KIAP

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF IT LØSNINGER TIL ALMEN PRAKSIS OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING 2

2. KIAP'S UDTALELSE 5

3. KIAP'S BESKRIVELSE AF IT LØSNINGER TIL ALMEN PRAKSIS 7

Indledning 7

KiAP's kontrolmål, herunder regler og procedurer samt gennemførte kontroller 7

Principper vedrørende behandling af personoplysninger 7

Risikostyring i KiAP 8

Organisation og ansvar 8

GDPR og KiAP's rolle og ansvar som processor 9

Ændringer i perioden 1. januar til 31. december 2023 11

Komplementerende kontroller hos de dataansvarlige 11

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST 13

Kontrolområde A 15

Kontrolområde B 18

Kontrolområde C 28

Kontrolområde D 33

Kontrolområde E 34

Kontrolområde F 35

Kontrolområde H 37

Kontrolområde I 38

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF IT LØSNINGER TIL ALMEN PRAKSIS OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i KiAP
KiAPs kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af KiAP (databehandleren) for hele perioden fra 1. januar til 31. december 2023 udarbejdede beskrivelse i sektion 3 af IT løsninger til almen praksis 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 og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

BDO Statsautoriseret revisionsaktieselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen og den operationelle effektivitet 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 og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. 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 eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. 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.

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 IT løsninger til almen praksis, 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. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af IT løsninger til almen praksis og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret i hele perioden fra 1. januar til 31. december 2023, 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 i hele perioden fra 1. januar til 31. december 2023, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar til 31. december 2023.

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 IT-løsninger til almen praksis, 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 2. februar 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, statsautoriseret revisor

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

2. KIAP'S UDTALELSE

KiAP varetager behandling af personoplysninger i forbindelse med IT-løsninger til almen praksis 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 IT løsninger til almen praksis, 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.

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

KiAP bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af IT-løsninger til almen praksis og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden fra 1. januar til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for IT løsninger til almen praksis, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger 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 IT-løsninger til almen praksis 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. Indeholder relevante oplysninger om ændringer i IT-løsninger til almen praksis og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden fra 1. januar til 31. december 2023.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af IT-løsninger til almen praksis 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 IT-løsninger til almen praksis, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

KiAP 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 og fungerede effektivt i hele perioden fra 1. januar til 31. december 2023. 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.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden fra 1. januar til 31. december 2023.

KiAP bekræfter, at der er implementeret og opretholdt 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.

Odense, den 2. februar 2024

KiAP

Jan Kristensen
IT-drifts- og udviklingschef

3. KIAP'S BESKRIVELSE AF IT LØSNINGER TIL ALMEN PRAKSIS

INDLEDNING

Formålet med denne beskrivelse er at levere oplysninger til KiAP's kunder og deres interessenter (herunder revisorer) om kravene og indholdet af EU' s Generelle Databeskyttelsesforordning ("GDPR").

Desuden er formålet med denne beskrivelse at give specifikke oplysninger om spørgsmål vedrørende sikkerheden ved behandling, tekniske og organisatoriske foranstaltninger, ansvar mellem dataansvarlige (lægeklinikker) og KiAP, og hvordan de tilbudte tjenester kan hjælpe med at understøtte de registreredes rettigheder.

KiAP anser et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, og som et kvalitetselement for at kunne tilbyde en sikker service overfor sundhedsfaglige brugere, patienter og samarbejdspartnere. Informationssikkerhed er en nøgleværdi for KiAP, og en naturlig del af vores aktiviteter. Ledelsen foretager løbende overvågning af informationssikkerhed og risikobilledet for virksomheden, og kontrolbeskrivelsen evalueres som minimum årligt.

Følgende løsninger er omfattet af kontrolbeskrivelsen:

- Forløbsplaner (sundhedsfaglig login) og Sundhedsmappe (patient-login af Forløbsplaner)
- KiAP.dk /klynger (sundhedsfagligt login, herunder klyngevisninger)

Løsninger, der ikke indeholder personfølsomme data eller andre sundhedsfaglige eller på anden vis følsomme data, er ikke omfattet af nærværende beskrivelse.

KIAP'S KONTROLMÅL, HERUNDER REGLER OG PROCEDURER SAMT GENNEMFØRTE KONTROLLER

KiAP har defineret kvalitetsstyringssystemet ud fra vores overordnede målsætning om at være en troværdig og kompetent samarbejdspartner i sundhedsvæsenet. Vores digitale værktøjer og datahåndtering skal være meningsfulde og brugbare i lægernes kliniske arbejde. For at kunne gøre det, er det nødvendigt, at vi har aktive politikker og procedurer, der sikrer ensartet og gennemsigtige leverancer.
Vores IT-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle produkter og leverancer.

PRINCIPPER VEDRØRENDE BEHANDLING AF PERSONOPLYSNINGER

Hvis du har indgået kontrakt med en tredjepart, skal du skitsere aftalen herom, samtidig med at du overvejer risici (lov og overholdelse) og tilføjer disse i følgende afsnit "Risikostyring".

KiAP's sikkerhedspolitik er baseret på at gældende lovgivningsmæssige krav, herunder bl.a. persondataforordning og GDPR overholdes.

KiAP har yderligere defineret nogle principper for god og sikker brugeradfærd i IT-sikkerhedspolitikken, som medarbejderne skal overholde. Det er bl.a. et princip, at alle persondata behandles fortroligt i alle tilfælde. Politikken indeholder også retningslinjer for passwords, brugerroller samt god og sikker adfærd på nettet. Det er også et princip, at adgang til kritiske data eller infrastrukturkomponenter, servere mm. Alene gives på baggrund af, at der findes en arbejdsbetinget opgave, der skal løses.

KiAP har udarbejdet en række forskellige kontroller, som udføres med regelmæssighed fordelt ud over året. Disse kontroller er styret af et årshjul. Alle kontroller har en udførende ansvarshavende. Resultatet af hver kontrol skal logges. Hvis kontrollen ikke er udført som planlagt, skal begrundelsen herfor logges. KiAP overvejer løbende, om nye kontroller skal tilføjes.
Kontrollerne er rettet mod konkrete arbejdshandlinger/processer. Der kan være yderligere kontroller defineret. Konkrete arbejdshandlinger er og bliver beskrevet i Standard Operating Procedure (SOP) dokumenter.

