udviklingsafdelingen og i drifts- og supportafdelingen. Enhver udviklings- og ændringsopgave gennemløber et testforløb, og der anvendes anonymiserede produktionsdata som testdata. Der anvendes versionsstyringssystem.

DATABEHANDLERENS GARANTIER

JCD har indført politikker og procedurer, der sikrer, at JCD 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. JCD har

etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik og databeskyttelsespolitik, der løbende, og minimum en gang årligt, gennemgås og opdateres. 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

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

BISTAND TIL DEN DATAANSVARLIGE I FORHOLD TIL BEHANDLINGSSIKKERHED OG KONSEKVENSANALYSE

JCD har indført politikker og procedurer, der sikrer, at JCD kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed og artikel 36 om konsekvensanalyser.

BISTAND TIL DEN DATAANSVARLIGE I FORHOLD TIL REVISION OG INSPEKTION

JCD har indført politikker og procedurer, der sikrer, at JCD kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige. JCD giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

FORTEGNELSE OVER KATEGORIER AF BEHANDLINGSAKTIVITETER

JCD 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. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

SLETNING OG TILBAGELEVERING AF PERSONOPLYSNINGER

JCD 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 PERSONOPLYSNING

JCD 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. Opbevaring af persondata sker hos underdatabehandlere, som varetager drift af kundernes systemmiljøer, JCD vil i begrænset omfang opbevare personoplysninger i forbindelse med datakonverteringer ved skift af systemer.

UNDERDATABEHANDLERE

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

JCD vurderer underdatabehandleren og dennes garantier, forinden der indgås aftale, for at sikre, at underdatabehandleren kan overholde de forpligtelser, som er pålagt JCD. JCD 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 ISO 27001, ISAE 3000, SOC 2 eller lignende dokumentation.

OVERFØRSEL AF PERSONOPLYSNINGER TIL TREDJELANDE

JCD har indført politikker og procedurer, der sikrer, at overførslen af personoplysninger til underdatabehandlere i lande uden for EU sker i henhold til EU-US Privacy, standardkontrakt eller andet gyldigt overførselsgrundlag og ifølge instruks fra den dataansvarlige.

BISTAND TIL DEN DATAANSVARLIGE I FORHOLD TIL DEN REGISTREREDES RETTIGHEDER

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

UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

JCD 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 JCD er blevet opmærksom på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at vurdere, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

BISTAND TIL DEN DATAANSVARLIGE I FORHOLD TIL BRUD PÅ PERSONDATASIKKERHEDEN

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

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 skal sikre, at instruksen fra den dataansvarlige er lovlig i forhold til den til enhver tid gældende databeskyttelseslovgivning, og at instruksen er hensigtsmæssig i forhold til den indgåede kontrakt og databehandleraftalen.
- Den dataansvarlige er forpligtet til ikke at indskrive fortrolige og/eller følsomme personoplysninger i henhold til databeskyttelsesforordningens artikel 9 i fritekstfelter i JCD udviklede løsninger, medmindre løsningen er udviklet til dette formål.

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 JCD A/S beskrivelse af konsulentforretning ved brug af Microsoft produkter samt for udformningen af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

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

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 31. august 2024.

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 implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.

For de ydelser, som Microsoft leverer inden for systemløsninger til de dataansvarlige, hvor JCD A/S yder support, har vi modtaget SOC 2 type 2 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Continia Software A/S leverer inden for OCR-behandling eller OIO-behandling, har vi modtaget ISAE 3402 type 2 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Atlytix ApS leverer inden for installation og udvikling af Business Intelligence løsninger på Microsoft Power BI, har vi modtaget gennemført tilsynet via et spørgeskema for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som AnyCloud A/S leverer inden for opbevaring af data ved konverteringsopgaver, har vi modtaget ISAE 3000 type 1 erklæring for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Twoday A/S leverer inden for løsninger til kontrakt-og aftalestyring, har vi modtaget ISAE 3402 type 2 erklæring for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Disse underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i JCD A/S beskrivelse af konsulentforretning ved brug af Microsoft produkter og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos JCD A/S, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

