REGION NORDJYLLAND
– i gode hænder

REGION NORDJYLLAND

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 31 DECEMBER 2021 OM BESKRIVELSEN AF KIH XDS REPOSITORY 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

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 31. DECEMBER 2021 OM BESKRIVELSEN AF KIH XDS REPOSITORY 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 Region Nordjylland
MedCom, som fællesoffentlig systemforvalter for KIH XDS Repository

Omfang

Vi har fået som opgave at afgive erklæring om den af Region Nordjylland (databehandleren) pr. 31. december 2021 udarbejdede beskrivelse i sektion 3 af KIH XDS Repository 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.

Vi er underlagt den internationale standard om kvalitetsstyring ISQC 1, og vi anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om 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 KIH XDS Repository, 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 KIH XDS Repository 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. december 2021, 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. december 2021.

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 KIH XDS Repository, 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 10. april 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. REGION NORDJYLLANDS UDTALELSE

Region Nordjylland varetager behandling af personoplysninger i forbindelse med KIH XDS Repository 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 KIH XDS Repository, 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.

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

Region Nordjylland bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af KIH XDS Repository og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 31. december 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

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

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af KIH XDS Repository 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 KIH XDS Repository, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

Region Nordjylland 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. december 2021. 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.

Region Nordjylland 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.

Aalborg, den 10. april 2022

Region Nordjylland

Grethe Kiehn Kristensen
Vicekontorchef
Cyber- og Informationssikkerhed

3. REGION NORDJYLLANDS BESKRIVELSE AF KIH XDS REPOSITORY

REGION NORDJYLLAND

Regionens hovedopgave er det nordjyske sundhedsvæsen. Regionen har desuden et overordnet ansvar for den regionale udvikling og tager sig også af specialiserede opgaver på det sociale område og i forhold til handicappede børn og voksne. Regionen dækker et areal på 7.886 km^2. Region Nordjylland består af 11 kommuner og er regional myndighed for 589.936 nordjyder.

Regionen leverer offentlig service til nordjyderne på en række forskellige områder. Regionens vigtigste opgave er drift af sygehuse, sygesikring samt øvrige opgaver på sundhedsområdet. Regionen tager sig også af tværgående regional udvikling og driver sociale tilbud. På næsten alle områder løser regionen sine opgaver i et tæt samarbejde med kommunerne.

Digitalisering og IT er Region Nordjyllands centrale it-afdeling, hvis kerneopgave er at it-understøtte og videreudvikle regionens sundhedsydelser, samt at bidrage til sammenhæng, effektivitet og kvalitet i den samlede opgaveløsning.

Digitalisering og IT favner it-løsninger inden for både Sundhedssektoren, Specialsektoren, Regional udvikling og Administrationen, hvor størstedelen af it-indsatsen dog er koncentreret inden for Sundhedssektoren. Digitalisering og IT er organiseret i tre kontorer og en stabsfunktion, som hver ledes af en kontorchef. Herudover har IT tilknyttet en lægefaglig konsulent, der fungerer som bindeled mellem Digitalisering og IT og brugerne på regionens hospitaler. Informationssikkerhed er organiseret under en vice-kontorchef og omfatter p.t. 4 teams (SOC, GRC, Proces og ServiceDesk).

Om DIT's forvaltning og drift kan helt generelt nævnes:

- Al adgang til systemer gives kun til kendte brugere
- Der foretages logning af al adgang til Region Nordjyllands systemer
- MFA er etableret til alle systemer udefra, mens der anvendes NAC som ekstra faktor ved login fra regionens egne lokationer
- Privilegeret adgang til systemer fra eksterne lokationer foretages via et PAM system. Lokal adgang varetages hovedsageligt af en stillingsfuldmagt ud fra et arbejdsbetinget behov, som revideres halvårligt
- Alle eksterne forbindelser som minimum ssl-krypteret og autentifikation med minimum SHA-256.

KIH XDS REPOSITORY OG BEHANDLING AF PERSONOPLYSNINGER

Region Nordjylland er driftsleverandør med ansvar for drift af systemer og underliggende infrastruktur på KIH XDS Repository. Regionen udvikler ikke applikationssoftware til systemet. Softwareudvikling af applikation varetages af eksterne udviklingshuse.

KIH/XDS

KIH XDS Repository (KIH) er en del af en national infrastruktur for dokumentdeling, hvis formål er effektivt og sikkert at dele og skabe overblik over relevante data i et behandlingsforløb på tværs af sundhedsvæsenets aktører. Infrastrukturen er baseret på IHE XDS-standarden med fællesnationalt registrer, der indeholder information om, og pegepinde til kliniske data. MedCom er fællesoffentlig systemforvalter for KIH og er en del af organisationen for systemforvaltningen af fællesoffentlige sundheds-it-løsninger. Driften af KIH varetages af Region Nordjylland.

STYRING AF PERSONDATASIKKERHED

Informationssikkerhed oplever et stadig stigende fokus såvel i Region Nordjylland som i Danmark generelt. Det er der flere gode grunde til, herunder at offentlighedens interesse for databeskyttelsesforordningen

og muligheden for, at der kan udstedes store bøder til private såvel som offentlige virksomheder. Derudover fylder cybertrusler, hacking og phishing stadig mere i danskernes bevidsthed.

Informationssikkerhedsområdet er i sammenligning med de fleste andre områder i regionen et relativt ungt område, og der er således endnu ikke opbygget en stor grad af rutine og forudsigelighed i opgaveløsningen. Konkret betyder det, at der løbende sker justeringer af hvordan og i hvilke fora opgaver løses.