RISIKOSTYRING I KIAP

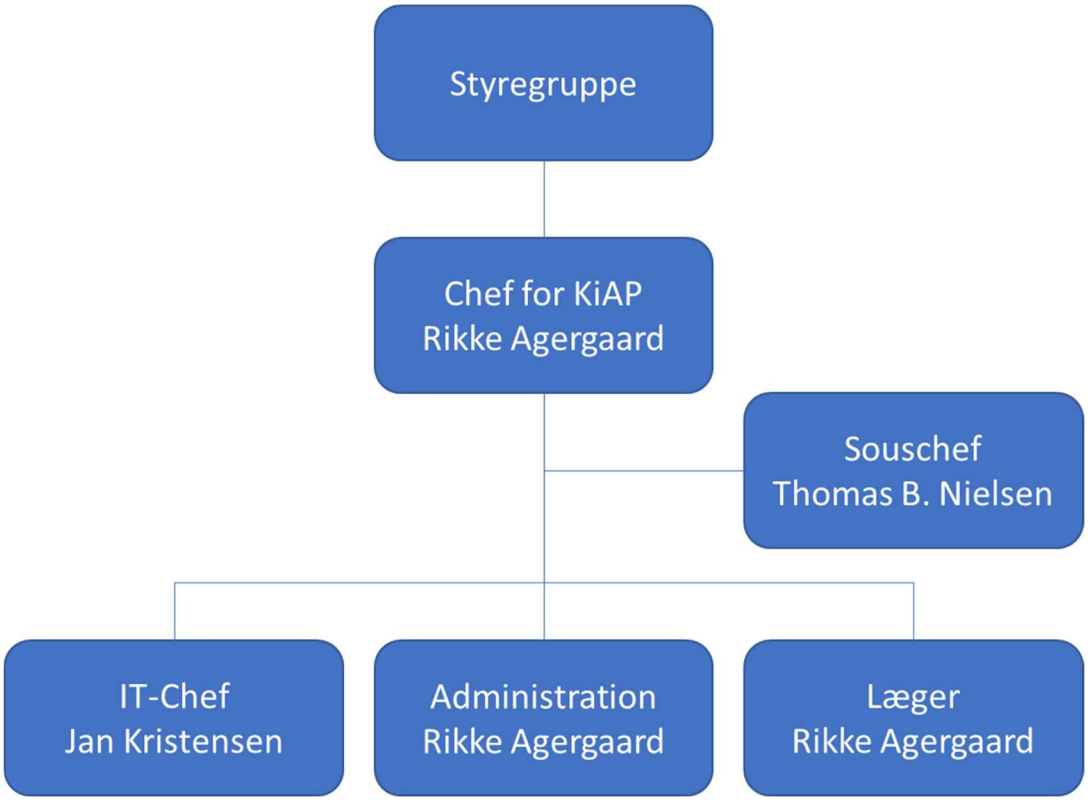
Alle vores trusler vurderes systematisk og ensartet med afsæt i en fastlagt klassifikationsmetode for at sikre transparens, overskuelighed og fælles forståelse. Identifikation, analyse og vurdering af ricisi med betydning for KiAP's forretning kan tage afsæt i både udefra kommende trusler og interne forhold.

Risikovurderingen er en fast del af alle arbejds- og udviklingsprocesser. Både til sikring af vores produkt-kvalitet, forventningsafstemning med lægefaglige kunder samt integriteten af vores forretningsplatform. Risikovurderingen foretages både periodisk og på øverste ledelsesniveau minimum en gang årligt eller hvis der opstår særligt kritiske forhold, som ledelsen skal kende/tage stilling til. Risikovurderingen foretages også på daglig basis, når der indgår kundeønsker, foretages ændringer eller nye systemer implementeres. Risici beregnes som produkter af sandsynlighed og konsekvens, der vurderes på en skala fra 1-5, hvor 1 er mindst alvorligt og 5 er mest alvorligt.

Risici identificeres både ved konference med lægefaglige specialister, teknisk personale, forretningsmæs-sige og organisatoriske forhold med afsæt i patientens risiko.

ORGANISATION OG ANSVAR

KiAP's organisation ser pr. oktober 2022 således ud:



Bemærk: Organiseringen af KiAP's Styregruppe gældende fra 1/1-2022.

KiAP's øverste ledelse Rikke Agergaard er chef for KiAP. Virksomheden er fordelt over to lokationer i hhv. København og Odense. KiAP's praksis-læger er organisatorisk placeret under Rikke, som står for det læge-faglige kvalitetsarbejde og inddrages IT-udviklingsprocesserne efter behov. Administrationen dækker de projektopgaver, som udføres i forbindelse med kvalitetsarbejdet. Al it-udvikling, it-drift og support sker i Odense-afdelingen, som organisatorisk er placeret under Jan Kristensen. Ansvaret for alle processer og kontroller i forbindelse med it-aktiviteterne er placeret her.

GDPR OG KIAP'S ROLLE OG ANSVAR SOM PROCESSOR

KiAP udvikler software og driver en række it-løsninger, som anvendes af praktiserende læger til forskellige sundhedsfaglige og administrative opgaver:

- **Forløbsplaner og Sundhedsmappe** (hhv. læge- og patientdelen af samme system) indeholder sundhedsfaglige data på patienter[1]. KiAP har ansvar for, at data opbevares sikkert efter gældende lovgivning og, at data kun tilgås af autoriserede personer med et gyldigt formål.
- **Klyngevisning**. Aggregeret sundhedsfaglige pr. læge/klinik data baseret på patientoplysninger. KiAP udvikler statistikker på baggrund af patientdata. KiAP har ansvar for, at data kun tilgås af autoriserede personer med et gyldigt formål.
- **Akkreditering**: Drift af løsningen er ophørt pr. april 2022. Faglig vurdering af læge ift. at lægen kan opretholde sin bestalling. KiAP har ansvar for, at data modtages og behandles korrekt og sikkert. Data videregives kun til godkendte modtagere.
- **DanPep**. Løsningen er lukket pr. 4. juli 2022, og driften er ophørt pr. 13. september 2022. Patienter logger ind og evaluerer deres behandlingsforløb hos en læge. Der gemmes ikke sundhedsfaglige data i Danpep. KiAP har ansvar for, at data modtages og behandles korrekt og sikkert. Data kan kun tilgås af godkendte modtagere.

