MEMOX APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED BEGRÆNSET SIKKERHED PR. 31. MARTS 2023 OM BESKRIVELSEN AF DE SOCIALFAGLIGE YDELSER 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

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED BEGRÆNSET SIKKERHED PR. 31. MARTS 2023 OM BESKRIVELSEN AF DE SOCIALFAGLIGE YDELSER 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 Memox ApS
Memox ApS's kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om Memox ApS's beskrivelse i sektion 3 af de socialfaglige ydelser pr. 31. marts 2023 og om udformningen og funktionen af 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.

Vores konklusion udtrykkes med begrænset sikkerhed.

Databehandler's ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at 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 Databehandler's 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 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på at opnå begrænset 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, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af de socialfaglige ydelser samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurde-

ringen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. Vores handlinger har ved analyse og forespørgsel omfattet vurdering af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give begrænset sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål 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.

Omfanget af de handlinger vi har udført, er mindre end ved en erklæringsopgave med høj grad af sikkerhed. Som følge heraf er den grad af sikkerhed, der er for vores konklusion, betydeligt mindre end den sikkerhed, der ville være opnået, hvis der var udført en erklæringsopgave med høj grad af sikkerhed.

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

Databehandler's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved de socialfaglige ydelser, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Under vores arbejde er vi ikke blevet bekendt med forhold, der giver os anledning til at konkludere,

a) at beskrivelsen af de socialfaglige ydelser, således som denne var udformet og implementeret pr. 31. marts 2023, ikke i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, ikke i alle væsentlige henseender var hensigtsmæssigt udformet pr. 31. marts 2023.

Beskrivelse af vurdering af kontroller

De specifikke kontroller, der blev vurderet, samt arten, den tidsmæssige placering og resultater af disse vurderinger fremgår i sektion 4.

Tiltænkte brugere og formål
Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens socialfaglige ydelser, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 31. marts 2023

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Brian Bomholdt
Partner, CISA, CISM, CISSP

2. MEMOX APS'S UDTALELSE

Memox ApS behandler socialfaglige personoplysninger på vegne af dataansvarlige i henhold til databehandleraftale.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt de socialfaglige ydelser, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt. Memox ApS bekræfter, at:

1. Den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af de socialfaglige ydelser, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 31. marts 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

    a) Redegør for, hvordan de social faglige ydelser var udformet og implementeret, herunder redegør for:

        - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
        - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og 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 underrettelse til de registrerede
        - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger 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
        - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

    b) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de socialfaglige ydelser til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved behandlingen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

2. De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt udformet pr. 31. marts 2023. Kriterierne anvendt for at give denne udtalelse var, at:

   (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

   (ii) De identificerede kontroller ville, hvis udført som beskrevet, give begrænset sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

3. Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

København, den 31. marts 2023

Memox ApS

Eva Dahl

Eva Thulesen Dahl
HR chef'

3. BESKRIVELSE AF BEHANDLING

INDLEDNING

Memox ApS er en landsdækkende socialfaglig konsulentvirksomhed, der er specialiseret i at tilbyde familiebehandling og andre ydelser i både familier med anden etnisk baggrund og etnisk danske familier i Danmark.

Ydelserne leveres i hovedsagen til kommuner, der ønsker at udlicitere den praktiske ydelse af sine socialretlige forpligtelser.

Memox ApS leverer med andre ord nogle af de ydelser, som kommunerne er forpligtet til at tilbyde sine borgere på basis af serviceloven. Persondataretligt medfører det, at Memox ApS er databehandler for kommunerne. Årsagen hertil er, at Memox ApS leverer sine ydelser og de relaterede behandlinger af personoplysninger på vegne af kommunerne.

Det skal bemærkes, at Memox ApS's hovedydelse består i fysisk tilstedeværelse. Det er således alene den understøttende administration, der er digitalt funderet.

Medfølgende beskrivelser er tilvejebragt med henblik på at give Memox ApS's kunder mulighed for at vurdere, hvorvidt og i hvilket omfang Memox ApS efterlever databehandleraftalen, (jf. Databeskyttelsesforordningens artikel 28, stk. 3, 1. afsnit, litra h).