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

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet 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.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Indgåelse af databehandleraftale med den dataansvarlige ▶ Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ▶ Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. ▶ Ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, anvender databehandleren en tjekliste, som fastlægger hvad databehandleren kan leve op til. ▶ Databehandleraftaler underskrives og opbevares elektronisk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for indgåelse af databehandleraftaler og observeret, at denne indeholder relevante elementer for indgåelse af databehandleraftaler. Vi har inspiceret skabelon for indgåelse af databehandleraftaler og observeret, at denne indeholder relevante afsnit i forhold til persondatabeskyttelsesloven ud fra de konsulentydelser som databehandleren varetager Vi har stikprøvevis inspiceret indgået databehandleraftale og observeret, at skabelonen er anvendt samt at databehandleren har gennemført punkter på tjekliste. Vi har inspiceret at databehandler har opbevaret databehandleraftaler elektronisk i underskrevet stand.	Ingen afvigelser konstateret.
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens databehandleraftaleskabelon og observeret, at den indeholder instruks fra den dataansvarlige. Vi er ved forespørgsel blevet oplyst om, at databehandler indhenter instruks fra dataansvarlig for behandling af personoplysninger ved indgåelse af databehandleraftale, Vi har for en stikprøve inspiceret indgåede databehandleraftaler og observeret, at de indeholder instruks fra dataansvarlig.	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.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig. ▶ Databehandlerens procedurer gennemgås og opdateres efter behov og minimum en gang årligt. ▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for efterlevelse af indgående instruks fra dataansvarlige og observeret, at der er fastsat retningslinjer og kriterier for vurdering af behandling af persondata Vi har observeret, at proceduren er revurderet i april 2024: Vi har inspiceret databehandlerens databehandleraftaleskabelon og observeret, at denne indeholder instruks fra den dataansvarlige. Vi har inspiceret databehandlerens egenkontrol på efterlevelse af de dataansvarlige instrukser. Kontrollen er udført i april 2024.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig, i tilfælde hvor den dataansvarliges instruks, strider mod databeskyttelseslovgivningen. ▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for underretning af kunde ved ulovlig instruks og observeret, at databehandler skal fastsat retningslinje for underretning af dataansvarlig, hvis databehandleraftalen strider mod databeskyttelseslovgivningen. Vi er på forespørgsel blevet oplyst om, at der ikke har været nogen tilfælde af ulovlig instruks, hvorfor vi ikke har kunnet teste dette.	Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde af ulovlig instruks. Vi kan derfor ikke udtale os om kontrollens implementering. Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for gennemført risikovurdering af databehandlede systemer/processer, som er baseret på risici for datas tilgængelighed, fortrolighed og integritet for de registrerede Vi har inspiceret risikovurderingen og observeret, at sårbarheder i systemer og processer vurderes ud fra de identificerede trusler. Vi har inspiceret dokumentation for, at de foretagne risikovurderinger udarbejdes med det formål at minimere risici ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. Vi har inspiceret databehandlerens risikovurdering og observeret, at den seneste er opdateret i marts 2024.	Ingen afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, beredskabsplanerne er tidssvarende og effektive i kritiske situationer. ▶ Beredskabstest dokumenteres og evalueres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens beredskabsplan og observeret, at denne indeholder processor for hurtig genoprettelse. Vi har observeret, at beredskabsplanen senest er blevet opdateret marts 2024. Vi har inspiceret dokumentation for afprøvning af beredskabsplanen og observeret, at afprøvning er gennemført og resultatet er evalueret og dokumenteret.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang. ▶ Alle adgange registreres og logges. ▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret fysisk adgangskontrol, hvilken styres vha. slusesystem, adgangskort og gæstekort således at kun autoriserede personer med adgangskort kan opnå adgang til bygningen, hvori der opbevares og behandles personoplysninger. Vi har inspiceret adgangslog for log på hoveddør samt adgangslog på adgange til serverrum. Vi har inspiceret at logs gennemgås løbende og minimum 1 gang årligt,	Ingen afvigelser konstateret.
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret og tildeles ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter, herunder krav om to-faktor autentifikation. ▶ Der foretages logning af brugeradgange til systemer ▶ Der foretages mindst en gang årligt gennemgang af brugere og brugerrettigheder. .	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for brugeradministration, hvori der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til almindelige og privilegerede brugere, herunder at adgange tildeles ud fra et arbejdsbetinget behov. Vi har inspiceret dokumentation for, at der er implementeret password krav systemmiljøerne, herunder anvendelse af to-faktor autentifikation. Vi har inspiceret it-sikkerhedspolitikken, som anfører, at password krav skal følges af alle medarbejdere og konsulenter. Vi har inspiceret dokumentation for opsætning og konfigurering af brugeradgangslog. Vi har inspiceret dokumentation for gennemført review af brugere og brugerrettigheder.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. ▶ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse ▶ Fjernadgang skal foregå via to-faktor autentifikation	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitikken. Vi har inspiceret at mobile enheder har installeret antivirus ud fra centralt styrede AD policy procedurer Vi har inspiceret at der er krav og der benyttes krypteret VPN for at tilgå systemer i JCD fra eksterne lokationer Vi har inspiceret at der benyttes 2-faktor ved brug af VPN-adgange.	Ingen afvigelser konstateret.
