MEMOX APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 31. MARTS 2024 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 SIKKERHED PR. 31. MARTS 2024 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' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Memox ApS' (databehandleren) pr. 31. marts 2024 udarbejdede beskrivelse i sektion 3 af de socialfaglige ydelser 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 de socialfaglige ydelser, 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 de socialfaglige ydelser og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 31. marts 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. marts 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 socialfaglige ydelser, 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 18. april 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Brian Bomholdt
Partner, CISA, CISM, CISSP

2. MEMOX APS' UDTALELSE

Memox ApS varetager behandling af personoplysninger i forbindelse med socialfaglige ydelser 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 de socialfaglige ydelser, 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.

Memox ApS anvender en underdatabehandler. Denne underdatabehandlers relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Memox bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af de socialfaglige ydelser og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 31. marts 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for de socialfaglige ydelser, 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 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 de socialfaglige ydelser 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 de socialfaglige ydelser, som den enkelte dataansvarlige måtte anse for vigtigt efter deres særlige forhold.

Memox ApS bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 31. marts 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.

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

København, den 18. april 2024

Memox ApS

Eva Thulesen Dahl
HR chef

3. MEMOX APS' BESKRIVELSE AF DE SOCIALFAGLIGE YDELSER

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 hovedsageligt til kommuner, der ønsker at udlicitere den praktiske ydelse af deres socialretlige forpligtelser.

Memox ApS leverer med andre ord nogle af de ydelser, som kommunerne er forpligtede 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' 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' 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 deres 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' bestyrelse ansvarlig for persondatasikkerheden. Ansvaret for den praktiske udførelse af arbejdet er placeret hos direktøren. Endeligt 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' fortegnelser.

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

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 etablerede 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' 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' 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.

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

ARTIKEL	OMRÅDE
Artikel 28, stk. 1	Databehandlerens garantier
Artikel 28, stk. 3	Databehandleraftale
Artikel 28, stk. 3, litra a og h, og stk. 10 Artikel 29 Artikel 32, stk. 4	Instruks for behandling af personoplysninger
Artikel 28, stk. 2 og 4	Underdatabehandlere
Artikel 28. stk. 3, litra b	Fortrolighed og lovbestemt tavshedspligt
Artikel 28, stk. 3, litra c	Tekniske og organisatoriske sikkerhedsforanstaltninger
Artikel 28, stk. 3, litra g	Sletning og tilbagelevering af personoplysninger
Artikel 28, stk. 3, litra e, f og h	Bistand til den dataansvarlige
Artikel 30, stk. 2, 3 og 4	Fortegnelse over kategorier af behandlingsaktiviteter
Artikel 33, stk. 2	Underretning om brud på persondatasikkerheden.

RISIKOVURDERING

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

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

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller udføres der en løbende risikovurdering af de ydelser, Memos ApS leverer til dataansvarlige. 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 følgende beskrivelse.

Databehandlerens garantier

Memox ApS har indført politikker og procedurer, der sikrer, at Memox ApS 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. Memox ApS har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende 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.

Databehandleraftale

Memox ApS har politikker og procedurer, der sikrer, 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.

Instruks for behandling af personoplysninger

Memox ApS har indført politikker og procedurer, der sikrer, at Memox ApS handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske. Proceduren sikrer desuden, at Memox ApS informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

Underdatabehandlere

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 lovbestemt tavshedspligt

Memox ApS har politikker og procedurer for at sikre fortrolighed i forbindelse med behandlingen af personoplysninger. Memox ApS' medarbejdere og konsulenter, som håndterer personoplysninger på vegne af kunderne, er omfattede af Forvaltningslovens regler om tavshedspligt. Det indskærpes desuden over for fratrædende medarbejdere og konsulenter, at tavshedspligten også gør sig gældende efter ansættelsesforholdets ophør.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering

Memox ApS gennemfører løbende risikovurderinger med henblik på at afdække og håndtere risici for de registrerede rettigheder og frihedsrettigheder, som er 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, så 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.

Håndtering af inddata- og uddatamaterialer
Memox ApS har indført procedurer for inddata til den anvendte SaaS-løsning, som sker via en krypteret forbindelse.

Memox ApS har indført procedurer for håndtering af uddata fra den anvendte SaaS-løsning, som sikrer, at uddatamateriale kun må behandles af de medarbejdere, der er beskæftigede med behandlingen af personoplysninger, og håndteres på krypterede enheder og forbindelser.