SAMTYKKE

Patientdata i Sundhedsmappe kræver, at der er afgivet samtykke, før data overføres fra det lægefaglige journalsystem. Løsningen er teknisk bygget op således, at data ikke overføres til Sundhedsmappe, medmindre der er positivt markeret i samtykke-feltet. Hvis samtykke senere tilbagekaldes, så standser synkroniseringen af data. Der udføres en sletning af patientens data på sundhedsmappen, hvis der modtages instruks herom fra den dataansvarlige læge.

KiAP har procedurer for bl.a. håndtering af risikostyring, persondatahenvendelser, adgangsstyring og udvikling, kunders instrukser og tilsyn med underdatabehandlere.

Kontrollerne omfatter bl.a. adgang til data, hændelsesstyring, kunders instrukser, persondatahenvendelser, Anskaffelse og udviklings, fortegnelse mv. Et samlet overblik over alle kontroller kan ses i Årshjulet for sikkerhedskontroller.

BEHANDLING AF FORSKELLIGE KATEGORIER AF PERSONOPLYSNINGER

Data og systemer i KiAP klassificeres i forhold til tilgængelighed, informationssikkerhed og fortrolighed:

Tilgængelighed af data og systemer prioriteres indbyrdes i følgende kategorier:
A. **Høj:** Forretningskritisk og kan ikke erstattes af manuelle procedurer
B. **Medium:** Vigtigt, men funktionerne kan udføres manuelt i en begrænset tidsperiode
C. **Lav:** Ikke kritisk og funktionerne kan afbrydes i en længere tidsperiode

Informationssikkerhed af data klassificeres efter følgende kategorier:
1. **Høj:** Forretningskritiske beslutninger bliver taget på grundlag af data
2. **Medium:** Data danner grundlag for beslutninger, men de er ikke kritiske
3. **Lav:** Data danner aldrig, eller kun sjældent, grundlag for beslutninger

Fortrolighed af data klassificeres efter følgende kategorier:
i. **Fortroligt:** Data der kun må være tilgængeligt for en begrænset gruppe af personer
ii. **Internt brug:** Materiale der er tilgængeligt for alle internt i organisationen
iii. **Frit tilgængelig:** Der er ingen fortrolighed og ingen begrænsninger for hvem, der må få adgang til data

DEN REGISTREREDES RETTIGHEDER

KiAP er underlagt de forpligtigelser, som er beskrevet i de gældende databehandleraftaler samt gældende lovgivning. Herunder bl.a. personers rettigheder i forbindelse med henvendelse til KiAP. Der er udarbejdet

[1] KiAP har alene patientdata på egne servere. Lægens data ligger ikke på KiAP's servere.

procedurer for, hvordan sådanne henvendelser modtages, behandles og håndteres med henblik på korrekt behandling samt overholdelse af tidsfrister.

GENERELLE FORPLIGTELSER SOM PROCESSOR

KiAP har udarbejdet procedurer, som skal sikre, at der ikke indgås databehandleraftaler (eller andre kontrakter), der medfører risiko for brud på gældende lovgivning ved efterlevelse.

KiAP har også udarbejdet procedurer for brug af underdatabehandlere, herunder også retningslinjer for hvorledes der føres tilsyn.

DATABESKYTTELSESANSVARLIG (DPO)

KiAP har udnævnt en DPO pr. september 2023. Den valgte DPO er udnævnt på baggrund af datatilsynets retningslinier. DPO'ens opgaver er formuleret i fht. at rådgive, vejlede og overvåge, at de databeskyttelsesretlige regler (GDPR) overholdes, samt at være kontaktperson til Datatilsynet.

DPO'en refererer direkte til KiAP's øverste chef.

KiAP har pr. 10. oktober 2022 besluttet, at opgaven som DPO fremover skal varetages af en ekstern konsulent med den rette juridiske baggrund. Arbejdet med at finde en ny ekstern DPO er igangsat.

OVERFØRSEL AF PERSONOPLYSNINGER

KiAP's servere er placeret i et højt sikret datacenter i Danmark. Datacentret er koblet på sundhedsdatanettet. Derudover kar KiAP en sikker MPLS forbindelse direkte fra arbejdsstedet til datacentret.

KiAP overfører ikke persondata til tredjepart. Herunder overføres ikke persondata til lande udenfor EU/EØS. KiAP har udarbejdet en procedure, som sikrer, at dette sker ved at kontrollere nye kontrakter samt kontraktændringer for netop dette forhold, inden de godkendes.

Borgere kan tilgå egne patientdata på sundhedsmappen. Det kræver login med Mit-ID. Borgerens data er kun tilgængelige på Sundhedsmappen, såfremt der er givet samtykke. Samtykke kan ændres alene ved kontakt til egen læge.

SIKKERHED FOR BEHANDLING, ANMELDELSE OG KOMMUNIKATION

KiAP har en informationssikkerhedspolitik, som overordnet definerer og sætter rammerne for de tekniske og organisatoriske foranstaltninger. Sikkerhedspolitikken er baseret på anerkendte standardarder og er i overensstemmelse med gældende lovgivning herunder GDPR.