Organisatorisk blev det tidligere Informationssikkerhedsudvalg i 2018 erstattet af to mindre fora i form af 'Udvidet Informationssikkerhedsledelse' (UISL) og 'Informationssikkerhedsledelse'(ISL) for at styrke beslutningskraften på området. I andet halvår af 2019 blev det dog besluttet at suspendere UISL, som udover medlemmerne i informationssikkerhedsledelsen bestod af en række medlemmer, der repræsenterede forskellige funktioner i den omkringliggende organisation. Begrundelsen for nedlæggende var, at det i praksis er det mere operationelle ISL, der gennem sit daglige arbejde med området har mulighed for at træffe beslutninger med kortere varsel.

Til gengæld blev der oprettet et korps af i-sikkerhedsambassadører, som bidrager med vigtig viden om "rigets tilstand" fra regionens mange afdelinger og funktioner. De organisatoriske ændringer, der blev foretaget i 2018, blev således i store træk bibeholdt, men dog justeret ved suspendering af UISL.

I Region Nordjylland er forvaltningen af de fleste større systemer placeret i Digitalisering & IT (DIT), men der findes dog en del større og mindre systemer, hvor forvaltningen blandt andet foregår i klinikkerne. En ny-introduceret Styringsmodel for Services bidrager til at formalisere og udbrede regionens model med tre forvaltningsroller. Disse tre roller er:

- Serviceejer: Overordnet ansvarlig for servicen i hele regionen. Ansvar: Økonomi, kontrakter, Databehandleraftaler
- Serviceforvalter: Dagligt ansvarlig. Ansvar: Følge op på SLA, planlægning af udvikling, ændringsanmodninger, fejl, vejledninger, vedligeholde i-sikkerhedsmateriale.
- Driftsansvarlig: Implementere ændringer, sikre oppetid/drift i henhold til SLA, dokumenterer ændringer med mere. Bistå med i-sikkerhedsmateriale.

Med styringsmodellen vil den opgavefordeling, som har været kendt i DIT gennem en årrække, blive bredt ud til den resterende organisation. Modellen vil fremadrettet kunne bruges som dialogværktøj mellem blandt andet serviceejere/forvaltere og DIT, Informationssikkerhed, eksterne m.fl. Den ansvarsfordeling, som modellen udstikker, vil dog kunne fraviges i det omfang dette besluttes og dokumenteres blandt de relevante interessenter baseret på en konkret risikovurdering.

De tekniske og organisatoriske sikkerhedsforanstaltninger og kontroller til beskyttelse af personoplysninger er udformet i henhold til konsekvensvurderinger, og disse implementeres for at sikre fortrolighed, integritet og tilgængelighed ved regionens behandling af persondata med henblik på overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke konkrete kontrolaktiviteter er udformet:

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.
Artikel 37, stk. 1 og 5 Artikel 38 Artikel 39	Databeskyttelsesrådgiver

RISIKOVURDERING

Ledelsen er ansvarlig for, at der iværksættes initiativer, der imødegår det trusselsbillede, som Region Nordjylland til enhver tid står over for, og at der indføres passende tekniske og organisatoriske sikkerhedsforanstaltninger og kontroller, så risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, udføres der risikovurderinger af regionens systemer løbende.

Risikovurderingerne belyser sandsynligheder og konsekvenser for specifikke, udvalgte hændelser, der kan true persondatasikkerheden og dermed fysiske personers rettigheder og frihedsrettigheder, herunder tilfældige, forsætlige og uforsætlige hændelser, såsom personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Med udgangspunkt i de identificerede risici foretages der en løbende vurdering af, hvilket tekniske og organisatorisk sikkerhedsniveau der er passende, og evt. mitigerende initiativer iværksættes. I fastlæggelsen af initiativer tages hensyn til det aktuelle tekniske og organisatoriske sikkerhedsniveau samt implementeringsomkostningerne.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

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

Databehandlerens garantier

Regionen har indført politikker og procedurer, der sikrer, at regionen 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.

Regionen har etableret en organisering vedrørende persondatasikkerhed 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

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

Instruks for behandling af personoplysninger

Regionen har indført politikker og procedurer, der sikrer, at regionen handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Proceduren sikrer, at Regionen informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

Underdatabehandlere

Regionen har indført politikker og procedurer, der sikrer, at underdatabehandlere er blevet pålagt de samme databeskyttelsesforpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og regionen.

Fortrolighed og lovbestemt tavshedspligt

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

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering

Region Nordjylland har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom under "Risikovurderinger".

Beredskabsplaner

Region Nordjylland har etableret beredskabsplaner, således Region Nordjylland rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser.

Region Nordjylland har etableret et kriseberedskab, der træder i kraft i disse tilfælde. Organisering af kriseberedskabsgruppe er etableret, og der indført retningslinjer for aktivering af kriseberedskabet.
Region Nordjylland har udformet detaljerede beredskabsplaner og planer for retablering af systemer og data, der blandt andet sikrer personuafhængighed i forbindelse med aktivering af beredskabet og retableringen.
Planerne er i kopi opbevaret sikret uden for Region Nordjylland 's it-systemer. Planerne afprøves og revideres løbende i forbindelse med ændringer.

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

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

Kunder, leverandører og andre besøgende ledsages.

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

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

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

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

Fjernarbejdspladser og fjernadgang til systemer og data
Region Nordjylland har implementeret en sikret VPN-forbindelser med to-faktor autentifikation (ESA), der sikrer, at adgang fra arbejdspladser uden for Region Nordjyllands netværk og fjernadgang til systemer og data sker så sikkert som muligt.

For computere med mobile arbejdspladser er der desuden implementeret en always-on VPN-løsning, der sikrer at så snart en mobil computer udlevereret af Region Nordjylland etablerer en netværksforbindelse, føres trafikken via Region Nordjyllands interne netværk.

Regionen tilbyder også adgang til samarbejdsplatformen Office365 mv. udenfor ESA, og den kan også kun foretages via to-faktor autentifikation.

Eksterne kommunikationsforbindelser
E-mail og anden kommunikation, der indeholder følsomme personoplysninger, er krypteret i forsendelsen ved anvendelse af TLS (enforced).