Memox ApS anvender databehandlere til digital understøttelse af levering af sine ydelser til kunderne, herunder behandlingen af personoplysninger på vegne af kunden.

Memox ApS arbejder risikobaseret med etableringen af tekniske såvel som organisatoriske foranstaltninger med henblik på at værne om de registreredes rettigheder.

Rent organisatorisk er Memox ApS's bestyrelse ansvarlig for persondatasikkerheden. Ansvaret for den praktiske udførelse af arbejdet er placeret hos direktøren. Endelig ligger ansvaret for den praktiske efterlevelse i hverdagen hos alle, der behandler personoplysninger for Memox ApS.

Memox ApS har desuden udarbejdet fortegnelser over behandlingsaktiviteterne. Memox ApS har valgt at inkludere mere information i sine behandlingsfortegnelser end, der stilles krav om i databeskyttelsesforordningens artikel 30, stk. 2. Dette er et bevidst valg, som er truffet med henblik på at få et bedre udgangspunkt for at kunne gennemføre de risikovurderinger, der også følger af Memox ApS's fortegnelser.

DATABESKYTTELSE OG INFORMATIONSSIKKERHED

Memox ApS har politikker og procedurer, der sikrer, at Memox ApS kan stille tilstrækkelige garantier over for sine kunder i overensstemmelse med kundernes forpligtelser efter artikel 28, stk. 1.

Garantierne er etableret med henblik på at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger, så behandlingen opfylder kravene i databeskyttelsesforordningen, og sikrer beskyttelse af den registreredes rettigheder.

Memox ApS har en ledelsesforankret organisering af sit arbejde med persondatasikkerheden, hvilket indebærer, at ledelsen godkender Memox ApS's databeskyttelses- og informationssikkerhedspolitikker. Det udfærdigede materiale gennemgås desuden løbende og opdateres efter behov.

Det bemærkes i den forbindelse, at informationssikkerhed som udgangspunkt er stilet mod en organisations evne til at værne om information, der er nødvendig for, at organisationen kan indfri sine strategiske mål. Databeskyttelse er fokuseret på beskyttelsen af personoplysninger, der er en forudsætning for at værne om de registreredes rettigheder og frihedsrettigheder også kendt som deres menneskerettigheder.

I Memox ApS's tilfælde er der et betydeligt overlap mellem de organisationsstrategiske mål, og forpligtelsen til at værne om de registreredes rettigheder, for så vidt angår de behandlingsaktiviteter, som Memox ApS foretager på vegne af sine kommunale kunder.

REKRUTTERING OG FRATRÆDELSE

Memox ApS har procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for uddannelse og instruktion af medarbejdere, som behandler personoplysninger, herunder gennemførelse af awareness og oplysningskampagner.

UNDERVISNING OG AWARENESS

Memox ApS sender løbende relevant information til medarbejderne for at skabe awarness. Det bemærkes, at nyansatte i Memox ApS får samme træning, som øvrige ansatte.

DATABEHANDLERAFTALER - INDGÅELSE

Memox ApS har politikker og procedurer for at sikre, at der indgås databehandleraftaler i tilknytning til kundekontrakterne. Databehandleraftalerne fastsætter betingelserne for behandling af personoplysninger, som Memox ApS foretager på vegne af den dataansvarlige. Memox ApS anvender en skabelon for databehandleraftaler, som relaterer sig til de tjenester, der leveres, herunder information om brugen af underdatabehandlere. Databehandleraftalerne tiltrædes og opbevares elektronisk.

DATABEHANDLERAFTALER – DOKUMENTERET INSTRUKS

Memox ApS har politikker og procedurer, der sikrer, at behandlingen af personoplysninger følger dokumenteret instruks fra den dataansvarlige. Memox ApS sikrer opretholdelse af procedurerne gennem instruktion af sine medarbejdere i, hvorledes behandling af personoplysninger skal ske, herunder hvordan instruks potentielt i strid med databeskyttelseslovgivningen, skal håndteres.

UNDERDATABEHANDLERAFTALER

Memox ApS har politikker og procedurer, som sikrer, at underdatabehandlere pålægges de samme databeskyttelsesforpligtelser, som Memox ApS selv er underlagt i databehandleraftalen mellem kunden og Memox ApS. Derudover er der politikker og procedurer for sikring af, at underdatabehandlerne også kan give tilstrækkelige garantier til beskyttelse af personoplysninger.