Der er implementeret følgende procedurer og kontroller:

- Human resource security. HR-funktionen varetages af Danske Regioners Løn- og Personalekontor. Der er udarbejdet procedurer for, at KiAP opbevarer og behandler ansøgninger fortroligt i forbindelse med rekrutteringsforløb.
- Kryptografi. Al ekstern adgang kræver nem-login, uanset om det gælder patienter eller sundhedspersonale. Der anvendes to-faktor login for medarbejdere, når der logges på VPN. Der er kontroller for adgang til personfølsomme data samt kritiske infrastrukturkomponenter.
- Fysisk og miljømæssig sikkerhed. Adgangen til alle fysiske lokaliteter er sikret mod uvedkommendes adgang. Fysisk adgang til data kræver særlig tilladelse og skal anmeldes på forhånd. Kun medarbejdere med et arbejdsmæssigt betinget formål kan opnå fysisk adgang til data. KiAP's servermiljøer er baseret på princippet om funktionsadskillelse. Kritisk it-udstyr er overvåget.
- Driftssikkerhed, inkl .:
    - Driftsprocedurer og overvågning. Der udarbejdes SOP (Standard Operation Procedures) for alle nye løsninger, der sættes i drift. Der er etableret overvågning af servere og netværksudstyr, som vil alarmere udvalgte medarbejdere i tilfælde af, at der opstår unormalitet i

driftsmiljøet. Der udføres periodisk gennemgang af sikkerhedsscanninger og driftsrapporter.
    - Udvikling, kvalitetssikring af ledelsen. Der er udarbejdet procedurer for risikovurdering ved anskaffelse og/eller udvikling og vedligehold af systemer. Herunder særligt fokus på kritiske funktioner, indeholdende personfølsomme data, som omfatter både udviklingsprocessen og test. Der er en procedurer for eskalering af særligt kritiske forhold til ledelsen. Der er udarbejdet procedure for anvendelse af pseudoanonymiseret data til lægefaglige test af særligt kritiske funktioner.
    - Logning. Adgang til personfølsomme data samt kritisk infrastruktur logges. Der udføres periodisk kontrol af adgang og logningen.
- Kommunikationssikkerhed. KiAP's IT-sikkerhedspolitik omhandler udveksling af data. Behandling af personfølsomme data, herunder sundhedsdata, må ikke foregå over e-mail eller andre åbne kommunikationskanaler. Udveksling af personfølsomme data med samarbejdspartnere sker via SDN (Sundhedsdatanettet).
- Informationssikkerhedshændelse og hændelseshåndtering. KiAP har udarbejdet en procedure for hændelseshåndtering af fejl samt sikkerhedshændelser. Der er kontroller for evaluering af hændelser og iværksættelse af nødvendige ændringer.

FULD GENNEMSIGTIGHED FOR DATAKONTROLLERE OG REGISTRERede

KiAP's procedurer og kontroller involverer medarbejderne i IT. Resultatet af gennemførte kontroller journaliseres løbende.
Brugere af KiAP's løsninger har ret til at henvende sig og få udleveret oplysninger, vi har registreret om dem. Der er udarbejdet procedurer for korrekt og behandling af sådanne henvendelser sker indenfor den gældende tidsfrist.

FORTROLIGHED VED DESIGN / STANDARD

KiAP's retningslinjer for udvikling / ændringshåndtering indeholder faste kriterier for sikkerhedsrelaterede vurderinger, herunder eskalation til ledelsen.

COMPLIANCE

KiAP har udarbejdet en række forskellige procedurer og kontroller med afsæt i GDPR/persondataforordningens kriterier for sikkerhed. Kontrollerne gennemføres periodisk jf. årshjulet, som sikrer en udjævning af opgaverne fordelt ud på året. Frekvensen for den enkelte kontrol er fastsat ud fra en vurdering af kritikaliteten. Hvis der findes forhold, der vurderes alvorlige, iværksættes den fornødne aktivitet for at håndtere situationen, evt. udarbejde en handlingsplan og eksekvere den.

Der sker mindst en gang årligt en samlet afrapportering af resultatet fra kontrollerne til ledelsen.

ÆNDRINGER I PERIODEN 1. JANUAR TIL 31. DECEMBER 2023

- KiAP har ikke foretaget væsentlige ændringer i it løsninger til almen praksis og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i erklæringsperioden.

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 dataansvarlig har ansvaret for at sikre, at administratorernes brug af IT løsninger til almen praksis og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen.

- Den dataansvarlig styrer brugerrettighederne i IT løsninger til almen praksis, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.
- Den dataansvarlige må ikke anvende IT løsninger til almen praksis til behandling, herunder opbevaring af følsomme personoplysninger, og det er den dataansvarliges ansvar at sikre, at der ikke indtastes eller uploades sådanne personoplysninger i IT løsninger til almen praksis.

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 KiAP's beskrivelse af IT løsninger til almen praksis samt for udformningen og den operationelle effektivitet 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 eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af KiAP, 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 og har fungeret effektivt i hele perioden fra 1. januar til 31. december 2023.

Udførte testhandlinger

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

Type	Beskrivelse
Forespørgsel	Forespørgsler hos KiAP's 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.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som Itavis leverer inden for Hosting services, har vi modtaget en ISAE 3402 erklæring for perioden 1. januar til 31. december 2022 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Denne underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i KiAP's beskrivelse af IT-løsninger til almen praksis og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos KiAP, 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 og implementeret eller ikke har fungeret effektivt i perioden.

Kontrolområde A

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige ▶ Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ▶ Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. ▶ Ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, anvender databehandleren en tjekliste, som fastlægger, hvad databehandleren kan leve op til. ▶ Databehandleraftaler underskrives og opbevares elektronisk. ▶ Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for indgåelse af skriftlige databehandleraftaler og observeret, at denne anfører, at informationsbehandling kun må ske på et korrekt grundlag og overholdelse af gældende retningslinjer for sikkerhed. Vi har foretaget inspektion af databehandlerens procedure for indgåelse af skriftlige databehandleraftaler, og observeret, at denne anfører, at der ved indgåelse af databehandleraftale tages udgangspunkt i datatilsynets standard databehandleraftale og, at aftalen tilpasses aktuelle vilkår i den konkrete databehandleraftale. Vi har på forespørgsel fået oplyst, at der ikke er indgået databehandleraftaler i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollerne. Vi har inspiceret, at indgået databehandleraftale er underskrevet og foreligger elektronisk samt, at denne indeholder bestemmelse om godkendelse og information af brug af underdatabehandlere.	Ingen afvigelser konstateret.
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for indgåelse af skriftlig databehandleraftale og observeret, at denne anfører, at den er med til at sikre, at de krav, som er i den pågældende databehandleraftale, overholdes.	Ingen afvigelser konstateret.