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

Firewall
Region Nordjylland har indført procedurer, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter af dedikeret personale. Arbejdsstationer benytter firewall (EPP).

Netværkssikkerhed
Region Nordjylland har indført procedurer, der sikrer, at netværk i forhold til anvendelse og sikkerhed er opdelt i et antal virtuelle netværk (VLAN), hvor trafik mellem de enkelte virtuelle netværk kontrolleres af firewall.

Antivirusprogram
Region Nordjylland har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der er automatiseret opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer på end points.

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

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

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

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

Overvågning
Region Nordjylland har indført procedurer, der sikrer, at der sker løbende overvågning af systemet og indførte tekniske sikkerhedsforanstaltninger.

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

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

Databeskyttelse gennem design og standardindstillinger

Region Nordjylland udvikler ikke software i relation til KIH XDS Repository. Regionen har indført en Change Management procedure omfattende ændringer til og vedligeholdelse af infrastruktur, der anvendes til drift af KIH XDS Repository. Procedurer sikrer behørig godkendelse af ændringer til infrastrukturen gennem RFC'er. Ved udarbejdelse af RFC'er sker der en vurdering af ændringens eventuelle påvirkning af persondatabeskyttelsen.

Sletning og tilbagelevering af personoplysninger

Region Nordjylland har indført politikker og procedurer omkring sletning og tilbagelevering af personoplysninger. Sletning og/eller tilbagelevering sker som hovedregel i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Regionen efterlever nationale regler for håndtering af sundhedsdata. Databeskyttelsesforordningen giver nogle rettigheder til at få slettet personoplysninger, men i Journalføringsbekendtgørelsens § 15 anføres, at patientjournaler skal opbevares i mindst 10 år. Derudover skal patientjournaler mindst opbevares så længe journalen kan være nødvendig for en verserende klage-, tilsyns-, eller erstatningssag.

Bistand til den dataansvarlige

Region Nordjylland har indført politikker og procedurer, der sikrer, at Region Nordjylland kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder, ligesom Region Nordjylland konkret kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 34 – 36 om konsekvensanalyser.

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

Fortegnelse over kategorier af behandlingsaktiviteter

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

Underretning om brud på persondatasikkerheden

Region Nordjylland har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at Region Nordjylland er blevet opmærksom på, at der er sket brud på persondatasikkerheden.

De registrerede informationer gør den dataansvarlige i stand til at vurdere, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

Databeskyttelsesrådgiver

Region Nordjylland har indgået en aftale med Deloitte om varetagelse af rollen som databeskyttelsesrådgiver for regionen. Det nyoprettede GRC-team i Informationssikkerhedsafdelingen understøtter og koordinerer samarbejdet med databeskyttelsesrådgiveren, som refererer til den øverste ledelse i Region Nordjylland, og der er i fællesskab udarbejdet stillings- og funktionsbeskrivelse for databeskyttelsesrådgiveren, herunder beskrevet databeskyttelsesrådgiverens opgaver.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

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

- Den dataansvarlige skal sikre, at instruksen fra den dataansvarlige er lovlig i forhold til den til enhver tid gældende databeskyttelseslovgivning, og at instruksen er hensigtsmæssig i forhold til den indgåede kontrakt og databehandleraftalen.
- Den dataansvarlige har ansvaret for, at applikationen som afvikles hos databehandleren, er designet og konfigureret til at kunne efterleve databeskyttelseslovgivningen.
- Den dataansvarlig er ansvarlig for lokale brugerrettighederne i systemet, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.

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 Region Nordjyllands beskrivelse af KIH XDS Repository samt for udformningen af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

BDO's test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af Region Nordjylland, 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. december 2021.

Udførte testhandlinger

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

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

For de ydelser, som Cloudio A/S leverer inden for backup, har vi modtaget en ISAE 3402 Type 2-erklæring og databehandlerens GDPR-tilsyn om generelle it-kontroller, deres udformning, implementering og funktionalitet for Backup Services for perioden fra 1. januar til 31. december 2021.

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

Resultat af test

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

En afvigelse foreligger, når:

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

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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens ramme for Informationssikkerhed. Vi har observeret, at den er godkendt af ledelsen.	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens ramme for Informationssikkerhed og observeret, at den senest er blevet gennemgået og opdateret den 23. april 2019.	Vi konstaterer, at databehandlerens ramme for Informationssikkerhed senest er godkendt af ledelsen i april 2019. Ingen yderligere afvigelser konstateret.
Organisering af informationssikkerhed ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af Informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har etableret en cyber- og informationssikkerhedsledelse ud fra den centrale ledelse indenfor Informationssikkerhed. Vi har inspiceret, at der afholdes løbende, møder i cyber- og informationssikkerhedsledelsen. Vi har inspiceret, at databehandleren har etableret og udnævnt en række informationssikkerhedsambassadører, som er et korps af medarbejdere, der har til opgave at være cyber- og informationssikkerhedsledelsens forlænget arm i organisationen.	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 på forespørgsel fået oplyst, at der ikke eksisterer en samlet formaliseret proces for rekruttering af medarbejdere, der fastsætter krav til screening og baggrundstjek af medarbejdere, som skal have adgang til KIH. Vi har observeret, at der ikke formelt er krav om indhentning af straffeattester for medarbejdere med adgang til KIH. Vi har på forespørgsel fået oplyst, at Regionen indhenter straffeattest på it-medarbejdere ud fra et individuelt skøn af behov og relevans for medarbejderes jobfunktion.	Vi konstaterer, at der ikke forefindes en samlet formaliseret proces for og dokumentation af rekruttering af medarbejdere. Herunder som fastsætter krav til screening, baggrundstjek og kriterier for eventuel indhentelse straffeattester på de medarbejdere, som skal have adgang til KIH. Ingen yderligere afvigelser konstateret.
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Databehandleren har udarbejdet og implementeret en procedure for off-boarding af fratrådte medarbejdere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for fratrædelse. Vi har yderligere inspiceret databehandlerens procedure for brugerstyring og observeret, at der er en automatiseret arbejdsgang, som lukker adgange på fratrådte medarbejdere. Vi har inspiceret, at fratrådte medarbejderes adgange er lukket. Vi har inspiceret Regionens ansættelsesbrev og observeret, at medarbejdere er underlagt tavshedspligt under og efter ansættelse.	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. ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. ▶ Databehandleren foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og Informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens e-læringsportal for informationssikkerhedstræning. Vi har inspiceret at nye medarbejdere har gennemført Regionens e-læringsportal for informationssikkerhedstræning. Vi har inspiceret, at der løbende bliver lagt awareness materiale op på Regionens intranet. Vi har inspiceret, at databehandleren har etableret og udnævnt en række informationssikkerhedsambassadører, som er et korps af medarbejdere, der har til opgave at være cyber- og informationssikkerhedsledelsens forlænget arm i organisationen og løbende træne og sparre med Regionens personale.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren udfører løbende awareness-kampagner ▶ Databehandleren udfører oplysningskampagner for medarbejdere om databeskyttelse og Informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens e-læringsportal for informationssikkerhedstræning. Vi har inspiceret at nye medarbejdere har gennemført Regionens e-læringsportal for informationssikkerhedstræning. Vi har inspiceret, at der løbende bliver lagt awareness materiale op på Regionens intranet.	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**
	Vi har inspiceret, at databehandleren har etableret og udnævnt en række informationssikkerhedsambassadører, som er et korps af medarbejdere, der har til opgave at være cyber- og informationssikkerhedsledelsens forlænget arm i organisationen og løbende træne og sparre med Regionens personale.	

