et trygt samfund med it og data

KiAP

CVR nr.: 30 47 48 80

Revisorerklæring

Erklæring fra uafhængig revisor – ISAE 3000
Erklæringsafgivelse i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov som databehandler for leverancen af lægesystemer pr. 14. december 2020

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

December 2020

Indholdsfortegnelse

Afsnit 1: KiAP's beskrivelse af behandling

Kontrolbeskrivelse for udvikling og drift af KiAP's IT-løsninger til almen praksis

Indledning

Formålet med denne beskrivelse er at levere oplysninger til KiAP's brugere, dvs. alment praktiserende læger samt patienter (registrerede), om hvordan KiAP sikrer alle registreredes rettigheder, styrer ansvaret mellem dataansvarlige (lægeklinikker mfl.) og KiAP, samt besvarelse af spørgsmål fra personer, som har spørgsmål til KiAP's behandling af deres data.

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 (sundhedsfagligt login) og Sundhedsmappe (patient-login af Forløbsplaner)
- Akkreditering
- DanPep
- KiAP.dk /klynger (sundhedsfagligt login)

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

Vi har defineret vores kvalitetsstyringssystem 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 ensartede 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 risici 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.

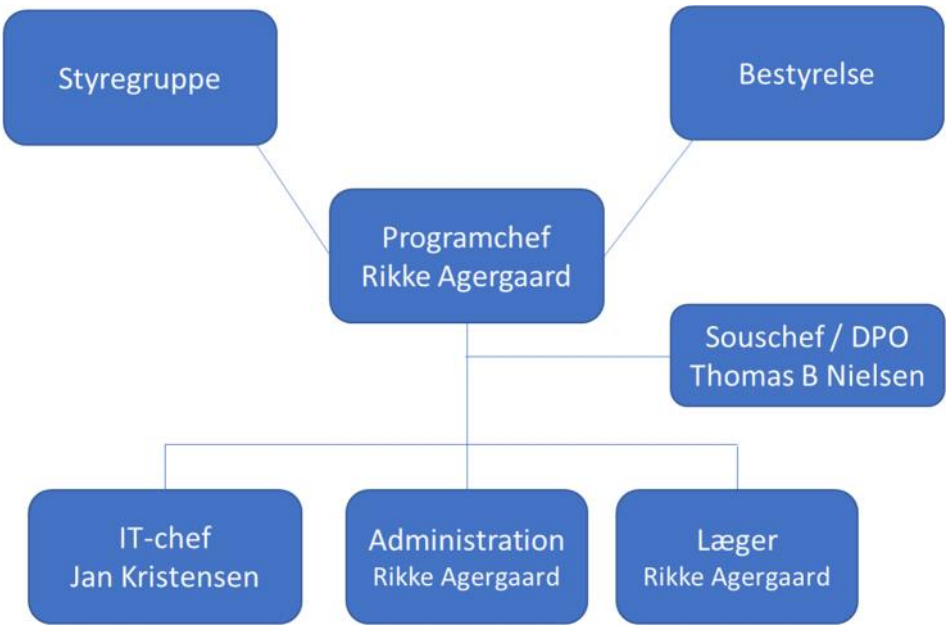
Risikovurderingen foretages både periodisk og på øverste ledelsesniveau minimum en gang årligt eller hvis der opstår særligt kritiske forhold, som ledelsen skal kende/tage stilling til. Risikovurderingen foretages også på daglig basis, når der indgår kundeønsker, foretages ændringer eller nye systemer 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, forretningsmæssige og organisatoriske forhold med afsæt i patientens risiko.

Organisation og ansvar

KiAP's organisation ser pr. oktober 2020 således ud:



KiAP's øverste ledelse er Programchef Rikke Agergaard. Virksomheden er fordelt over to lokationer i hhv. København og Odense. KiAP's praksis-læger er organisatorisk placeret under Rikke, og står for det lægefaglige kvalitetsarbejde og inddrages IT-udviklingsprocesserne efter behov. Administrationen dækker de projektopgaver, som udføres i forbindelse med kvalitetsarbejdet. Al it-udvikling, 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. 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**: 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**: 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 udføres en automatiseret sletning af patientens data på Sundhedsmappe.

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 udvikling, 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 tilgængelige 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, der er beskrevet i de gældende databehandleraftaler samt gældende lovgivning. Herunder bl.a. personers rettigheder i forbindelse med henvendelse til KiAP. Der er udarbejdet 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 2020. Den valgte DPO er udnævnt på baggrund af datatilsynets retningslinjer. DPO er pr. oktober 2020 i færd med at gennemføre en certificeret DPO-uddannelse. Det er endnu ikke udarbejdet en selvstændig opgaveoversigt for DPO, udover det eksisterende sikkerheds årshjul.

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

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 NEM-ID.