Kontrolområde A		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret skabelon for databehandleraftale og observeret, at denne indeholder instruks fra den dataansvarlige.	
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 og minimum en gang årligt. ▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandleraftale og observeret, at denne indeholder instruks fra den dataansvarlige. Vi har på forespørgsel fået oplyst, at databehandleren kun udfører behandling af personoplysninger i henhold til instruks. Vi har inspiceret databehandlerens procedure for behandling af instrukser og observeret, at denne anfører, at databehandlerens medarbejdere ikke må iværksætte instruksen, førend der er sikkerhed for, at den har hjemmel i eksisterende aftaler. Vi har inspiceret proceduren for behandling af instrukser og observeret, at denne opdateres årligt. Vi har inspiceret dokumentation for, at egenkontrol af efterlevelse af instruks ved indgåelse af databehandleraftaler er foretaget.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen. ▶ Databehandleren underretter straks den dataansvarlige i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for behandling af instrukser og observeret, at denne anfører, at vurderes en instruks at være ulovlig underrettes den dataansvarlige hurtigst muligt.	Ingen afvigelser konstateret.

Kontrolområde A		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har på forespørgsel fået oplyst, at der ikke har været modtaget instrukser, der strider mod databeskyttelseslovgivningen, hvorfor vi ikke har kunnet efterprøve proceduren herfor.	

Kontrolområde B

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering 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. ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for risikovurdering og observeret, at denne anfører, at risikovurdering skal gennemgås mindst en gang årligt med henblik på at revurdere, om sandsynlighed, konsekvens og handlingsplaner stadig er aktuelle. Vi har inspiceret risikovurderingen og observeret, at denne anfører potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. Vi har inspiceret databehandlerens risikovurdering og observeret, at denne anfører potentielle sårbarheder i systemer og processer. Vi har inspiceret dokumentation for, at den foretagne risikovurdering er udarbejdet med det formål at minimere risici ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. Vi har inspiceret databehandlerens risikovurdering og observeret, at denne senest er opdateret september 2023.	Ingen afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens beredskabsplan og observeret, at denne er opdateret i erklæringsperioden samt, at den indeholder oplysninger om kommunikation og eskaleringskriterier til sikring af hurtig responstid til brug for genetablering af normal drift.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Beredskabstest dokumenteres og evalueres.	Vi har inspiceret databehandlerens beredskabsplan og observeret, at planen er testet i 2023. Vi har inspiceret dokumentation for seneste beredskabstest og observeret, at den er blevet dokumenteret og evalueret.	
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring af, at kun autoriserede personer har adgang. ▶ Alle adgange registreres og logges. ▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har on-site observeret, at kontorlokalerne har glaspartier til gangarealet, således gæster ikke kan komme ind ad døren uden at blive set. Vi har observeret, at persondata ikke lå fremme fysisk på kontorerne. Vi har observeret, at alarmsystem logger adgange og at der er foretaget gennemgang af log, senest maj 2023	Ingen afvigelser konstateret.
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration, der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra et arbejdsbetinget behov. ▶ Der foretages kvartalsvis gennemgang af brugere og brugerrettigheder. ▶ Der foretages logning af alle brugeradgange og brugeraktiviteter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at brugeroprettelser- og nedlæggelser bliver styret via servicedesk med lederens godkendelse. Vi har ved en stikprøve inspiceret dokumentation for oprettelse er foretaget ud fra et arbejdsbetinget behov. Vi har endvidere inspiceret dokumentation for egenkontrol af brugeradgange. Vi har inspiceret udtræk over admin. rettigheder og observeret, at der ikke har været ændringer i perioden. Vi har inspiceret auditlog og observeret, at handlinger logges på databaseniveau.	Ingen afvigelser konstateret.

Kontrolområde B

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation. ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter.	Vi har observeret, at der er implementeret logisk adgangskontrol i form af password politik i active directory og to-faktor autentifikation. Vi har på forespørgsel fået oplyst, at eksterne konsulenter skal anvende samme password krav som medarbejdere, men at der ikke er anvendt ekstern konsulent i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollen.	
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. ▶ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse. ▶ Fjernadgang skal foregå via to-faktor autentifikation.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret alle mobile enheder og observeret, at de har installeret antivirus og er opdateret med seneste version. Vi har inspiceret dokumentation for, at krypterede VPN-forbindelser anvendes ved fjernadgang til systemer og databaser. Vi har observeret, at der er implementeret logisk adgangskontrol i form af to-faktor autentifikation.	Ingen afvigelser konstateret.
Eksterne kommunikationsforbindelser ▶ Eksterne adgange til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og VPN. ▶ Eksterne kommunikationsforbindelser er krypteret. ▶ Databehandleren har en oversigt over, hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at al udveksling af persondata sker gennem it-systemerne og det krypterede Sundhedsdatanet. Vi har observeret, at der kræves VPN ved fjernadgang. Vi har inspiceret dokumentation for, at firewall regler er sat op, således at kendte MAC og IP adresser får adgang til det lokale netværk, men ukendte kun får adgang til internettet.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Kryptering af personoplysninger ▶ Databehandleren har implementeret en krypteringspolitik for kryptering af personoplysninger. Politikken definerer styrken og protokollen for kryptering. ▶ Bærbare medier med personoplysninger krypteres ved overførsel af fortrolige og følsomme personoplysninger via internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens krypteringspolitik og observeret, at denne anfører, at hovedreglen er, at persondata ikke sendes manuelt, men deles gennem de systemintegrationer, som er oprettet til formålet. Vi har inspiceret dokumentation for, at bærbare medier er krypterede. Vi har inspiceret dokumentation for, at krypterede VPN-forbindelser anvendes ved fjernadgang til systemer og databaser.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler anvender kun services/porte, som de har behov for. ▶ Firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret firewallopsætningen og observeret, at firewallen er konfigureret således, at kun tilsigtede åbne porte kan få adgang.	Ingen afvigelser konstateret.
Netværkssikkerhed ▶ Netværkstopologien er struktureret således, at servere, som driver applikationer, ikke kan nås direkte fra internettet. ▶ Databehandlerens netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret interface konfigurationen og observeret, at netværket er segmenteret i vlan alt efter, hvilke roller serverne har. Vi har på forespørgsel fået oplyst, at ekstern datacenterleverandør styrer netværksopsætningen, herunder firewall opsætning og bruteforce setup for at beskytte internt netværk.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Databehandleren anvender kendte netværksteknologier og mekanismer (Firewall/Intrusion DetectionSystem/Intrusion Prevention System) for at beskytte internt netværk.		
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateres med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at antivirus er installeret på alle servere og arbejdsstationer. Vi har på forespørgsel fået oplyst, at ekstern datacenterleverandør sikrer løbende opdatering af antivirus-software på servere. Vi har inspiceret dokumentation herfor. Vi har inspiceret dokumentation for, at arbejdsstationer er opdaterede, herunder observeret, at visuel kontrol af dashboard løbende foretages, som viser, at arbejdsstationer tilsluttet Intune løsningen, alle er opdaterede.	Ingen afvigelser konstateret.
Sårbarhedsscanning ▶ Der udføres årligt en sårbarhedsscanning af databehandlerens netværk. Resultatet dokumenteres i en rapport. ▶ Databehandleren gennemgår rapporten, og følger op på konstaterede svagheder. ▶ Databehandler håndterer/mitigerer eventuelle sårbarheder ud fra en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af, at der er foretaget SSL server test. Vi har inspiceret dokumentation for, at rapporter er gennemgået, og at sårbarheder håndteres ud fra en risikobetragtning.	Ingen afvigelser konstateret.