Artikel 28, stk. 3: Databehandleraftale

Kontrolmål

- *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige - Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. - Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. - Databehandleraftaler underskrives og opbevares elektronisk. - Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens politik og procedure for indgåelse af skriftlige databehandleraftaler. Vi har inspiceret databehandlerens databehandlerskabelon. Vi har observeret, at skabelonen generelt følger gældende praksis og denne senest er opdateret den 20. januar 2020. Vi har inspiceret, at indgået databehandleraftaler underskrives og opbevares elektronisk. Vi har stikprøvevis observeret, at databehandleraftalen på KIH-installationen ikke specifikt omtaler brug af backupleverandør som underdatabehandler.	Vi konstaterer, at indgået databehandleraftale ikke indeholder informationer om brug af backupleverandør som underdatabehandler. Ingen yderligere afvigelser konstateret.

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* ▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret indgået databehandleraftaler, og observeret at den indeholder 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. ▶ Databehandlerens procedurer gennemgås og opdateres løbende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der i skabelon for databehandleraftaler er beskrevet, at databehandleren alene udfører behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. Vi har inspiceret databehandlerens politik og procedure for indgåelse af skriftlige databehandleraftaler og observeret, at de begge er opdateret den 1.marts 2022. Vi har observeret, at der stilles krav om, at der minimum en gang årligt føres kontrol med, at databehandleraftalen overholdes, herunder at databehandling alene sker som anført i instruksen. Vi har på forespørgsel fået oplyst, at den udførte gennemgang ikke dokumenteres således det efterfølgende er muligt at vurdere det udførte tilsyn.	Vi konstaterer, at det udførte tilsyn med efterlevelse af instrukser fra databehandleraftalen, ikke formelt dokumenteres for KIH. Ingen yderligere afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks	Vi har udført forespørgsel hos passende personale hos databehandleren.	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**
▶ 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 inspiceret databehandlerens procedure for håndtering af ulovlige instrukser og observeret, at databehandleren straks skal underrette den dataansvarlige i tilfælde heraf. Vi har på forespørgsel fået oplyst, at der ikke er identificeret en databehandleraftale med ulovlig instruks, hvorfor vi ikke har kunne efterprøve implementeringen af kontrollen.	