Procedurerne sikrer blandt andet, at kunden giver Memox ApS forudgående specifik eller generel skriftlig godkendelse i forhold til de valgte underdatabehandlere, og at ændringer i godkendte underdatabehandlere løbende administreres.

Memox ApS vurderer desuden underdatabehandlerne og deres garantier forud for indgåelse af aftalen. Memox ApS fører også et årligt tilsyn med sine underdatabehandlere, baseret på en risikovurdering af den konkrete behandling, som underdatabehandleren varetager. Tilsynene består i gennemgang af underdatabehandlernes materiale, fx revisorerklæringer af typen ISAE 3000 eller SOC 2 eller lignende dokumentation.

FORTROLIGHED OG TAVSHEDSPLIGT

Memox ApS har politikker og procedurer for at sikre fortrolighed i forbindelse med behandlingen af personoplysninger. Memox ApS's medarbejdere og konsulenter, som håndterer personoplysninger på

vegne af kunderne, er omfattet af forvaltningslovens regler om tavshedspligt. Det indskærpes desuden overfor fratrædende medarbejdere og konsulenter, at tavshedspligten også gør sig gældende efter ansættelsesforholdets ophør.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

Risikovurderinger

Memox ApS gennemfører løbende risikovurderinger med henblik på at afdække og håndtere risici for de registrerede rettigheder og frihedsrettigheder forbundet med de behandlingsaktiviteter, som Memox ApS gennemfører på vegne af sine kunder.

Beredskabsplaner

Memox ApS har aftaler med sine leverandører om etablering af beredskabsplaner således, at tilgængeligheden til personoplysninger kan genoprettes i tilfælde af fysiske eller tekniske hændelser.

Memox ApS har desuden etableret et kriseberedskab, og indført retningslinjer for aktivering af dette.

Opbevaring af personoplysninger

Memox ApS har indført procedurer, der sikrer, at opbevaring af personoplysninger alene finder sted i overensstemmelse med databehandleraftalen med kunden.

Fysisk adgangskontrol

Memox ApS har procedurer og leverandøraftaler, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Det er således kun personer med et arbejdsbetinget behov, der har adgang til lokalerne. Derudover er der etableret særlige sikkerhedsmæssige foranstaltninger er indført for områder, hvor der foretages behandling af personoplysninger. Kunder, leverandører og andre besøgende ledsages, når de er hos Memox ApS.

Der er indgået leverandøraftaler, der sikrer, at adgang til serverrum er tildelt ud fra et arbejdsbetinget behov.

Logisk adgangskontrol

Memox ApS har procedurer og leverandøraftaler, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Brugere oprettes med unikke credentials, som anvendes ved tildeling af adgang til ressourcer og systemer. Brugerrettighedsstyringen sker ud fra et arbejdsbetinget behov. Der foretages gennemgang og ajourføring af de oprettede brugere og deres rettigheder. Processen understøttes af procedurer og kontroller for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Memox ApS følger best practice for så vidt angår adgangskontrollernes længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg. Adgangskontrollerne understøttes af tekniske foranstaltninger.

Fjernarbejdspladser og fjernadgang til systemer og data

Memox ApS har procedurer, der sikrer, at adgang fra de anvendte SaaS-løsninger sker via krypterede forbindelser og ved brug af multi-faktor autentifikation.

Det bemærkes, at Memox ApS ikke har nogle systemer on-premise, hvorfor alle systemer Memox ApS anvender, teknisk set er via fjernadgang. Memox ApS opretholder fortroligheden af personoplysninger i transit ved hjælp af TLS 1.2 eller højere, da alle Memox ApS's systemer er SaaS.

Eksterne kommunikationsforbindelser
Memox ApS har procedurer for at sikre, at kommunikationen med kunderne sker via krypterede forbindelser. Derudover er der mulighed for at gøre brug af end-to-end-kryptering i det omfang, der er behov herfor.

Kryptering af personoplysninger
Memox ApS har politikker og leverandøraftaler, som sikrer, at personoplysninger krypteres i transit og "at rest" i det omfang sidstnævnte er mulig.