Kontrolområde B

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
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 som minimum årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at ekstern datacenterleverandør står for backup og restore af servere hos KiAP. Ud over filbackup af hele serveren, tager ekstern datacenterleverandør også MSSQL server backup af SQL server instanserne. Vi har inspiceret ISAE 3402 erklæring fra underdatabehandler og observeret, at der heri ikke er observationer vedrørende backup. Vi har inspiceret dokumentation for, at der er foretaget specifik restoretest af KiAP data.	Ingen afvigelser konstateret.
Vedligeholdelse af systemsoftware ▶ Databehandler fører en oversigt over systemsoftware/tredjepartsprogrammer som vedligeholdes og opdateres løbende. ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende. ▶ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for opdatering af systemsoftware for henholdsvis servere og arbejdsstationer og observeret, at databehandler har en oversigt over anvendte systemsoftware/tredjepartsprogrammer. Vi har inspiceret dokumentation for, at der løbende er foretaget patching, herunder konfigurationen herfor. Vi har inspiceret procedure for opdatering af software og observeret, at det styres via Intune løsning.	Ingen afvigelser konstateret.

Kontrolområde B

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges. ▶ Loggen slettes efter den fastsatte retentionsperiode ▶ Databehandler monitorerer og logger netværkstrafik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af, at logning foretages, herunder ved en stikprøve inspiceret log af VPN, Windows, SSH, som viser både succesfulde og mislykkede adgangsforsøg. Vi har inspiceret konfigurationen for retention perioden på applikations- og securitylogs. Vi har på forespørgsel fået oplyst, at logning af netværkstrafik ligger i firewall hos datacenter udbyderen. Vi har inspiceret dokumentation for monitorering af sites, og at mail modtages, hvis netværksforbindelsen går ned.	Ingen afvigelser konstateret.
Overvågning ▶ Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. ▶ Databehandleren notificeres om identificerede alarmer, og følger op herpå.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret service manager og observeret, at der er overvågning af kapacitet mv. Vi har ved en stikprøve inspiceret dokumentation for overvågning af servere. Vi har stikprøvevist inspiceret alarmer i perioden, som databehandleren har modtaget via mail til brug for opfølgning.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Reparation og service samt bortskaffelse af it-udstyr ▶ Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger. ▶ Databehandleren foretager sikker sletning af data på databærende medier ▶ Databehandleren fører en oversigt af destrueret it-udstyr.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer og observeret, at enheder wipes inden levering til destruktion. Vi har inspiceret liste over destrueret udstyr i erklæringsperioden og ved en stikprøve inspiceret dokumentation for, at den seneste destruktion af IT-udstyr er sket i henhold til relevant procedure.	Ingen afvigelser konstateret.
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurderer og evaluerer effektiviteten af, at de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for afprøvning og vurdering af tekniske sikkerhedsforanstaltninger, herunder sikkerhedsscanninger af webserverne. Vi har inspiceret dokumentation for, at databehandler har foretaget vurdering af de organisatoriske sikkerhedsforanstaltninger, som bl.a. inkluderer log over adgang til personfølsomme data, organisering i udviklingsteams og drift.	Ingen afvigelser konstateret.
Udvikling og vedligeholdelse af systemer ▶ Databehandleren arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelsesopgaver. ▶ Risikovurdering af systemændringer er udført for, at sikre databeskyttelse gennem design og standardindstillinger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for anskaffelse, udvikling og vedligehold og observeret, at der heri er medtaget retningslinier i forhold til sikring af pricacy-by-design.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har ved en stikprøve inspiceret dokumentation for, at risikovurdering ved systemændring har inkluderet databeskyttelse.	
Informationssikkerhed i udvikling og ændringer ▶ Databehandler arbejder ud fra security-by-design principper i udviklings- og ændringsopgaver. ▶ Rollback-plan er implementeret i tilfælde af fejl i produktionsmiljøet. ▶ Brugeroprettelse sker som udgangspunkt med laveste brugerrettighedsniveau. ▶ Kun databehandlerens udviklere har adgang til kildekode.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for anskaffelse, udvikling og vedligehold. Vi har observeret, at alle servere har samme sikkerhedsforanstaltninger. Vi har inspiceret GitHub, hvori kildekoden opbevares, og som muliggør rollback. Vi har observeret, at kun udviklere og it-driften har adgang til GitHub, herunder at det kun er IT-chefen, som har admin adgang i henhold til arbejdsbetinget behov. Vi har ved en stikprøve inspiceret, at udvikler er oprettet med laveste rettigheder.	Ingen afvigelser konstateret.
Adskillelse af udviklings-, test og produktionsmiljø ▶ Der er indført funktionsadskillelse mellem udvikling og drift. ▶ Ændringer af funktionalitet testes, inden det sættes i drift. ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. ▶ Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode. ▶ Udviklings- og testmiljøer er adskilte.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af netværksdiagram og observeret, at der er adskillelse mellem udvikling og drift. Vi har inspiceret udtræk over udviklingssager i erklæringsperioden, og observeret, at der skelnes mellem udviklingsprojekter og driftsprojekter.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har for en stikprøve inspiceret dokumentation for, at test er foretaget før release. Vi har inspiceret dokumentation for versionsstyring. Vi har observeret, at der skelnes mellem udvikling og driftsprojekter, og inspiceret dokumentation for at udvikling, test og produktionsmiljøet er adskilte.	
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes fiktionelt og/eller anonymiseret testdata i udviklings- og testmiljø.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi er ved forespørgsel blevet informeret om, at testdata for klyngevisninger er aggregeret og således anonymiseret, og at data i øvrigt i udviklingsmiljøet indeholder opdigtede sygdomsforløb, navne og cpr-numre. Vi har ved en stikprøve inspiceret testdata på forløbsplaner og observeret, at der anvendes fiktive testdata.	Ingen afvigelser konstateret.
Supportopgaver ▶ Supporterede adgange og håndtering af personoplysninger ved supportopgaver sker ud fra support tickets og supporterens arbejdsbetingede behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at supportere ikke har adgang til personoplysninger.	Ingen afvigelser konstateret.