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandlers indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for indgåelse af underdatabehandleraftaler. Vi har inspiceret databehandlerens databehandlerskabelon. Vi har observeret, at underdatabehandleren er underlagt samme krav, som de stillede krav til databehandleren i instruksen fra dataansvarlige. Vi har inspiceret, indgået underdatabehandleraftale med Cloudio A/S vedrørende backup. Vi har observeret, at underdatabehandleren er pålagt samme krav, som de stillede krav til databehandleren i instruksen fra dataansvarlige. Vi har observeret, at databehandleraftalen med underdatabehandlerne underskrives og opbevares elektronisk.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret proceduren for indgåelse af underdatabehandleraftaler og skabelonen for databehandleraftaler. Vi har observeret, at den dataansvarlige skal informeres om brugen af underdatabehandlere. Orienteringen skal ske senest tre måneder inden underdatabehandleren tages i brug.	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
	Vi har inspiceret dokumentation for orientering af den dataansvarlige omkring skift af backupleverandør	
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 inspiceret databehandlerens procedure for indgåelse af underdatabehandleraftaler og observeret, at der stilles krav om underretning fra de dataansvarlige ved ændring af underdatabehandlere. Vi har på forespørgsel fået oplyst, at databehandleren har skiftet underdatabehandler fra ATEAS A/S til Cloudio A/S i relation til ydelser inden for backup. Vi har inspiceret, at databehandleren har adviseret de dataansvarlige om skiftet, men dog først efter at ændringen af underdatabehandleren er trådt i kraft.	Vi konstaterer, at databehandleren har adviseret de dataansvarlige ved ændringen af underdatabehandleren. Dette er dog først sket efter at aftalen er trådt i kraft. Ingen yderligere afvigelser konstateret.
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet, hvem der er kontaktperson, lokation for behandling, samt hvilken type af behandling og kategori af personoplysninger, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren ikke har en oversigt over godkendte underdatabehandlere i relation til KIH.	Vi konstaterer, at der ikke foreligger en formel oversigt over godkendte underdatabehandlere i relation til KIH. Ingen yderligere 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 indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering. ▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året, baseret på en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for tilsyn med underdatabehandlere. Databehandleren benytter et tilsynssystem, udviklet af konsulenthuset Bech Bruun. Vi har inspiceret spørgerammen for tilsyn med underdatabehandlere. Vi har inspiceret, at der er ført GDPR tilsyn med Cloudio A/S. Vi har yderligere inspiceret modtaget ISAE 3402 erklæring fra Cloudio A/S. for perioden 1 januar til 31 december 2021.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt		
Kontrolmål ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Lovbestemt tavshedspligt ▶ Alle medarbejdere er underlagt lovbestemt tavshedspligt efter straffelovens bestemmelser.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens ansættelsesbrev, hvor det fremgår, at alle medarbejdere er underlagt tavshedspligt og er underlagt tavshedspligt gennem forvaltningsloven.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens ansættelsesbrev, hvor det fremgår, at alle medarbejdere er underlagt tavshedspligt og er underlagt tavshedspligt gennem forvaltningsloven. Tavshedspligten gælder også efter endt ansættelse. Vi er på forespørgsel fået oplyst, at alle ansatte hos databehandleren er underlagt forvaltningsloven krav om fortrolighed i sundhedssektoren. Vi har stikprøvevist inspiceret, at eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▸ Der foretages løbende og som minimum en gang årligt en risikovurdering af systemerne baseret på 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. ▸ Risikovurderingerne opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens politik og retningslinjer for risikostyring og observeret, at der foreligger en formel procedure for udarbejdelse af risikovurderinger, hvor risici taget udgangspunkt i identificerede trusler og risici minimeres ud fra sandsynlighed og konsekvens for Regionen til et accepteret niveau. Vi har inspiceret, at risikovurderingerne skal opdateres efter behov. Vi har på forespørgsel fået oplyst, at risikovurderingen for KIH-installationen ikke har været opdateret inden for det seneste år.	Vi konstaterer, at risikovurderingen for KIH ikke har været opdateret inden for det seneste år. Ingen yderligere afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▸ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▸ Databehandleren har etableret årlig afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer. ▸ Beredskabstest dokumenteres og evalueres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens beredskabsplan. Vi har inspiceret, at der i beredskabsplanen er taget stilling til flere forskellige trusselsscenarier, herunder både fysiske og tekniske hændelser.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at beredskabsplanen er tilgængelig både fysisk og online. Vi har inspiceret, at databehandleren har foretaget beredskabstest i januar 2021 og efterfølgende evalueret denne.	
Opbevaring af personoplysninger - Personoplysninger opbevares utilgængeligt for andre. - Fysiske materialer indeholdende personoplysninger opbevares aflåst.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for persondata i fysisk form. Vi har inspiceret, at databehandlerens datacenter er certificeret som Tier IV datacenter, herunder at der ikke er adgang til datacenteret uden et arbejdsbetinget behov. Vi har inspiceret seneste offentliggjorte ISAE 3402 erklæring for 2021 fra Cloudio A/S og observeret, at der ikke er konstateret afvigelser i relationer til opbevaring af backup.	Ingen afvigelser konstateret.
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.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
▸ Alle adgange registreres og logges. ▸ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter.	Vi har observeret, at døren til databehandlerens it-kontor er aflåst, og at der alene gives adgang til databehandlerens it-medarbejdere med behov for at have adgang til lokalerne. Vi har observeret, at gæster bliver ledsaget ved besøg. Vi har observeret, at alle personer ved adgang til maskinstuer registreres. Vi har inspiceret dokumentation for registrering ved adgang til maskinstuer. Vi har inspiceret liste over personer med adgang til maskinstuer, og det er oplyst, at disse alle har et arbejdsbetinget behov for adgang. Vi har inspiceret, at der er foretaget gennemgang af personer med adgang til serverrummet. Vi har inspiceret, at databehandlerens datacenter er certificeret som Tier IV datacenter.	
Fysisk sikkerhed ▸ Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. Den fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav. ▸ Databehandleren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum omfattende følgende forhold: - Bygning	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandlerens datacenter er Tier IV certificeret og således er bevis på høj forsyningssikkerhed, herunder at det lever op til alle krav om fysisk sikkerhed.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
- Gulve - Klima - Strøm - Adgang - Alarmmonitorering - Brandslukning - Kabling	Vi har observeret, at databehandleren har etableret sikringsforanstaltninger til beskyttelse mod eksterne og miljømæssige trusler, herunder: • Særlig indrettede it-lokaler • Hævede gulve med alarmer for opstigning af vand • Klimaregulering i form af køling i rackskabe • Strømregulering gennem UPS med tilkoblet nødstrømsgenerator • Fysisk adgangskontrol med overvågning • Alarmmonitorering i driftscenter • Brandbekæmpelses anlæg • Organiseret og afmærket kabling Vi har yderligere inspiceret 3402 erklæring fra Cloudio A/S og observeret, at der ikke har angivet nogle anmærkninger vedrørende den fysiske sikkerhed i relation til opbevaring af backup.	
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for tildeling, ændring og nedlukning af brugere og observeret, at brugerrettigheder tildeles ud fra et arbejdsbetinget behov.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
▸ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. ▸ Der foretages halvårlig gennemgang af brugere og brugerrettigheder. ▸ Der foretages logning af alle adgange til systemer og data. ▸ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere.	Vi har inspiceret, at brugeroprettelser tildeles efter et arbejdsbetinget behov gennem Regionens IDM-system, som sikrer at alle brugeroprettelser og ændringer er ledelsesgodkendt. Vi har inspiceret, at fratrådte brugeres rettigheder fjernes i relevante systemer gennem Regionens IDM-system. Vi har inspiceret procedure for privilegerede (administrative) adgangsrettigheder. Vi har inspiceret tildelte privilegerede rettigheder til KIH-installationen. Vi har på forespørgsel fået oplyst, at der ikke indenfor det seneste år har været tildeling af privilegerede (administrative) adgangsrettigheder. Vi har inspiceret to udtræk fra logpoint og observeret, at databehandleren logger adgangsforsøg til KIH. Vi har inspiceret, at der er udført halvårlig periodisk gennemgang af brugere og deres tilhørende rettigheder, som senest er udført i efteråret 2021. Vi har inspiceret et udtræk af databehandlerens passwordpolitik for almindelige- og privilegerede adgange.	