Firewall
Memox ApS har politikker og leverandøraftaler, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset til det nødvendige, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Firewall er desuden enablet på Memox ApS's enheder og i Memox ApS's SaaS-miljøer.

Netværkssikkerhed
Memox ApS har politikker og leverandøraftaler for at sikre, at adgangen til og fra Memox ApS's WiFi foregår gennem firewall.

Antivirusprogram
Memox ApS har politikker og leverandøraftaler, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en automatisk og løbende opdatering samt tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselsniveau.

Sårbarhedsscanning
Memox ApS har politikker og leverandøraftaler for at sikre, at der løbende foretage sårbarhedsscanninger.

Vedligeholdelse af systemsoftware
Memox ApS har politikker og leverandøraftaler for at sikre, at systemsoftware opdateres løbende og i overensstemmelse med leverandørernes foreskrifter og anbefalinger.

Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger
Memox ApS har politikker og leverandøraftaler for derigennem at sikre, at behandling af personoplysninger, der foretages på vegne af kunderne, logges i det omfang, det er relevant.

Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger
Memox ApS har politikker og leverandøraftaler for derved at sikre løbende efterprøvning og forbedring af Memox ApS's it-tekniske setup og manuelle processer relateret til behandlingen af personoplysninger.

SLETNING OG TILBAGELEVERING AF PERSONOPLYSNINGER

Memox ApS har politikker og procedurer for derigennem at kunne håndtere sletningen af personoplysninger relateret til et samarbejdes ophør.

BISTAND TIL DEN DATAANSVARLIGE

Memox ApS har politikker og procedurer for håndtering af bistand til sine kunder efter forespørgsel. Politikkerne og procedurerne vedrører alle former for persondataretlige henvendelser fra kunderne, herunder forespørgsler vedrørende de registreredes rettigheder, sikkerhedshændelser og sletning.

FORTEGNELSE OVER KATEGORIER AF BEHANDLINGSAKTIVITETER

Memox ApS har politikker og procedurer for løbende udarbejdelse og vedligehold af fortegnelser over de behandlingsaktiviteter, som Memox ApS varetager på vegne af sine kunder.

UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

Memox ApS har politikker og procedurer, der sikrer, at kunderne orienteres i overensstemmelse med databeskyttelsesreglerne i tilfælde af brud på persondatasikkerheden.

4. KONTROLMÅL, KONTROLAKTIVITETER, VURDERING OG RESULTAT HERAF

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Informationssikkerhedspolitik ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Databehandleren har udarbejdet og implementeret en databeskyttelsespolitik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af, at databehandlerens politikker er udarbejdet.	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 ved forespørgsel fået oplyst, at den daglige ledelse bliver orienteret om ændringer til politikker, og godkender disse, senest marts 2023.	Ingen afvigelser konstateret.
Organisering af informationssikkerhedspolitik ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed. ▶ Databehandler har dokumenteret og etableret ledelsesstyrring af databeskyttelse(politikken).	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens politikker og observeret, at ledelsesstyring er forankret hos den daglige ledelse.	Ingen afvigelser konstateret.
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret rekrutterings- og personalehåndbogen og observeret, at der heri er opsat procedure, som er med til at	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Databehandleren udfører baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	sikre, at medarbejdere underskriver en tavshedserklæring, og at der blandt andet også indhentes børne-& straffeattest. Vi har ved forespørgsel fået oplyst, at børne-og straffeattesterne bliver genindhentet én gang årligt i Q1. Vi har ved seneste ansættelse inspiceret dokumentation for, at procedurerne ved rekruttering er fulgt.	
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at der foreligger tjeklister til brug for offboarding. Vi har for seneste fratrædelse observeret, at der i fratrædelsesbrevet til den fratrædende medarbejder anføres, at tavshedspligten fortsat er gældende efter fratræden.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren udfører løbende awareness-kampagner i form af, opslag, morgenmøder [mv.] ▶ Databehandleren udfører oplysningskampagner for medarbejdere om databeskyttelse og informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at der løbende udsendes mails med awareness informationer til medarbejderne.	Ingen afvigelser konstateret.