Eksterne kommunikationsforbindelser ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og VPN. ▶ Udveksling af personoplysninger via e-mail, sker vha. SikkerMail løsning. ▶ Eksterne kommunikationsforbindelser er krypteret. ▶ Databehandleren har en oversigt over hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret fastsatte krav til eksterne kommunikationsforbindelse og inspiceret Databehandlerens oversigt over hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk. Vi har inspiceret dokumentation for opsætning af firewalls og VPN-forbindelser på kommunikationsforbindelser. Vi har påset, at der anvendes TLS kryptering på sikker mails Vi har inspiceret databehandlerens netværkstopologitegning og observeret, at medarbejderne skal anvende VPN med kryptering for at kunne komme ind på produktionsmiljøet. Vi har inspiceret at JCD har en oversigt over enheder som har adgang til JCD's netværk.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret at Databehandleren har en oversigt over hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk.	
Kryptering af personoplysninger ▶ Databehandleren har implementeret en krypteringspolitik for kryptering af personoplysninger. Politikken definerer styrken og protokollen for kryptering. ▶ Bærbare medier med personoplysninger krypteres ved overførsel af fortrolige og følsomme personoplysninger via internettet, og der anvendes e-mail-kryptering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret politik for kryptering og observeres, at der er fastsat krav til styrke og protokol for kryptering. Vi har inspiceret opsætning af fjernadgang til systemer og databaser, og observeret, at det kræver krypteret TLS VPN-forbindelse for at tilgå. Vi har inspiceret opsætning af bitlocker på arbejdsenheder	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall efter best-practice standard. ▶ Databehandler konfigurerer firewalls så kun services/porte er åbne ud fra konkrete behov for forbindelser.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for konfigureret firewall og observeret, at der er staget stilling til relevante services/porte. Vi har på forespørgsel fået oplyst, at opsætning af regler i firewall er sket ud fra konkrete behov.	Ingen afvigelser konstateret.
Netværkssikkerhed ▶ Databehandlerens netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Databehandleren anvender kendte netværksteknologier og mekanismer (Firewall/Intrusion DetectionSystem/Intrusion Prevention System) for at beskytte internt netværk.	Vi har inspiceret design af netværk og observeret, at netværket er struktureret ud fra best-practice principper, og at det er segmenteret så interne services ikke kan kommunikere direkte med internettet. Vi har inspiceret dokumentation for implementeret intrusion system.	
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateret med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitik og observeret, at der stilles krav om anvendelse af antivirus, Vi har inspiceret dokumentation for installation af antivirus på servere og klienter, herunder at der er opsat retningslinjer for løbende opdatering af Antivirus software.	Ingen afvigelser konstateret.
Sårbarhedsscanning og penetrationstests ▶ Der udføres årligt en sårbarhedsscanning af databehandlerens netværk. ▶ Databehandleren gennemgår rapporten og følger op på konstaterede svagheder. ▶ Databehandler håndterer/mitigerer eventuelle sårbarheder ud fra en risikovurdering. ▶ Databehandler har dokumenteret deres håndtering/mitigering af fundne sårbarheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for udført sårbarhedsskanninger, herunder dokumentation for evaluering af resultatet og igangsætning af handlinger for udbedring af sårbarheder i relevant omfang baseret på en risikovurdering.	Ingen afvigelser konstateret.
Sikkerhedskopiering og retablering af data ▶ Der foretages regelmæssigt backup af systemer og data.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Drift og opbevaring af backup overvåges. ▶ Der udføres restore-tests som minimum årligt.	Vi har inspiceret procedurer for backup og observeret, at der er konfigureret tekniske backup setup til sikring af systemer og data. Vi har inspiceret dokumentation for kørt backup, herunder at resultat af backup logget i det tekniske setup for overvågning Vi har inspiceret dokumentation for gennemført restore-test af sikkerhedskopiering.	
Vedligeholdelse af systemsoftware ▶ Databehandler fører en oversigt over systemsoftware/tredjepartsprogrammer som vedligeholdes og opdateres løbende. ▶ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for vedligeholdelse af system software og observeret, at der er fast kriterie for løbende vedligeholdelse og opdatering af systemsoftware. Vi har inspiceret dokumentation for opdateret liste over godkendte applikationer. Vi har inspiceret opgave i supportsystemet for vurdering og opdatering af systemsoftware.	Ingen afvigelser konstateret.
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer, netværk og data logges. ▶ Alle brugerændringer i system og databaser logges. ▶ Loggen slettes efter den fastsatte retentionsperiode ▶ Databehandler monitorerer og logger netværkstrafik. ▶	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure og logning af systemer, databaser og netværk. Vi har forespurgt til procedurer for logning på systemet, databaser, netværk og data.	Vi har konstateret, at der er konfigureret logning på relevante systemer, men der foreligger ikke en formel procedure med fastsættelse af krav til logning ud fra en risikovurdering af tilstrækkelig logning til identifikation af sikkerhedsbrud og persondatabrud. Ingen yderligere afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret dokumentation for konfiguration af logning på brugere og databaser samt netværk samt når JCD konsulenter logger på kundemiljøerne. Vi har inspiceret opsætning af retention perioden og observeret at denne er fastsat ud fra en risikovurdering. Vi har inspiceret, at log automatisk slettes efter udløb af retentionsperiode.	
Overvågning ▶ Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. ▶ Databehandleren notificeres om identificeret alarmer og følger op herpå.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret overvågningssystem og observeret, at servere med produktionsmiljø bliver overvåget ift. oppetid, ydeevne og kapacitet. Vi har observeret, at databehandleren bliver notificeret med alarmer, og at der sker opfølgning heraf.	Ingen afvigelser konstateret.
Reparation og service samt bortskaffelse af it-udstyr ▶ Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger. ▶ Databehandleren fører en oversigt af destrueret it-udstyr. ▶ Databehandleren foretager sikker sletning af data på databærende medier	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret at der er procedure for aflevering af udstyr til skrotning. Vi har inspiceret at databehandleren fører en oversigt over destrueret udstyr. Vi har inspiceret, at sletning af persondata på databærende medier varetages af ekstern samarbejdspartner på en sikker måde.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurdere og evaluerer effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. De data som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for afprøvning, vurdering og evaluering af effektiviteten af sikkerhedsforanstaltninger og observeret, at proceduren har til formål at sikre sikkerhedsforanstaltninger er passende og effektive for de data der behandles på vegne af den dataansvarlig. Vi har inspiceret dokumentation for, at vurderingen er gennemført.	Ingen afvigelser konstateret.