Opbevaring af personoplysninger
Memox ApS har indført procedurer, der sikrer, at opbevaring af personoplysninger på vegne af kunden alene finder sted i overensstemmelse med databehandleraftalen med kunden. Memox ApS opbevarer personoplysninger på vegne af sine kunder i et til formålet udviklet system, der udbydes af en national aktør, og som allerede anvendes af hovedparten af Memox ApS' kunder.

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

Logisk adgangssikkerhed
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 via sikkerhedsgrupper. 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 den anvendte SaaS-løsning sker via krypterede forbindelser og ved brug af multi-faktor autentifikation.

Det bemærkes, at Memox ApS ikke har nogle systemer on-premise, hvorfor alle de systemer, som 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' 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' enheder og i Memox ApS' SaaS-miljøer.

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

Antivirusprogram
Memox ApS har politikker og leverandøraftaler, der sikrer, at enheder med adgang til netværk og applikationer er beskyttede 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
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.

Reparation og service samt bortskaffelse af it-udstyr
Memox ApS har indført procedurer, der sikrer, at udstyr, som udleveres til tredjemand for service, reparation, destruktion eller bortskaffelse registreres og destrueres af autoriseret leverandør.

Afprøvning, vurdering og evaluering
Memox ApS har politikker og leverandøraftaler for derved at sikre løbende efterprøvning og forbedring af Memox ApS' it-tekniske set up og manuelle processer, relaterede til behandlingen af personoplysninger.

Sletning og tilbagelevering af personoplysninger

Memox ApS har politikker og procedurer for derigennem at kunne håndtere sletningen af personoplysninger, relaterede 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, der sikrer løbende udarbejdelse og vedligehold af fortegnelser over de behandlingsaktiviteter, som Memox ApS varetager på vegne af sine kunder. Fortegnelsen opbevares elektronisk, og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

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, 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 Memox ApS beskrivelse af de socialfaglige ydelser 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 udformede.

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 Memox ApS, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 31. marts 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, så 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 KMD A/S leverer inden for WorkZone (ESDH-system), har vi modtaget ISAE 3402 erklæring vedrørende generelle it-kontroller og ISAE 3000 GDPR-erklæring for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. januar til 31. december 2023.

Denne underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Memox ApS' beskrivelse af de socialfaglige ydelser og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos Memox ApS, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

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

En afvigelse foreligger, når:

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

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 databehandleren har udarbejdet en informationssikkerhedspolitik og databeskyttelsespolitik, og observeret, at de er implementerede.	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 foretaget inspektion af, at databehandleren har gennemgået og i nødvendigt omfang opdateret politikkerne i september og december 2023 samt i februar og marts 2024.	Ingen afvigelser konstateret.
Organisering af informationssikkerhedspolitik ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed. ▶ Databehandler har dokumenteret og etableret ledelsesstyrring af databeskyttelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens politikker og observeret, at ledelsesstyring af informationssikkerhed og databeskyttelse er forankret hos bestyrelsen, direktionen og HR-chefen. Vi har inspiceret, at informationssikkerhed og databeskyttelse er gennemgået på bestyrelsesmøde i december 2023.	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**
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse. ▶ Databehandleren udfører baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af rekrutterings- og personalehåndbøger og observeret, at der heri er opsat procedure om udførelse af screening og baggrundstjek af potentielle medarbejdere før ansættelse. Vi har for den seneste fastansatte medarbejder og konsulent inspiceret, at proceduren er implementeret, idet der er foretaget screening og baggrundstjek før ansættelse.	Vi har konstateret, at databehandleren har opbevaret straffeattester i op 12 til måneder trods formålet (selve rekrutteringen og den løbende 12 måneders re-attestation) er afsluttet. Ingen yderligere afvigelser konstateret.
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 foretaget inspektion af databehandlerens procedure for fratrædelse af medarbejdere ved ophør af ansættelse og observeret, at den blandt andet omhandler aflevering af udstyr, nedlukning af brugeradgange og orientering om, at tavshedspligten fortsat er gældende efter fratrædelse. Vi har for den seneste fratrådte medarbejder inspiceret dokumentation for, at fratrædelsesproceduren er implementeret.	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**
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og informationssikkerhed i forlængelse af ansættelsen. ▶ Databehandleren foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at HR-chefen afholder awareness-træning af nye medarbejdere omhandlende databeskyttelse og informationssikkerhed, samt at nye medarbejdere derudover deltager i uddannelsesdage. Vi har foretaget inspektion af databehandlerens procedure for uddannelse og awareness i forhold til informationssikkerhed og databeskyttelse og observeret, at den er implementeret.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren udfører løbende awareness-kampagner i form af opslag, morgenmøder, nyhedsbreve mv. ▶ Databehandleren udfører oplysningskampagner for medarbejdere om databeskyttelse og informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af dokumentation for, at der løbende udsendes mails med awareness-informationer om informationssikkerhed og databeskyttelse til medarbejdere.	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 foretaget inspektion af 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 den er udarbejdet på baggrund af databehandlerens skabelon, at den er underskrevet og opbevaret 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 foretaget inspektion af senest indgåede databehandleraftale og observeret, at denne indeholder en instruks fra den dataansvarlige.	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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af procedure for efterlevelse af instruks for behandling af personoplysninger og observeret, at der er implementeret kontroller af, at der alene udføres behandling af personoplysninger i overensstemmelse med instruks fra dataansvarlige.	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 foretaget inspektion af databehandlerens procedure for underretning til dataansvarlig ved modtagelse af instruks, der strider mod databeskyttelseslovgivningen. Vi er på forespørgsel blevet oplyst, at databehandleren ikke har modtaget instrukser, som strider mod databeskyttelseslovgivningen. Vi har derfor ikke kunne teste implementeringen af kontrollen.	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 dataansvarlige 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 foretaget inspektion af procedure for indgåelse af underdatabehandleraftaler og observeret, at databehandler ved brug af underdatabehandlere skal de pålægges samme databeskyttelsesforpligtelser, som databehandleren er pålagt fra dataansvarlige. Vi har inspiceret underdatabehandleraftalen med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at instrukser fra dataansvarlige er videregivet til underdatabehandleren, og at aftalen er underskrevet og opbevares elektronisk, samt at aftalen indeholder information 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 indgåelse af databehandleraftaler og observeret, at databehandler kun må anvende underdatabehandlere, der er godkendt af dataansvarlige. Vi har inspiceret den senest indgået databehandleraftale og observeret, at anvendte underdatabehandlere er godkendt af 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
Ændringer i godkendte underdatabehandlere ▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere. ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af procedure for indgåelse af databehandleraftaler og observeret, at databehandler har en skabelon til brug for indgåelse af databehandleraftaler, hvoraf proces for godkendelse ved brug af udskiftning og anvendelse af nye underdatabehandlere fremgår. Vi har på forespørgsel fået oplyst, at der ikke har været udskiftet eller tilkommet nye underdatabehandlere i de seneste 12 måneder. Vi har derfor ikke kunne teste implementering af kontrollen.	Ingen afvigelser konstateret.
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. Oversigten over godkendte underdatabehandlere indeholder blandt andet, hvem der er kontaktperson, lokation for behandling samt hvilken type af behandling og kategori af personoplysninger, underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens oversigt over godkendte underdatabehandlere og observeret, at den blandt andet indeholder information om, hvem der er kontaktperson, lokation for behandling, samt hvilken type af behandling og kategori af personoplysninger underdatabehandler foretager.	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
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn, herunder indhentes og gennemgå 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 foretaget inspektion af dokumentation for, at databehandler har udført tilsyn med KMD A/S, baseret på en risikovurdering af den konkrete behandling, som underdatabehandleren varetager. Vi har inspiceret ISAE 3000 erklæring fra KMD A/S for perioden 1. januar til 31. december 2023, og databehandlerens stillingtagen til observationer heri.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra b: Fortrolighed og tavshedspligt		