Artikel 28, stk. 3: Databehandleraftale		
Kontrolmål ▶ *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Indgåelse af databehandleraftale med den dataansvarlige ▶ Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ▶ Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. ▶ Databehandleraftaler underskrives og opbevares elektronisk. ▶ Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for indgåelse af databehandleraftaler og observeret, at databehandler har en skabelon til brug for indgåelse af databehandleraftaler. Vi har inspiceret seneste indgåede databehandleraftale og observeret, at denne foreligger elektronisk samt, at aftalen indeholder informationer om brugen af underdatabehandlere.	Ingen afvigelser konstateret.

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* ▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
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 seneste indgåede databehandleraftale og observeret, at denne indeholder en instruks fra den dataansvarlige. Vi har på forespørgsel fået oplyst, at databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige i forbindelse med indgåelse af databehandleraftale.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig. ▶ 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 efterlevelse af instruks for behandling af personoplysninger og observeret, at der heri anføres, at opstår der tvivl om, hvorvidt en kundeanmodning skal imødekommes, inddrages den daglige ledelse således, at det sikres, at der alene behandles efter instruks fra den dataansvarlige.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for indgåelse af databehandleraftaler og observeret, at databehandler har en skabelon til brug for indgåelse af databehandleraftaler, herunder at ved brug af underdatabehandlere, så skal de pålægges samme instruks.	Vi har konstateret, at der ikke foreligger underdatabehandleraftaler med alle underdatabehandlere anført i databehandleraftalen med dataansvarlig, hvorfor der ikke foreligger dokumentation for videregivelse af instruks. 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 indgåelse af databehandleraftaler og observeret, at databehandler har en skabelon til brug for indgåelse af databehandleraftaler, hvoraf godkendte underdatabehandlere fremgår. Vi har inspiceret indgået databehandleraftale og observeret, at anvendte underdatabehandlere er godkendt.	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere ▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for indgåelse af databehandleraftaler og observeret, at databehandler har en skabelon til brug for	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler. ▶ Dataansvarlig har mulighed for at gøre indsigelse vedr. udskiftning af underdatabehandler. ▶ Ved udskiftning af underdatabehandler skal databehandleren have en ny forudgående specifik skriftlig godkendelse fra dataansvarlig.	indgåelse af databehandleraftaler, hvoraf proces for godkendelse ved brug af nye underdatabehandlere fremgår. Vi har på forespørgsel fået oplyst, at der ikke er tilkommet nye underdatabehandlere i nyere tid, hvorfor proceduren ikke er testet.	
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at databehandler har udført tilsyn med underdatabehandlere, baseret på en risikovurdering af den konkrete behandling, som underdatabehandleren varetager. Vi har inspiceret ISAE 3000 og ISAE 3402 erklæringer fra KMD og databehandlerens stillingtagelse til observationer heri.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra b: Fortrolighed og tavshedspligt		
Kontrolmål ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet en ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Alle medarbejdere har underskrevet en tavsheds- og fortrolighedsaftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret personalehåndbogen og observeret, at der heri er opsat procedure, som er med til at sikre, at medarbejdere underskriver en tavshedserklæring og oplyses om, at den fortsat er gældende ved fratrædelse. Vi har for seneste ansættelse og fratrædelse inspiceret dokumentation for, at procedurerne er fulgt.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at en procedure for risikovurdering foreligger. Vi har inspiceret databehandlerens ydelseskatalog og fortegnelser over ydelser og observeret, at disse indeholder en risikovurdering med vurdering af identificerede trusler, samt sandsynlighed og konsekvens heraf.	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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren har aftaler med sine leverandører om etablering af beredskabsplaner således, at tilgængeligheden til personoplysninger kan genoprettes i tilfælde af fysiske eller tekniske hændelser. Vi har inspiceret, en procedure for hændelseshåndtering, herunder at den daglige ledelse er ansvarlig for vurdering af hændelsen og igangsætning af proceduren.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Håndtering af inddata- og uddatamaterialer ▶ Databehandler sikrer, at inddata og uddata bliver håndteret med fortrolighed. ▶ Inddata og uddata sikres fortrolighed vha. kryptering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at koordinatorer skal sende "dagbog" til dataansvarlig, og at der ved afsendelse heraf anvendes sikker-mail. Vi har ved forespørgsel fået oplyst, at kommunikation ind og ud af Workzone er krypteret.	Ingen afvigelser konstateret.