Kontrolområde C

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt. ▶ Databehandlerens databeskyttelsespolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik samt senest opdateret august 2023. Vi har inspiceret, at databehandleren har udarbejdet og implementeret en databeskyttelsespolitik samt senest opdateret november 2023.	Ingen afvigelser konstateret.
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 inspiceret databehandlerens procedure ved ansættelse af medarbejdere, og har ved forespørgsel fået oplyst, at eksternt rekrutteringsbureau sikrer screening af potentielle medarbejdere. Vi har inspiceret huskeliste, som anvendes i forbindelse med ansættelse og ved en stikprøve observeret, at proceduren er fulgt.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har Inspiceret databehandlerens huskeliste ved ophør af ansættelse, hvori aktiviteter vedr. nedlæggelse af brugeradgange, inddragelse af aktiver og organisatoriske handlinger fremgår.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har ved en stikprøve af fratrådte medarbejdere inspiceret huskelisten og observeret, at den indeholder krav om afslutningsmøde, hvor medarbejderen informeres om, at tavshedsklausulen fortsat er gældende efter ansættelsens ophør.	
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 samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret proceduren for awareness-træning, hvoraf det fremgår, at alle medarbejdere skal gennem træningsprogrammet. Vi er ved forespørgsel blevet informeret om, at nye medarbejdere tilmeldes programmet ved ansættelse, og at der bliver udsendt rykkere til medarbejdere hvert kvartal, hvis de er mere end 2 kurser bagud. Vi har inspiceret dokumentation for medarbejderes deltagelse i træning og ved forespørgsel fået oplyst, hvordan der er fulgt op på medarbejdere, der mangler at færdiggøre træningen.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren udfører løbende awareness-kampagner i form af, opslag, morgenmøder [mv.] ▶ Databehandleren udfører oplysningskampagner for medarbejdere om databeskyttelse og informationssikkerhed. ▶ Databehandleren afholder møder månedligt om behandling og beskyttelse af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret træningsmateriale samt awareness posters mv. og observeret, at der løbende foretages træning og er kampagner mv.	Ingen afvigelser konstateret.

Kontrolområde C

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Alle medarbejdere har underskrevet en tavsheds- og fortrolighedsaftale. ▶ Eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret ansættelsestjeklisten og ved en stikprøve udvalgt ansættelseskontrakt og observeret, at det heraf fremgår, at der underskrives en fortrolighedserklæring. Vi har ved en stikprøve inspiceret fortrolighedserklæringen og observeret, at den foreligger i underskreven stand. Vi har inspiceret aftale med ekstern datacenterleverandør og observeret, at denne indeholder et afsnit vedrørende tavshedspligt.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til behandlingssikkerhed og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32 og 35-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har en inspiceret databehandleraftalen og observeret, at denne indeholder et afsnit vedrørende databehandlerens bistand til den dataansvarlige i forbindelse med overholdelse af dennes forpligtelser i medfør af Databeskyttelsesforordningens artikel 32-36. Vi har på forespørgsel fået oplyst, at der ikke har været forespørgsel fra dataansvarlig vedrørende bistand, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde C

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Bistand til den dataansvarlige i forhold til revision og inspektion ▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandler bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandleraftalen og observeret, at databehandler heri forpligter sig til at stille en erklæring til rådighed. Nærværende erklæring gør, at databehandler overholder denne forpligtelse. Vi har inspiceret databehandleraftalen og observeret, at denne indeholder et afsnit vedrørende databehandlerens bistand til den dataansvarlige i forbindelse med overholdelse af dennes forpligtelser i medfør af Databeskyttelsesforordningens artikel 32-36. Vi har på forespørgsel fået oplyst, at der ikke har været forespørgsel fra dataansvarlig vedrørende bistand, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
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. ▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret fortegnelse over behandlingsaktiviteter og har observeret, at denne løbede er blevet opdateret i erklæringsperioden, samt at fortegnelsen opbevares elektronisk.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Udvælgelse af Databeskyttelsesrådgiver ▶ 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 ved forespørgsel fået oplyst, at databehandleren ikke havde en DPO de første tre måneder i perioden, men efterfølgende har udpeget en DPO. Vi har fået oplyst at databehandleren ikke har en procedure for udpegelsen af DPO, men følger datatilsynets vejledning.	Vi har konstateret, at databehandleren ikke havde en DPO i perioden 1. januar til 31. marts 2023. Ingen yderligere 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. ▶ Databehandleren har udarbejdet og implementeret en beskrivelse af databeskyttelsesrådgiverens stilling. ▶ Databehandleren inddrager databeskyttelsesrådgiveren vedrørende beskyttelse af personoplysninger. ▶ Databeskyttelsesrådgiveren rapporterer direkte til databehandlerens ledelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret DPO'ens opgaver og stillingsbeskrivelse. Vi er blevet oplyst om, at DPO inddrages i sager omkring personoplysninger, og at DPO rapporterer direkte til ledelsen. Vi har inspiceret kontrakt for DPO og observeret, at den indeholder bestemmelse om fortrolighed.	Ingen afvigelser konstateret.
Databeskyttelsesrådgiverens opgaver ▶ Databehandleren har udarbejdet og implementeret en opgavebeskrivelse af databeskyttelsesrådgiverens opgaver. ▶ Databeskyttelsesrådgiveren udfører ikke andre opgaver, der er i konflikt med opgaverne som databeskyttelsesrådgiver hos databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret DPO'ens opgavebeskrivelser. Vi har ved forespørgsel fået oplyst, at DPO'en ikke udfører opgaver, som er i konflikt med andre opgaver.	Ingen afvigelser konstateret.