Kontrolmål ▶ *At sikre, at de personer, der er autoriserede 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af 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 ansættelser inspiceret dokumentation for, at procedurerne er fulgt, og at de ansatte er underlagt tavshedspligt.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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 foretaget inspektion af databehandlerens procedure for risikovurdering og observeret, at denne anfører, at databehandleren løbende, og som minimum en gang årligt, skal foretage risikovurdering af potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder, samt at sårbarheden vurderes ud fra identificerede trusler. Vi har inspiceret databehandlerens ydelseskatalog og fortegnelser over ydelser og observeret, at disse indeholder en risikovurdering fra marts 2024, som beror på identificerede trusler samt sandsynlighed og konsekvens heraf, og de indeholder mitigerende foranstaltninger.	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 foretaget inspektion af databehandlerens procedure for hændelseshåndtering, der skal være med til at sikre hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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 er på forespørgsel blevet oplyst, at der ikke har været relevante hændelser de seneste 12 måneder. Vi har derfor ikke kunne teste implementering af kontrollen. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at KMD har forpligtet til sig rettidigt at kunne genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet genopretning af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.	
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 foretaget inspektion af, at forbindelsen til ESDH-systemet WorkZone er krypteret. Vi har foretaget inspektion af, at når persondata sendes til dataansvarlige, sker dette via en mail-løsning, der sikrer, at mails fremsendes krypteret.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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
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 foretaget inspektion af databehandlerens procedure for adgangsstyring og observeret, at den er implementeret ved anvendelse af sikkerhedsgrupper i Microsoft Entra ID samt for seneste ansatte medarbejdere inspiceret, at de på baggrund af et arbejdsbetinget behov har fået tildelt adgang til personoplysninger i ESDH-systemet WorkZone via sikkerhedsgrupper i Microsoft Entra ID. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at KMD har forpligtet sig til at sikre fortrolighed, integritet og robusthed i WorkZone. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet sikring af fortrolighed, integritet og robusthed. Vi er på forespørgsel blevet oplyst, at alle pc'er, der kan få adgang til dataansvarliges personoplysninger, er krypterede. Vi har for en tilfældig udvalgt pc observeret, at pc'en var krypteret. Vi har på forespørgsel fået oplyst, at databehandleren er reguleret af retssikkerhedsloven § 43, som fastlægger, at databehandleren er underlagt Forvaltningsloven, herunder regler om aktindsigt, og derfor opbevarer personoplysninger i 5 år efter endt forløb, hvilket er hjemlet i artikel 28, stk. 3, 1. afsnit,	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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
	litra g. Vi har videre inspiceret databehandlerens databehandlerskabelon og senest indgåede databehandleraftale og observeret, at der heri også er indskrevet nødvendigheden af at opbevare personoplysninger efter endt forløb, jf. national lovgivning.	
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 foretaget inspektion af databehandlerens beskrivelse af fysiske adgangskontroller, som omhandler forebyggelse af sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring af, at kun autoriserede personer har adgang og har under revisionsbesøget observeret, at de fysiske adgangskontroller var implementerede.	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 autoriserede. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for brugeradministration og observeret, at brugeroprettelser og -nedlæggelser skal følge en styret proces, og at alle brugeroprettelser er autoriserede. Vi har for seneste ansatte medarbejder og seneste fratrådte medarbejder inspiceret, at brugeroprettelsen og brugernedlæggelsen har fulgt 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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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
▸ 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. ▸ Der foretages kvartalsvis gennemgang af brugere og brugerrettigheder.	Vi har foretaget inspektion af, at brugerrettigheder tildeles ud fra et arbejdsbetinget behov. Vi har foretaget inspektion af privilegerede adgangsrettigheder og observeret, at de er tildelt ud fra et arbejdsbetinget behov. Vi har foretaget inspektion af databehandlerens passwordpolitik og anvendelse af to-faktor autentifikation. Vi har foretaget inspektion af databehandlerens procedure for kvartalsvis gennemgang af brugere og brugerrettigheder. Vi har inspiceret, at databehandleren har planlagt næste gennemgang i april 2024.	
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 foretaget inspektion af, at databehandleren har standardinstallationspakker til alle mobile enheder, herunder antivirus. Vi har inspiceret, for en tilfældig udvalgt pc, at der var installeret opdateret antivirus. Vi har foretaget inspektion af, at forbindelsen til ESDH-systemet WorkZone er krypteret, og at der kun kan opnås adgang for brugere, der er oprettede i Microsoft Entra ID.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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 foretaget inspektion af, at der skal anvendes to-faktor autentifikation, før der kan opnås adgang til ESDH-systemet WorkZone.	
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. sikkermailløsning. ▶ Eksterne kommunikationsforbindelser er krypterede.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af, at der kun kan opnås adgang til ESDH-systemet WorkZone for brugere, der er oprettede i Microsoft Entra ID. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at KMD A/S har forpligtet til sig til at have passende tekniske foranstaltninger til beskyttelse af WorkZone. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet firewall og korrekt konfiguration af disse. Vi har foretaget inspektion af, at når persondata sendes til dataansvarlige, sker dette via en mail-løsning, der sikrer, at mails fremsendes krypteret. Vi har foretaget inspektion af, at forbindelsen til ESDH-systemet WorkZone er krypteret.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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
Kryptering af personoplysninger ▶ Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. ▶ 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 foretaget inspektion af databehandlerens krypteringspolitik og observeret, at den er implementeret. Vi har foretaget inspektion af, at når persondata sendes til dataansvarlige, sker dette via en mail-løsning, der sikrer, at mails fremsendes krypteret.	Ingen afvigelser konstateret.