Udvikling og vedligeholdelse af systemer ▶ Risikovurdering af systemændringer er udført for, at sikre databeskyttelse gennem design og standardindstillinger. ▶ Databehandleren arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelses opgaver.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for udviklingsproces og observeret, at der udvikles ud fra principper om databeskyttelse, herunder at der gennemføres risikovurdering af ændringerne Vi har inspiceret dokumentation for et udviklingsprojekt og konstateret, at procedure for udviklingsproces samt krav til risikovurdering er fulgt. Det er her observeret at der kun arbejdes med anonymiserede person/kunde data i udviklingsprocessen.	Ingen afvigelser konstateret.
Informationssikkerhed i udvikling og ændringer ▶ Databehandler arbejder ud fra security-by-design principper i udviklings- og ændringsopgaver.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Brugeroprettelse sker som udgangspunkt med laveste brugerrettighedsniveau ud fra et arbejdsbetinget behov. ▶ Kun databehandlerens udviklere har adgang til kildekode.	Vi har inspiceret procedure for udviklingsproces og observeret, at der udvikles ud fra principper om security-by-design, herunder at der gennemføres risikovurdering af ændringerne Vi har inspiceret brugeradministration til udviklingssystemer og observeret, at dette sker efter godkendelse og ud fra et arbejdsbetinget behov Vi har inspiceret dokumentation for kontrol af bruger adgange og rettigheder i udviklingssystemet, herunder at adgang kun er givet til udviklere.	
Adskillelse af udviklings-, test og produktionsmiljø ▶ Der er indført funktionsadskillelse mellem udvikling og drift. ▶ Der benyttes et versionsstyringssystem som registrerer alle ændringer i kildekode.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for udviklingsproces og observeret, at der er etableret adskillelse af systemmiljøer. Vi har inspiceret dokumentation for etableret funktionsadskillelse i systemmiljøerne. Vi har inspiceret dokumentation og observeret, at der benyttes et versionsstyringssystem som registrerer alle ændringer i kildekoden.	Ingen afvigelser konstateret.
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes funktionelt og/eller anonymiseret testdata i udviklings- og testmiljø.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at der ikke benyttes persondata i test miljøerne.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Supportopgaver ▶ Supporteres adgange og håndtering af personoplysninger ved supportopgaver sker ud fra support tickets og supporterens arbejdsbetingede behov ▶ Adgang til kundemiljøer logges	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for at supporters adgang og observeret, at håndtering og adgang til personoplysninger udføres ud fra support tickets. Vi har inspiceret dokumentation for, at der regelmæssigt følges op på supportadgange. Vi har inspiceret log over supporteradgange til kundemiljøer.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Informationssikkerhedspolitik ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik Vi har inspiceret, at databehandleren har udarbejdet og implementeret en databeskyttelsespolitik.	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt. ▶ Databehandlerens databeskyttelsespolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for at informationssikkerhedspolitik og databeskyttelsespolitik revurderet, og at dette er fastsat til at ske minimum en gang årligt.	Ingen afvigelser konstateret.
Organisering af informationssikkerhedspolitik ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed og databeskyttelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret Databehandlerens ISMS og observeret, at der etableret ledelsesstyring af informationssikkerhed og databeskyttelse.	Ingen afvigelser konstateret.
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere efter behov før ansættelse.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret procedure for rekrutteringsprocessen hos databehandleren og observeret, at der stille krav om screening af ansøgere efter behov. Vi har inspiceret log over ansatte og observeret, at der er taget stilling til eventuel screening.	
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for off bording processen. Vi har inspiceret dokumentation for gennemført off-bording af en medarbejder	Ingen afvigelser konstateret.
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger samt Awareness og oplysning af medarbejdere. ▶ Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og informationssikkerhed, i forlængelse af ansættelsen. ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. ▶ Databehandleren foretager løbende uddannelse og Awareness af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for awareness og træning til eksisterende og ny medarbejdere. Vi har inspiceret dokumentation for, at der er afholdt introduktionskursus for nye medarbejdere. Vi har inspiceret dokumentation for, at der er afholdt løbende uddannelse og medarbejdere i databeskyttelse og informationssikkerhed.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Alle medarbejdere har underskrevet en tavsheds- og fortrolighedsaftale. ▶ Eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for indgåelse af kontrakt med medarbejdere og eksterne konsulenter og observeret, at der stilles krav og tavshedspligt. Vi har inspiceret skabelon til ansættelseskontrakt og observeret, at der er bestemmelse om tavshedspligt. Vi har inspiceret underkrevet ansættelseskontrakt og observeret, at skabelonens bestemmelser om travhedspligt er videreført.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til behandlingssikkerhed og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32 og 35-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for bistand til den dataansvarlige i forhold til artikel 32 og 35-36.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til revision og inspektion ▶ Databehandler bistår den dataansvarlige ved at stille ressourcer til rådighed i forbindelse med et fysisk tilsyn ▶ Databehandleren stiller den nødvendige information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren. ▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandler vil bistå den dataansvarlige ved at stille ressourcer til rådighed i forbindelse med et fysisk tilsyn, samt for tilsynsmyndigheden ved revision og inspektion af databehandleren. Vi har inspiceret databehandlerens databehandleraftaleskabelon og observeret, at databehandleren er forpligtet til at stille en ISAE	Vi har på forespørgsel fået oplyst, at databehandler vil bistå den dataansvarlige og/eller tilsynsmyndigheden i forhold til revision og inspektion, men at der ikke har været henvendelser fra disse. Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	3000 GDPR-erklæring til rådighed for den dataansvarlige med oplysninger, der påviser, om databehandleren overholder databehandleraftalen. Vi har på forespørgsel fået oplyst, at der ikke har været forespørgsel fra dataansvarlig eller tilsynsmyndighederne på bistand, hvorfor vi ikke har kunnet efterprøve kontrollen.	