Fjernarbejdspladser og fjernadgang til systemer og data ▸ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse (SHA-2 & 256 bit)	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret databehandlerens VPN-forbindelse og observeret, at den er konfigureret med TLS-kryptering, og at der er krav om to-faktor autentifikation. Vi har inspiceret databehandlerens VPN-forbindelse og observeret, at Regionen anvender Any Connect.	
Eksterne kommunikationsforbindelser - Udveksling af personoplysninger via e-mail, sker vha. SikkerMail løsning eller sikker deling. - Eksterne kommunikationsforbindelser er krypteret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren benytter en TLS-kryptering til sikring af e-mails. VI har inspiceret, at databehandleren benytter Sharefiles med to-faktor autentifikation til deling af materiale med eksterne.	Ingen afvigelser konstateret.
Kryptering af personoplysninger - Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail. - Der er implementeret procedurer, der sikrer, at data på personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, er krypteret ved ibrugtagning, så adgang til data alene er mulig for autoriserede brugere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren benytter en TLS-kryptering til sikring af e-mails, således personoplysninger er krypteret under "transport". Vi har inspiceret, at databehandleren benytter sig af BitLocker, som krypterer indhold på databehandlerens arbejdsstationer.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Firewall ▸ Databehandler har konfigureret firewall korrekt efter best-practice standard. ▸ Databehandler anvender kun services/porte som de har behov for. ▸ Firewalls er konfigureret og valideret periodisk efter behov, så service/porte kun er åbne efter behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret koncept for opsætning af firewall og observeret, at konfigurationsprincippet er, at kun godkendt og relevant trafik tillades. Vi har på forespørgsel fået oplyst, at konfiguration af firewall løbende revurderes som en del af den daglige vedligeholdelse af netværksinfrastruktur. Vi har inspiceret, at der er implementeret standardprocedure for ændringer i firewall. Vi har inspiceret, at der er opsat firewall servere.	Ingen afvigelser konstateret.
Netværkssikkerhed ▸ Netværks topologien er struktureret efter best-practice principper, hvilket betyder at servere, som driver applikationer, ikke kan nås direkte fra internettet. ▸ Databehandlers netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet. ▸ Databehandleren anvender kendte netværksteknologier og mekanismer (Firewall/Intrusion DetectionSystem/Intrusion Prevention System) for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation og netværkstopologi og observeret, at der er etableret segmentering af systemer gennem anvendelse af firewalls. Vi har inspiceret dokumentation og netværkstopologi for og observeret, at applikationsservere er placeret internt hos databe-	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	handleren, og at disse kommunikerer med enheder i DMZ-zonen, som igen kommunikerer med Sundhedsnettet (SDN), før end trafikken rammer en slut bruger. Vi har observeret, at trafikken på alle lag sker gennem firewall som alene er konfigureret til at tillade godkendt trafik. Vi har inspiceret, at databehandler anvender flere forskellige IDS/IPS-teknologier til overvågning og spærring for uautoriseret trafik på netværket.	
Antivirusprogram ▸ Der er installeret antivirussoftware på alle servere og arbejdsstationer. ▸ Antivirus-software opdateres løbende med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har opsat McAfee, agent-server til overvågning af virus på databehandlerens servere og end-points. Vi har inspiceret, at antivirussoftware er konfigureret og at software og signaturfiler løbende opdateringer.	Ingen afvigelser konstateret.
Sårbarhedsscanning ▸ Der bliver løbende foretaget sårbarhedsscanning af databehandlerens netværk. Resultatet dokumenteres i en rapport. ▸ Databehandleren gennemgår rapporten og følger op på konstateret svagheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren løbende foretager sårbarhedsscanninger. Det er på forespørgsel oplyst, at identificerede	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
▸ Databehandler håndtere/mitigere eventuelle sårbarheder ud fra en risikovurdering. ▸ Databehandler har dokumenteret deres håndtering/mitigering af fundne sårbarheder.	sårbarheder risikovurderes og håndteres ud fra CVS score samt i forhold til en konkret risikovurdering hos Regionen. VI har inspiceret, hvordan databehandleren håndterer og dokumentere sårbarheder.	
Sikkerhedskopiering og retablering af data • Der foretages dagligt backup af systemer og data. • Drift og opbevaring af backup er outsourcet til underdatabehandler. • Der udføres restore-tests.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har aftale med Cloudio A/S, som foretager daglig backup af systemer og data. Vi har observeret, at Cloudio A/S er registreret som underdatabehandler, og at der foreligger en underdatabehandleraftale med selskabet. Vi har inspiceret seneste offentliggjorte ISAE 3402-erklæring for 2021 fra Cloudio A/S og observeret, at der ikke er konstateret afvigelser i relation til backup og restore-tests.	Ingen afvigelser konstateret.
Vedligeholdelse af systemsoftware ▸ Databehandler fører en oversigt over systemsoftware/tredjepartsprogrammer, som vedligeholdes og opdateres løbende. ▸ Operativsystemsoftware på servere og arbejdsstationer opdateres løbende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har indført procedure, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har stikprøvevist inspiceret, at systemsoftware er opdateret på servere.	
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger - Alle succesfulde og mislykkede adgangsforsøg til systemet logges. - Alle brugerændringer i system og database logges. - Loggen slettes efter den fastsatte retentionsperiode. - Databehandler monitorerer og logger netværkstrafik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren benytter systemet logpoint til overvågning, som er konfigureret ud fra ledelsens ønske til niveau af logning. Vi har inspiceret to udtræk fra logpoint og observeret, at databehandleren logger brugertrafik i KIH. Vi har inspiceret opsætning af retentionsperioder i logpoint og observeret, at disse efterlever praksis i databeskyttelsesforordningen. Vi har inspiceret, at databehandler anvender Stealthwatch til overvågning af netværkstrafik.	Ingen afvigelser konstateret.
Overvågning - Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. - Databehandleren notificeres om identificeret alarmer og følger op herpå.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren har etableret et overvågningssystem af relevante systemer gennem Scrum.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har observeret, at databehandleren notificeres om identificerede alarmer og følger op herpå i driftscenter.	
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 foretager sikker sletning af data på databærende medier (overskrivning/forvanskning, kryptering). ▸ Databehandleren fører en oversigt af destrueret it-udstyr. ▸ Databehandler følger anbefalet praksis fra Datatilsynet omkring sletning af databærende medier.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedurer for reparation, service og bortskaffelse af it-udstyr. Vi har stikprøvevis inspiceret sletningsrapport, hvor leverandørens sletningsalgoritme fremgår, som anbefales af datatilsynet. Vi har inspiceret, at databehandleren får en oversigt over destrueret it-udstyr som kvittering.	Ingen afvigelser konstateret.
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▸ Databehandler afprøver, vurdere og evaluerer effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens ramme for informationssikkerhed og observeret, at det er informationssikkerhedsledelsen, som har ansvaret for, at informationssikkerhedstiltag har den forventede effekt og løbende igangsætter nye tiltag.	Vi konstaterer, at databehandleren ikke har formaliseret dokumentation på regelmæssig egen kontrol og efterprøvelser af effektiviteten af de etablerede tekniske og organisatoriske sikkerhedsforanstaltninger som databehandler. Ingen yderligere afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Det er via forespørgsel oplyst, at databehandleren ikke har formaliseret dokumentation på regelmæssig egen kontrol og efterprøvelser af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger.	