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 den anerkendte standardard ISO 27001 og er i overensstemmelse med gældende lovgivning herunder GDPR.

Der er implementeret følgende procedurer og kontroller:

- Human ressource 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 NemLogin, 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 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 rejse alarmer til udvalgte medarbejdere i fald 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 procedure for eskalering af særligt kritiske forhold til ledelsen. Der er udarbejdet procedure for anvendelse af pseudoanonymiserede data til lægefaglig 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 de oplysninger vi har registreret om dem. Der er udarbejdet procedurer for at korrekt 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 eskalering til ledelsen.

Compliance

KiAP har udarbejdet en række forskellige procedurer og kontroller med afsæt i GDPR/persondata-forordningens kriterier for sikkerheden. 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.

Komplementerende kontroller for dataansvarlige

Som led i levering af ydelserne er der kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i beskrivelsen. Dette omfatter bl.a.:

- Stillingtagen til konsekvenser i relation til persondatabeskyttelse når der ændres i eksisterende løsninger (Privacy by design og Privacy by default) og fremsættelse af ændringsanmodning hertil til KiAP i relevant omfang.
- Stillingtagen til / test af nye versioner af løsninger ifm. implementering (Change Management).
- Opsætning og styring af egne brugere i løsningen i produktionsmiljøet (Identity and Access Management).
- Risikovurdering af kritiske komponenter
- Opsætning og styring af brugere fra KiAP, som har adgang til kundens miljø (Identity and Access Management).
- Sikring af at personfølsomme oplysninger ikke medsendes i supportsager til KiAP via tickets mv.
- Opfølgning på overholdelse af indgåede databehandleraftaler.
- Løbende overvågning af sikkerheden og iværksættelse af relevante tiltag for at sikre et fortsat højt sikkerhedsniveau.
- Løbende vurdering af om de eksisterende kontroller er dækkende/relevante og tilpasning af kontroller efter vurdering.

I forlængelse af ovenstående har KiAP udarbejdet en række kontroller, som udføres periodisk, og som har til formål at dokumentere, at virksomheden på tilfredsstillende vis arbejder på at fastholde og forbedre sikkerheden omkring fortrolige data i overensstemmelse med gældende lovgivning, databehandleraftaler og forpligtigelser. I det omfang kontrollerne finder afvigelser i forhold til gældende forpligtigelser, iværksættes den relevante håndtering for at forbedre sikkerheden. Ved alvorlige afvigelser orienteres relevante parter så hurtigt som muligt.

Afsnit 2: KiAP's udtalelse

Medfølgende beskrivelse er udarbejdet til brug for KiAP's kunder, som i rollen som dataansvarlige, har anvendt KiAP's systemer; Forløbsplaner, Akkreditering, DanPep og KIAP.dk til behandling af persondata (lægesystemerne), og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

KIAP bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 1, giver en retvisende beskrivelse af lægesystemerne, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 14. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan lægesystemerne var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
   - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

- Kontroller, som vi med henvisning til lægesystemerne afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål der er anført i beskrivelsen, er identificeret i beskrivelsen
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Indeholder relevante oplysninger om ændringer ved databehandlerens lægesystemer til behandling af personoplysninger foretaget pr. 14. december 2020.

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

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 14. december 2020. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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

Odense, den 14. december 2020

KiAP

Jan Kristensen
IT Drifts- og Udviklingschef

Afsnit 3: Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov pr. 14. december 2020

Til KiAP's ledelse, selskabets kunder i rollen som dataansvarlige og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring om KiAP's beskrivelse i "Afsnit 1" af udvikling og drift af KiAP's IT-løsninger til almen praksis pr. 14. december 2020 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

KiAP's ansvar

KiAP er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i "Afsnit 2", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme og implementere kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), som er baseret på de grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

REVI-IT A/S anvender international standard om kvalitetsstyring, ISQC 1[1] , og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om KiAP's beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning. 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 implementeret effektivt.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af udvikling og drift af KiAP's IT-løsninger til almen praksis, samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke implementeret effektivt. Vores handlinger har omfattet test af funktionaliteten 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 mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "Afsnit 1".

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en dataansvarlig

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

Konklusion

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

(a) at beskrivelsen af lægesystemerne, således som denne var udformet og implementeret pr. 14. december 2020, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 14. december 2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i det efterfølgende afsnit.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt KiAP's udvikling og drift af KiAP's IT-løsninger til almen praksis, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, 14. december 2020

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Director, CISA

Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

Den følgende oversigt er udformet for at skabe et overblik over de kontroller, som KiAP har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte artikler pr. 14. december 2020 er efterlevet.