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for fortegnelse over behandlingsaktiviteter og observeret, at den løbende er blevet opdateret i perioden, samt at den opbevares elektronisk.	Ingen afvigelser konstateret.
Opbevaring af og adgang til fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev. ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret fortegnelse over behandlingsaktiviteter og observeret, at den løbende er blevet opdateret i perioden, samt at den opbevares elektronisk Der har på erklæringstidspunktet ikke været anmodning fra Datatilsynet vedrørende adgang til fortegnelsen. Det har derfor ikke været muligt at teste kontrollen i forbindelse hermed.	Vi har på forespørgsel fået oplyst, at der ikke været anmodning fra Datatilsynet vedrørende adgang til fortegnelsen. Det har derfor ikke været muligt at teste kontrollen i forbindelse hermed. 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.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning eller tilbagelevering af personoplysninger ▶ Databehandleren sletter eller tilbagelevere den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen. ▶ Dataansvarlig og databehandler har aftalt i hvilket format, overførelse og medie data skal tilbageleveres, når det anmodes af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for sletning/tilbagelevering og observeret, at der forligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning/tilbagelevering af personoplysninger i overensstemmelse med aftalen med dataansvarlig. Det er oplyst af databehandleren at der ikke har været kunde sager, hvor databehandleren har opbevaret personoplysninger, som skal slettes eller tilbageleveres ved ophør af samarbejdet, hvorfor det ikke er muligt at teste kontrollen i forbindelse hermed.	Vi har på forespørgsel fået oplyst, at der ikke været anmodning fra de dataansvarlige på sletning eller tilbagelevering af persondata. Det har derfor ikke været muligt at teste kontrollen i forbindelse hermed. 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.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Opbevaring af personoplysninger ▶ Personoplysninger opbevares utilgængeligt for medarbejdere medmindre de har et arbejdsbetinget behov for adgang. ▶ Personoplysninger opbevares kun så længe der er hjemmel/en legitim grund.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for adgangsstyring til områder indeholdende personoplysninger og observeret, at adgange tildeles ud fra et arbejdsbetinget behov. Vi har via forespørgsel fået oplyst, at alle persondata slettes efter en datakonvertering.	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.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftaler og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler i relevant omfang. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandlers indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har via forespørgsel fået oplyst proces for indgåelse af databehandleraftaler med underdatabehandlere. Vi har inspiceret oversigt over indgåede DBA med underdatabehandlere og observeret, at databehandleraftalen i relevant omfang pålægger underdatabehandleren minimum de samme databeskyttelsesforpligtelser, som er pålagt databehandleren i instruksen Vi har inspiceret, at databehandleraftaler med underdatabehandler underskrives og opbevares elektronisk. Vi har inspiceret, at databehandleraftaler med underdatabehandlers indeholder informationer om brugen af underdatabehandlere	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for godkendelse af underdatabehandler. Vi har inspiceret oversigt over godkendte underdatabehandlere og observeret, at disse fremgår af databehandlerens standard for databehandleraftaler. Vi har inspiceret en kundeaftale og observeret, at denne henviser til databehandlerens standard DBA.	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.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Ændringer i godkendte underdatabehandlere ▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere. ▶ Databehandler underretter dataansvarlig og indhenter specifik skriftlig godkendelse fra dataansvarlig ved ændringer i underdatabehandlere. ▶ Dataansvarlig har mulighed for at gøre indsigelse vedrørende udskiftning af underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for ændringer i godkendte underdatabehandlere og observeret, at der er fastsat bestemmelser om skriftlig underretning af den dataansvarlige ved ændringer eller udskiftning af underdatabehandlere, hvorved den dataansvarlige får mulighed for at gøre indsigelser. Vi har inspiceret indgået databehandleraftale og observeret, at der ikke må gøres brug af andre underdatabehandlere uden specifikt skriftlig godkendelse.	Ingen afvigelser konstateret.
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet, hvem der er kontaktperson, lokation for behandling samt hvilken type af behandling og kategori af personoplysninger, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret oversigt over godkendte underdatabehandlere og observeret, at den indeholder kontaktperson, lokation for behandling samt type af behandling.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandler udfører tilsyn af underdatabehandler efter behov og minimum en gang om året, baseret på en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret kontrol for tilsyn med underdatabehandlere og observeret, at dette sker ud fra en risikovurdering af de enkelte underdatabehandleres sandsynlighed og konsekvens for databehandleren Vi har konstateret, at grundlag for tilsynet er baseret på ISAE revisionserklæringer, certifikater samt spørgeskemaer.	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.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret tilsyn og observeret, at tilsyn er planlagt og gennemført ud fra en konkret risikovurdering.	