Opbevaring af personoplysninger ▶ Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper. ▶ Fortroligheden af digitale personoplysninger opbevares i krypteret form. ▶ Personoplysninger opbevares kun så længe, der er hjemmel/en legitim grund.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at sikkerhedsgrupper er defineret via Active Directory. Vi har inspiceret sikkerhedsgrupper er opsat, således at medarbejdere tildeles rettigheder ud fra et arbejdsbetinget behov. Vi har ved forespørgsel fået oplyst, at kommunikation ind og ud af Workzone er krypteret. Vi har ved forespørgsel fået oplyst, at databehandleren ikke selv kan bestemme opbevaringsfristen for så vidt angår behandling af personoplysninger, der foretages på vegne af dataansvarlig. Vi har inspiceret behandlingsfortegnelsen og observeret, at overordnede retningslinier for opbevaring er indsat heri.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring af, at kun autoriserede personer har adgang.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at det kun er personer med et arbejdsbetinget behov, der har adgang til lokaler hos databehandler, og at kunder, leverandører og andre besøgende ledsages, når de er hos databehandleren.	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. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra et arbejdsbetinget behov. ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation. ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for seneste ansættelse og fratrædelse inspiceret dokumentation for, at der følges en ensartet proces for brugeradministration. Vi har ved forespørgsel fået oplyst, at medarbejdere tildeles adgang ud fra et arbejdsbetinget behov. Vi har inspiceret privilegerede adgangsrettigheder og observeret, at de er tildelt ud fra et arbejdsbetinget behov. Vi har ved forespørgsel fået oplyst, at databehandleren sikrer, at adgang til de anvendte SaaS-løsninger sker via krypterede forbindelser, og vi har observeret, at multi-faktor autentifikation er aktiveret.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at password politik er implementeret i henhold til proceduren herfor.	
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret anti-virus. ▶ 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 observeret, at anti-virusprogrammel er aktiveret og løbende opdateres. Vi har ved forespørgsel fået oplyst, at databehandleren sikrer, at adgang til de anvendte SaaS-løsninger sker via krypterede forbindelser, og vi har observeret, at multi-faktor autentifikation er aktiveret.	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 krypterede.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren sikrer, at adgang til de anvendte SaaS-løsninger sker via krypterede forbindelser, og vi har observeret, at multi-faktor autentifikation er aktiveret. Vi har ved forespørgsel fået oplyst, at koordinatorer skal sende "dagbog" til dataansvarlig, og at der ved afsendelse heraf anvendes sikker-mail.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har ved forespørgsel fået oplyst, at kommunikation ind og ud af Workzone er krypteret.	
Kryptering af personoplysninger ▶ Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. Politikken definerer styrken og protokollen for kryptering. ▶ Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren sikrer, at adgang til de anvendte SaaS-løsninger sker via krypterede forbindelser. Vi har ved forespørgsel fået oplyst, at koordinatorer skal sende "dagbog" til dataansvarlig, og at der ved afsendelse heraf anvendes sikker-mail. Vi har ved forespørgsel fået oplyst, at kommunikation ind og ud af Workzone er krypteret.	Ingen afvigelser konstateret.
Firewall ▶ Firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at firewall er aktiveret på netværket.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Netværkssikkerhed ▸ Databehandlerens netværk er segmenteret, så interne services ikke kan kommunikere direkte med internettet. ▸ Databehandleren anvender kendte netværksteknologier og mekanismer for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværkstopologi, og observeret, at internettet kun kan tilgås igennem firewall. Vi har inspiceret dokumentation for, at firewall er aktiveret på netværket.	Ingen afvigelser konstateret.
Antivirusprogram ▸ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▸ Antivirus-software opdateres løbende og opdateres med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at anti-virusprogrammel er aktiveret og løbende opdateres.	Ingen afvigelser konstateret.
Sårbarhedsscanning ▸ Der udføres årligt en sårbarhedsscanning af databehandlerens netværk. Resultatet dokumenteres i en rapport ▸ Databehandleren gennemgår rapporten og følger op på konstaterede svagheder. ▸ Databehandler håndterer/mitigerer eventuelle sårbarheder ud fra en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren har leverandøraftaler for at sikre, at der løbende foretages sårbarhedsscanninger og opfølgning herpå. Vi har observeret, at patch management er aktiveret som en mitigerende handling.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sikkerhedskopiering og retablering af data ▶ Drift og opbevaring af backup er outsourcet til underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren har leverandøraftaler for at sikre, at der løbende foretages sikkerhedskopier.	Ingen afvigelser konstateret.
Vedligeholdelse af systemsoftware ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren har leverandøraftaler for at sikre, at der løbende foretages opdatering af systemsoftware. Vi har observeret, at patch management er aktiveret.	Ingen afvigelser konstateret.
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at alle ændringer og åbning af filer logges i Workzone, herunder at der ikke skelnes mellem brugere. Vi har inspiceret log, som understøtter dette.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Reparation og service samt bortskaffelse af it-udstyr ▶ Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger. ▶ Databehandleren bortskaffer it-udstyr ved fysisk destruktion af databærende medier. ▶ Databehandleren fører en oversigt over destrueret it-udstyr.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at procedure for reparation og service samt bortskaffelse af it-udstyr foreligger. Vi har ved forespørgsel fået oplyst, at der ikke har været it-udstyr til reparation eller bortskaffelse i nyere tid, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurderer og evaluerer effektiviteten af, at 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 ved forespørgsel fået oplyst, at der er en løbende dialog med it-konsulent ud fra løbende risikovurdering, således at evaluering foretages.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren kan slette og tilbagelevere personoplysninger, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at oplysninger kan fremfindes ved opslag i systemet, men at der ikke har været ophørte hovedaftaler, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Tilbagelevering af personoplysninger ▶ Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at oplysninger kan fremfindes ved opslag i systemet, men at der ikke har været ophørte hovedaftaler, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige

Kontrolmål

- *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
De registreredes rettigheder ▶ Det er muligt at give indsigt i alle oplysninger, der er registreret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at oplysninger kan fremfindes ved opslag i systemet, men at der ikke har været forespørgsler om bistand, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at der ikke har været forespørgsler om bistand, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Revision og inspektion ▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandler bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standardskabelon for en databehandleraftale og observeret, at databehandleren heri forpligter sig til at få udarbejdet en ISAE 3000-erklæring. Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation. Vi har foretaget inspektion af databehandlerens standardskabelon for en databehandleraftale og observeret, at databehandle-	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige		
Kontrolmål ▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	ren heri forpligter sig til at give dataansvarlig mulighed for fysisk tilsyn. Vi har ved forespørgsel fået oplyst, at databehandleren ikke har fået forespørgsler om fysisk tilsyn, hvorfor vi ikke har kunnet efterprøve kontrollen.	

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter

Kontrolmål

- *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.*
- *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.*
- *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens ydelseskatalog og fortegnelser over ydelser og observeret, at disse indeholder behandlingsaktiviteter. Vi har ved forespørgsel fået oplyst, at fortegnelsen løbende opdateres og minimum en gang om året.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Fortegnelsen opbevares elektronisk ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens ydelseskatalog og fortegnelser over ydelser og observeret, at disse opbevares elektronisk og således kan udleveres til Datatilsynet ved anmodning. Vi har ved forespørgsel fået oplyst, at der ikke har været anmodninger herom.	Ingen afvigelser konstateret.

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden

Kontrolmål

- *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.*
- *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*

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. ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelonen for databehandleraftale og observeret, at databehandleren herigennem forpligter sig til at sikre underretning til den dataansvarlige ved brud på persondatasikkerheden. Vi har ved forespørgsel fået oplyst, at der ikke er sket brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har opsat foranstaltninger til at identificere brud på persondatasikkerheden ▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at der ikke er sket brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Registrering af brud på persondatasikkerheden ▶ Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen. ▶ Databehandleren har udarbejdet og implementeret en procedure for erfaringsopsamling ved brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret en procedure for hændelseshåndtering, herunder sikring af registrering af brud og relevante oplysninger til brug for erfaringsopsamling. Vi har ved forespørgsel fået oplyst, at der ikke er sket brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 80