Firewall ▶ Firewalls er konfigurerede og validerede periodisk efter behov, så service/porte kun er åbne efter behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens netværkstopologi og observeret, at der anvendes firewall til at beskytte netværket. Vi har inspiceret konfigurationen af firewall, og vi er på forespørgsel blevet oplyst, at konfigurationen valideres periodisk efter behov, så service/porte kun er åbne efter behov. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at KMD A/S har forpligtet sig til at have passende tekniske foranstaltninger til beskyttelse af WorkZone. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet firewalls og korrekt konfiguration af disse.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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 for at minimere risikoen for uautoriseret adgang til personoplysninger. ▶ Databehandleren anvender kendte netværksteknologier og mekanismer for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi er på forespørgsel blevet oplyst, at der ikke opbevares personoplysninger på databehandlerens netværk. Vi har foretaget inspektion af databehandlerens netværkstopologi og observeret, at internettet kun kan tilgås igennem firewall. Vi har foretaget inspektion af, at firewall er aktiveret på netværket. Vi har foretaget inspektion af, at databehandler overvåger og beskytter netværket via værktøjet Pfsense.	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 foretaget inspektion af, at databehandleren har standardinstallationspakker til alle arbejdsstationer, herunder antivirus. Vi har inspiceret for en tilfældig udvalgt pc, at der var installeret og opdateret antivirus. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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
	WorkZone og observeret, at KMD A/S har forpligtet til sig til at have passende tekniske foranstaltninger til beskyttelse af WorkZone. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet anvendelse af antivirus.	
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 foretaget inspektion af, at databehandleren har udført en sårbarhedsscanning af det interne netværk i marts 2024 og observeret, at sårbarhedsscanningen ikke gav anledning til at iværksætte mitigerende foranstaltninger. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at KMD A/S har forpligtet til sig til at have passende tekniske foranstaltninger til beskyttelse af WorkZone. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet sårbarhedsscanninger.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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 er på forespørgsel blevet oplyst, at databehandleren ikke selv hoster eller drifter systemer, der behandler personoplysninger, ligesom databehandleren ikke selv opbevarer personoplysninger. Dataansvarliges personoplysninger opbevares udelukkende i ESDH-systemet WorkZone. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at KMD A/S har forpligtet til sig til at have passende tekniske foranstaltninger til beskyttelse af WorkZone. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet sikkerhedskopieringer og reetablering af data.	Ingen afvigelser konstateret.
Vedligeholdelse af systemsoftware ▶ Operativsystem-software på 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.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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 for en tilfældig udvalgt arbejdsstation inspiceret, at operativsystem-softwaren var opdateret.	
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger - Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. - Alle brugerændringer i system og databaser logges.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af, at databehandleren har opsat logning af alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer. Vi har foretaget inspektion af databehandlerens underdatabehandleraftale med KMD A/S vedrørende ESDH-systemet WorkZone og observeret, at KMD A/S har forpligtet til sig til at have passende tekniske foranstaltninger til beskyttelse af WorkZone. Vi har inspiceret databehandlerens udførte tilsyn med KMD A/S fra marts 2024 og observeret, at tilsynet blandt andet har omhandlet logning af brugerændringer i systemer og databaser.	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 transmitterede, opbevarede eller på anden måde behandlede.*
- *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 databehandlerens procedure for reparation og service samt bortskaffelse af it-udstyr, herunder fysisk destruktion af databærende medier og observeret, at den er implementeret. Vi har inspiceret, at databehandleren fører en oversigt over destrueret it-udstyr.	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 inspiceret dokumentation for, at databehandleren løbende afprøver, vurderer og evaluerer effektiviteten af, at de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af dataansvarlig.	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 foretaget inspektion af databehandlerens databehandleraftaleskabelon og senest indgåede databehandleraftale og observeret, at der heri gives instruks fra dataansvarlig om, at personoplysninger skal slettes efter endt forløb, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne. Vi har på forespørgsel fået oplyst, at databehandleren er reguleret af retssikkerhedsloven § 43, som fastlægger, at databehandleren er underlagt Forvaltningsloven, herunder regler om aktindsigt. Derfor opbevarer databehandleren personoplysninger i 5 år efter endt forløb. Vi har inspiceret udtræk over sager i Workzone og observeret, at der ikke er opbevaret sager, der er over 5 år gamle efter "afsluttet"-dato.	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 foretaget inspektion af databehandlerens databehandleraftaleskabelon og senest indgåede databehandleraftale og observeret, at der gives mulighed for, at dataansvarlige kan anmode om tilbagelevering af dataansvarliges personoplysninger. Vi er på forespørgsel blevet oplyst, at der ikke har været anmodninger om tilbagelevering af personoplysninger. Vi har derfor ikke kunne teste implementeringen af 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 inspiceret, at oplysninger kan fremfindes ved opslag i ESDH-systemet WorkZone. Vi er på forespørgsel blevet oplyst, at der ikke har været anmodninger om indsigt i personoplysninger. Vi har derfor ikke kunne teste implementeringen af 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 inspiceret databehandlerens procedure vedrørende bistand til dataansvarlige og observeret, at den indeholder en proces for bistand til den dataansvarlige ved opfyldelse af de registreredes rettigheder. Vi er på forespørgsel blevet oplyst, at der har ikke har været henvendelse vedrørende de registreredes rettigheder. Vi har derfor ikke kunne teste implementering af 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
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 databehandleraftaleskabelon og senest indgåede 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 databehandleraftaleskabelon og senest indgåede databehandleraftale og observeret, at databehandleren heri forpligter sig til at give dataansvarlig mulighed for fysisk tilsyn og at stille den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren ikke har fået forespørgsler om tilsyn og revision. Vi har derfor ikke kunne teste implementering af kontrollen.	Ingen afvigelser konstateret.