Kontrolområde D

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sletning og tilbagelevering af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at der ikke eksisterer en politik for tilbagelevering og sletning af persondata, når en aftale ophører, idet databehandleren ikke opbevarer data, som ikke i forvejen findes i lægens journalsystem. Vi har inspiceret databehandleraftalen og observeret, at denne tilsvarende anfører, at krav om sletning og tilbagelevering ikke gælder, hvis der ikke opbevares data.	Ingen afvigelser konstateret.

Kontrolområde E

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Opbevaring af personoplysninger ▶ Personoplysninger opbevares utilgængeligt for andre. ▶ Adgang til personoplysninger tildeles på baggrund af et arbejdsbetinget behov/need-to-know principper.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at personoplysninger opbevares på drev utilgængeligt for andre, og kun dem med rettigheder får adgang hertil. Vi har inspiceret procedure for adgangsstyring. Vi har inspiceret adgangsgrupper til filserver og folderstruktur. Vi har inspiceret liste over medarbejdere med adgang til behandling af ind- og uddata, der viser, at adgang er givet i henhold til et arbejdsbetinget behov.	Ingen afvigelser konstateret.

Kontrolområde F

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftaler og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandleraftalen med underdatabehandler og databehandleraftaleskabelonen og observeret, at underdatabehandlere herigennem er pålagt samme databeskyttelsesforpligtelser, som databehandleren er underlagt. Vi har inspiceret dokumentation for, at databehandleraftale med underdatabehandler opbevares elektronisk samt, at denne indeholder informationer om brugen af underdatabehandlere.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelon for databehandleraftale og observeret, at godkendt underdatabehandler fremgår.	Ingen afvigelser konstateret.
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 vedrørende udskiftning af underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandleraftalen og observeret, at denne indeholder en proces for udskiftning af godkendte underdatabehandlere, herunder at dataansvarlig skal underrettes, hvorved den dataansvarlige har mulighed for at gøre indsigelse mod ændringer eller tilføjelser. Da der ikke har været ændringer i brugen af underdatabehandlere, har vi ikke kunnet teste dette.	Ingen afvigelser konstateret.

Kontrolområde F		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Ved udskiftning af underdatabehandler skal databehandleren have en ny forudgående specifik skriftlig godkendelse fra dataansvarlig.		
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet, hvem der er kontaktperson, lokation for behandling samt hvilken type af behandling og kategori af personoplysninger, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret oversigt over godkendte underdatabehandlere og observeret, at underdatabehandlere fremgår.	Ingen afvigelser konstateret.
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 foretaget inspektion for procedure ved tilsyn, og observeret, at der skal udføres skriftligt tilsyn ved underdatabehandlere. Vi har inspiceret seneste ISAE 3402 erklæring fra underdatabehandler og endvidere observeret, databehandlerens egen gennemgang heraf. Vi har ved forespørgsel fået oplyst, at der ud fra en risikobetragtning er foretaget yderligere tilsyn ved forespørgsel af underdatabehandler i forhold til overholdelse af GDPR specifikke forhold i henhold til databehandleraftalen. Vi har observeret, at tilsyn er foretaget i erklæringsperioden, og således minimum en gang om året.	Ingen afvigelser konstateret.

Kontrolområde H

Kontrolmål

- *Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsninger af oplysninger om behandling af personoplysninger til den registrerede.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Bistand til den dataansvarlige i forhold til de registreredes rettigheder ▶ Databehandler har udarbejdet en procedure for bistand til den 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 procedurer for bistand til den dataansvarlige og efterlevelse af de registreredes rettigheder. Vi har ved forespørgsel fået oplyst, at det er muligt at give indsigt, men at der ikke har været forespørgsel, idet lægerne selv har adgang til data, hvorfor vi ikke har kunnet efterprøve kontrollen. Vi har ved forespørgsel fået oplyst, at der ikke har været forespørgsler om bistand til den dataansvarlige, men vi har inspiceret dokumentation for dialog med datatilsynet i forhold til, hvordan de registreredes rettigheder kan overholdes i perioden mellem lægeskift.	Ingen afvigelser konstateret.

Kontrolområde I		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for hændelsesstyring og observeret, at der heri fremgår, at underretning skal gives uden unødig forsinkelse i et klart og tydeligt sprog, og skal ske via en sikker forbindelse Vi har observeret, at der er opsat handlinger, som skal udføres i forbindelse med reaktionen på en hændelse. Vi har ved forespørgsel fået oplyst, at der ikke har været brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har opsat foranstaltninger til at identificere brud på persondatasikkerheden. ▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at der med afsæt i den gældende risikovurdering og de lægefaglige processer i virksomheden, hvor der arbejdes med persondata, ikke er fundet grundlag for at opsætte specifik overvågning, men at der tages afsæt i awareness træning til identifikation af brud. Vi har inspiceret procedure for hændelsesstyring af brud på persondatasikkerheden og observeret, at denne indeholder krav i forhold til vurdering af konsekvensen af bruddet, og at proceduren har en skala, som konsekvensen vurderes ud fra. Vi har ved forespørgsel fået oplyst, at der ikke har været brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 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."

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner, chef for Risk Assurance, CISA, CRISC
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2024-02-15 14:18:32 UTC

Mit ID

Jan Kristensen
KiAP Fonden CVR: 30474880
IT-drifts- og udviklingschef
På vegne af: KiAP
Serienummer: ff8ade2e-445c-4d08-8353-8def6a19c518
IP: 94.18.xxx.xxx
2024-02-15 14:43:12 UTC

Mit ID

Nicolai Tobias Visti Pedersen
Partner, statsautoriseret revisor
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-02-15 15:17:08 UTC

Mit ID

Penneo dokumentnøgle: 4MPEG-XT1JF-JKA4W-M6KFW-CLQQL-OJYA2