Kontrolområde G		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Overførsel af personoplysninger til tredjelande ▶ Databehandleren overfører kun personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige. ▶ Databehandleren vurderer og dokumenterer, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for håndtering af underdatabehandlere og observeret, at denne indeholder bestemmelse om, at der ikke må ske overførelser til tredjelande. Vi har inspiceret databehandlerens standarddatabehandleraftale og observeret, at det heraf fremgår, at data ikke må behandles uden for EU/EØS uden den dataansvarliges samtykke. Vi har inspiceret oversigt over underdatabehandlere og observeret, at alle opbevarer data i EU i relation til Microsoft, har vi inspiceret, at persondata forefindes i EU og at Microsoft har tilsluttet sig EU-U.S. Data Privacy Framework (DPF).	Ingen afvigelser konstateret.

Kontrolområde H		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsninger af oplysninger om behandling af personoplysninger til den registrerede.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Bistand til den dataansvarlige i forhold til de registreredes rettigheder ▶ Databehandler har udarbejdet en procedure for bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for bistand til de dataansvarlige ved opfyldelse af de registreredes rettigheder Vi har inspiceret databehandlerens databehandleraftaleskabelon og observeret, at denne fastsætter bestemmelser omkring bistand af de registreredes rettigheder.	Ingen afvigelser konstateret.