Artikel 25, Databeskyttelse gennem design og standardindstillinger		
Kontrolmål ▶ *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Databeskyttelse ved ændringer og vedligeholdelse ▶ Databehandler har Change Management procedurer, som sikre databeskyttelse gennem design og standardindstillinger ved ændringer og vedligeholdelse af infrastrukturen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedurer for Change Management på infrastruktur. Vi har inspiceret dokumentation for, at proceduren for Change Management er fulgt.	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 inspiceret, at databehandleren har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige, dog således national lovgivning overholdelse. Vi har på forespørgsel fået oplyst, at der ikke har været ophørte aftaler inden for det seneste år, og proceduren har derfor ikke været mulig at efterprøve.	Ingen afvigelser konstateret.
Tilbagelevering af personoplysninger ▶ Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen. ▶ Dataansvarlig og databehandler har aftalt i hvilket format, overførelse og medie data skal tilbageleveres når det anmodes af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige, dog således national lovgivning overholdelse. Vi har på forespørgsel fået oplyst, at der ikke har været ophørte aftaler inden for det seneste år, og proceduren har derfor ikke været mulig at efterprøve.	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 ▶ Databehandler har udarbejdet en procedure for bistand til dataansvarlige ved opfyldelse af 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 den indgåede databehandleraftale indeholder krav om bistand til de dataansvarlig i forhold til de registreredes rettigheder. Vi har på forespørgsel fået oplyst, at databehandleren ikke har udarbejdet en procedure for bistand. Det er oplyst, at databehandleren anvender samme retningslinjer ved bistand til den dataansvarlige, som er fastsat i relation til databehandlerens rolle som dataansvarlig. Vi har på forespørgsel fået oplyst, at databehandleren ikke har fået henvendelser fra dataansvarlige på nogen af de relevante systemer i forhold til at yde bistand i forhold til den registreredes rettigheder.	Vi konstaterer, at databehandleren ikke har udarbejdet en formel procedure for databehandlerens bistand til den dataansvarlige ved opfyldelse af de registreredes rettigheder. Ingen yderligere 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 på forespørgsel fået oplyst, at databehandleren ikke har udarbejdet en procedure for bistand efter artikel 32 til 36 som databehandler. Det er oplyst, at databehandleren anvender samme retningslinjer ved bistand til den dataansvarlige, som er fastsat i relation til databehandlerens rolle som dataansvarlig. Vi har på forespørgsel fået oplyst, at databehandleren ikke har fået henvendelser fra dataansvarlige på efterlevelse af krav i artikel 32 til 36 på nogen af de relevante systemer.	Vi konstaterer, at databehandleren ikke har udarbejdet en formel procedure for databehandlerens bistand til den dataansvarlige ved opfyldelse af krav i artikel 32 til 36. Ingen yderligere 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. ▶ Databehandleren stiller den nødvendige 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. I henhold til nærværende erklæring vil databehandleren leve op til sin forpligtelse i forhold til udarbejdelsen af en ISAE 3000-erklæring, lige som at databehandleren vil besvare henvendelser fra de dataansvarlige i nødvendigt omfang.	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 inspiceret databehandleren fortegnelse over kategorier af behandlingsaktiviteter og observeret at den er opdateret løbende inden for det seneste år.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandlerens fortegnelse over kategorier af behandlingsaktiviteter opbevares elektronisk.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren vil udlevere fortegnelsen på anmodning fra Datatilsynet. Der har ikke været nogen anmodning herom, hvorfor kontrollen ikke har kunnet efterprøves.	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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret indgået databehandleraftaler og observeret, at databehandleren skal underrette dataansvarlige uden unødig forsinkelse ved brud på persondatasikkerheden. Vi har på forespørgsel fået oplyst, at der sker underretning af den dataansvarlige uden unødig forsinkelse ved brud på persondatasikkerheden. Vi har inspiceret databrudsloggen og observeret, at der ikke har være brud på persondatasikkerheden i relation KIH. Det har derfor ikke været muligt at efterprøve, om dataansvarlige underrettes rettidigt.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har opsat overvågning af system til detektion af 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 inspiceret procedure for persondatabrud på Regionens intranet. Vi har på forespørgsel fået fremvist databehandlerens funktionalitet til indberetning af brud på persondatasikkerheden på databehandlerens intranet. Vi har inspiceret databehandlerens dokument "Vurdering af brud på persondatasikkerheden" og observeret, at der tages stilling til en række relevante forhold i vurdering og indikationen af brud på persondatasikkerheden.	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 inspiceret databehandlerens databrudslog og observeret, at databrud generelt logges og bruges til intern statistik. Vi har inspiceret databrudsloggen og observeret, at der ikke har være databrud i relation til KIH.	Ingen afvigelser konstateret.