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 foretaget inspektion af, at databehandleren har etableret fortegnelse over databehandlerens behandlingsaktiviteter som databehandler og observeret, at den senest er opdateret i marts 2024.	Vi har konstateret, at fortegnelse over behandlingsaktivitet anfører, at slettefristen er senest to år efter den enkelte sag er afsluttet, trods vi på forespørgsel har fået oplyst, at databehandleren er reguleret af retssikkerhedsloven § 43, som fastlægger, at databehandleren er underlagt Forvaltningsloven, herunder regler om aktindsigt, og derfor opbevarer personoplysninger i 5 år efter endt forløb. Ingen yderligere 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 foretaget inspektion af fortegnelse over databehandlerens behandlingsaktiviteter som databehandler og observeret, at disse opbevares elektronisk, og således kan udleveres til Datatilsynet ved anmodning. Vi har på forespørgsel fået oplyst, at der ikke har været anmodninger herom. Vi har derfor ikke kunne teste implementering af kontrollen.	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. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for håndtering af brud på persondatasikkerhed og observeret, at den anfører, at databehandleren skal underrette den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse, og ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren, samt at kommunikation gemmes. Vi er på forespørgsel blevet oplyst, og har ved inspektion af databrudslog observeret, at der ikke har været brud på persondatasikkerheden. Vi har derfor ikke kunne teste implementering af 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 foretaget inspektion af, at databehandleren uddanner medarbejdere i identifikation af brud på persondatasikkerhed. Vi har foretaget inspektion af databehandlerens procedure for vurdering og identifikation af brud på persondatasikkerheden. Vi er på forespørgsel blevet oplyst, og har ved inspektion af databrudslog observeret, at der ikke har været brud på persondatasikkerheden. Vi har derfor ikke kunne teste implementering af kontrollen.	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**
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 foretaget inspektion af databehandlerens procedure for hændelseshåndtering, herunder sikring af registrering af brud og relevante oplysninger til brug for erfaringsopsamling. Vi er på forespørgsel blevet oplyst, og har ved inspektion af databrudslog observeret, at der ikke har været brud på persondatasikkerheden. Vi har derfor ikke kunne teste implementering af kontrollen.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

CVR-NR. 20 22 26 70

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

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

Nicolai Tobias Visti Pedersen
Partner, Statsautoriseret revisor
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-04-18 10:32:40 UTC

Brian Bomholdt Nielsen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner, CISA, CISM, CISSP
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: 3583d77e-7e8f-4ecf-80ae-13e70995aadf
IP: 77.243.xxx.xxx
2024-04-18 11:00:47 UTC

Eva Thulesen Dahl
HR- og økonomichef
På vegne af: Memox ApS
Serienummer: 8219358c-b498-463c-a66a-74b7187d6755
IP: 83.93.xxx.xxx
2024-04-19 17:51:53 UTC