Kontrolområde I		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for brud på persondatasikkerheden og observeret, at den indeholder krav til underretning af dataansvarlig og tilsynsmyndighed. Vi har på forespørgsel fået oplyst, at databehandleren ikke har været ramt af brud på persondatasikkerheden. Vi har derfor ikke kunnet teste implementering. Vi har inspiceret at databehandleren har oprettet en sikkerheds-brud 's log til registrering med som er uden hændelser	Vi har på forespørgsel fået oplyst, at der ikke været brud på persondatasikkerheden. Det har derfor ikke været muligt at teste kontrollen i forbindelse hermed. Ingen afvigelser konstateret.
Identifikation og Registrering af brud på persondatasikkerheden ▶ Databehandleren har opsat foranstaltninger til at identificere brud på persondatasikkerheden. ▶ Databehandleren har opsat foranstaltninger til at identificere brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for log på persondatasikkerheds brud og observeret, at databehandledes har opsat en log med tidslinje Vi har inspiceret loggen for brud på persondatasikkerhed og observeret, at denne log er tom, da der ikke har været nogle registrerede brud og dermed heller ikke input til erfaringsskabelonen. Vi har inspiceret databehandlerens procedure til erfaringsopsamling ved brud på persondatasikkerheden.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 33-34.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde I		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har foretaget inspektion af procedure for persondatabrud og observeret, at denne indeholder krav til, at databehandleren skal bistå den dataansvarlige ved deres anmeldelse til Datatilsynet.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

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."

Claus Bonde Hansen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Statsautoriseret revisor
Serienummer: 92ede3e7-9e85-40a7-9d75-0bcfcab9c71a
IP: 212.237.xxx.xxx
2024-09-16 18:45:32 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 62.66.xxx.xxx
2024-09-16 19:03:29 UTC

Per Nejstskov Kristoffersen
Adm. direktør
Serienummer: 7888a78b-3679-48b3-84bb-6d785c34d5f8
IP: 195.97.xxx.xxx
2024-09-17 06:21:33 UTC