Artikel 37, stk. 1 og 5, artikel 38 og artikel 39: Databeskyttelsesrådgiver

Kontrolmål

- *At sikre, at databeskyttelsesrådgiveren er udpeget på grundlag af sine faglige kvalifikationer.*
- *At sikre, at databehandleren inddrager databeskyttelsesrådgiveren tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.*
- *At sikre, at databeskyttelsesrådgiveren har de nødvendige ressourcer til at udføre opgaverne og opretholde ekspertisen.*
- *At sikre, at databeskyttelsesrådgiveren ikke modtager instrukser vedrørende udførelse af sine opgaver.*
- *At sikre, at databeskyttelsesrådgiveren rapporterer direkte til det øverste ledelsesniveau hos databehandleren.*
- *At sikre, at databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af opgaverne.*
- *At sikre, at databeskyttelsesrådgiveren ikke har andre opgaver og pligter, som medfører interessekonflikt.*
- *At sikre, at databehandleren har udarbejdet en opgavebeskrivelse vedrørende databeskyttelsesrådgiverens opgaver.*
- *At sikre, at databeskyttelsesrådgiveren udfører sine opgaver i henhold til opgavebeskrivelsen.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Udpegelse af databeskyttelsesrådgiveren ▸ Databehandleren har udpeget en databeskyttelsesrådgiver. ▸ Databehandleren har udarbejdet og implementeret en procedure for udpegelse af databeskyttelsesrådgiver.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens politik for udpegelse af databeskyttelsesrådgiver. Vi har på forespørgsel fået oplyst, at databehandleren har valgt en ekstern databeskyttelsesrådgiver.	Ingen afvigelser konstateret.
Databeskyttelsesrådgiverens stilling ▸ Databehandleren har udarbejdet og implementeret en beskrivelse af databeskyttelsesrådgiverens stilling. ▸ Databehandleren inddrager databeskyttelsesrådgiveren vedrørende beskyttelse af personoplysninger. ▸ Databeskyttelsesrådgiveren rapporterer direkte til databehandlerens ledelse. ▸ Databeskyttelsesrådgiveren er underlagt tavshedspligt/fortrolighed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databeskyttelsesrådgiverens stilling, forpligtelser og rettigheder er fastsat i aftalen med den eksterne databeskyttelsesrådgiver, og at det er sket efter retningslinjerne i databeskyttelseslovgivningen og databehandlerens politik for DPO-rollen.	Ingen afvigelser konstateret.
Databeskyttelsesrådgiverens opgaver ▸ Databehandleren har udarbejdet og implementeret en opgavebeskrivelse af databeskyttelsesrådgiverens opgaver.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Artikel 37, stk. 1 og 5, artikel 38 og artikel 39: Databeskyttelsesrådgiver		
Kontrolmål ▶ *At sikre, at databeskyttelsesrådgiveren er udpeget på grundlag af sine faglige kvalifikationer.* ▶ *At sikre, at databehandleren inddrager databeskyttelsesrådgiveren tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.* ▶ *At sikre, at databeskyttelsesrådgiveren har de nødvendige ressourcer til at udføre opgaverne og opretholde ekspertisen.* ▶ *At sikre, at databeskyttelsesrådgiveren ikke modtager instrukser vedrørende udførelse af sine opgaver.* ▶ *At sikre, at databeskyttelsesrådgiveren rapporterer direkte til det øverste ledelsesniveau hos databehandleren.* ▶ *At sikre, at databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af opgaverne.* ▶ *At sikre, at databeskyttelsesrådgiveren ikke har andre opgaver og pligter, som medfører interessekonflikt.* ▶ *At sikre, at databehandleren har udarbejdet en opgavebeskrivelse vedrørende databeskyttelsesrådgiverens opgaver.* ▶ *At sikre, at databeskyttelsesrådgiveren udfører sine opgaver i henhold til opgavebeskrivelsen.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Databeskyttelsesrådgiveren udfører ikke andre opgaver, der er i konflikt med opgaverne som databeskyttelsesrådgiver hos databehandleren.	Vi har inspiceret, at databeskyttelsesrådgiverens stilling, forpligtelser og rettigheder er fastsat i aftalen med den eksterne databeskyttelsesrådgiver, og at det er sket efter retningslinjerne i databeskyttelseslovgivningen og databehandlerens politik for DPO-rollen.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

PENNEO

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."

Grethe Kiehn Kristensen
Vicekontorchef
Serienummer: PID:9208-2002-2-624795801816
IP: 95.166.xxx.xxx
2022-04-10 13:55:06 UTC
NEM ID

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2022-04-10 13:57:27 UTC
NEM ID

Mikkel Jon Larssen
Partner
Serienummer: CVR:20222670-RID:52744874
IP: 77.243.xxx.xxx
2022-04-11 05:43:40 UTC
NEM ID