De krav, som fremgår direkte af forordningen eller loven, kan ikke fraviges. Derimod kan der justeres på, hvordan sikkerheden implementeres, da sikkerhedskravene i forordningen på flere punkter er af mere generel og overordnet karakter, som bl.a. skal tage hensyn til formål, behandlingens karakter, kategorien af personoplysninger mv. Herudover kan der være konkrete krav i de enkelte kundekontrakter, der kan have en rækkevidde, der går ud over databeskyttelseslovens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos KiAP's kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Vi har udført vores tests af kontroller hos KiAP via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos KiAP. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Kortlægning af kontrolområder op mod GDPR-artikler, ISO 27701 og ISO 27001/2

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2.

Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Nyt område ift. ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Nyt område ift. ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15**,** 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15**,** 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7
J.1	**7,** 9, **13, 14**, 18	**7.2.4**, 7.3.4	*Nyt område ift. ISO 27001/2*
J.2	7, 14, 18	**7.3.4**	*Nyt område ift. ISO 27001/2*
J.3	11, 13, 14, 15, 17, 18, 21 28	**7.3.2, 8.2.5, 8.3.1, 8.5.4, 8.5.6**	*Nyt område ift. ISO 27001/2*
J.4	11, 13, 14, 15, 17, 18, 21 28	**7.3.2, 8.2.5, 8.3.1, 8.5.4, 8.5.6**	*Nyt område ift. ISO 27001/2*
K.1	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*
K.2	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*
K.3	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til, at behandling skal følge instruks fra dataansvarlige. Vi har inspiceret politikken, og påset, at denne er opdateret.	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har inspiceret informationssikkerhedspolitikken, og stikprøvevis påset, at denne er i overensstemmelse med databehandleraftaler.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til ulovlig instruks.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, informationssikkerhedspolitikken, og påset, at der er taget stilling til overholdelse af aftaler. Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at aftale eller lignende sikringsforanstaltninger er blevet implementeret.	Ingen afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har inspiceret, informationssikkerhedspolitikken, og påset, at der er taget stilling til løbende risikovurdering. Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Vi har inspiceret, at databehandler har implementeret de tekniske foranstaltninger og organisatoriske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus-software. Vi har inspiceret, at antivirus-software er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Vi har inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har inspiceret oversigt over netværket, servere og vlan, og påset, at dette er segmenteret.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger og påset, at der er taget stilling til at brugere skal have et arbejdsbetinget behov. Vi har stikprøvevis inspiceret oprettelsen af nye brugere i perioden, og påset, at adgange er arbejdsbetinget.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har inspiceret, at der for systemer og databaser, som anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering og påset at overvågningen er sat til.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har inspiceret, at der foreligger formaliserede procedurer for kryptering, og påset, at der er taget stilling til kryptering ved transmission. Vi har inspiceret konfigurationen af SSL, NEM-ID og påset, at de teknologiske løsninger er i overensstemmelse med politikkerne. Vi har påset, at der anvendes kryptering ved transmissioner af følsomme og fortrolige personoplysninger via internettet.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.9	Der er etableret logning i systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har inspiceret, at der foreligger relevante formaliserede procedurer, og påset at disse omfatter opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Vi har inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Vi har inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form, og vi har påset at adgangen til personoplysninger skal skyldes et arbejdsbetinget behov.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til løbende test af systemer. Vi har inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til change management. Vi har stikprøvevis inspiceret ændringer, og påset, at disse følger politikken.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret proceduren for adgangsstyring, og påset, at den dækker tildeling og afbrydelse af brugeradgange. Vi har stikprøvevis inspiceret adgange på nye og fratrådte medarbejdere, og påset, at adgange er blevet tildelt eller afbrudt efter procedure. Vi har inspiceret kontrollen af adgange, og påset, at disse er blevet udført i henhold til proceduren. Vi har inspiceret, at der foreligger dokumentation for regelmæssig – som minimum årlig – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af tofaktor autentifikation.	Vi har forespurgt til, om adgang til personoplysninger, sker gennem to-faktor, og påset dokumentation herfor.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til fysisk adgangsstyring. Vi har inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har inspiceret kontrollen, og påset, at politikken løbende bliver opdateret. Vi har inspiceret dokumentation for, at informationssikkerheds-politikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at denne skal være i overens-stemmelse med aftaler. Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at informations-sikkerhedspolitikken er i overensstemmelse med aftalerne.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til ansættelse. Vi har inspiceret proceduren for ansættelse, og påset, at denne er opdateret i perioden. Vi har stikprøvevis inspiceret ansættelser i perioden, og påset, at proceduren for ansættelse er blevet fulgt.	Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har inspiceret ved en stikprøve på en nyansat medarbejder i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighed-saftale. Vi har inspiceret ved en stikprøve på en nyansat medarbejder i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: - Informationssikkerheds-politikken - Procedurer vedrørende databehandling, samt anden relevant information.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til inddragelse af aktiver og adgange. Vi har inspiceret ved en stikprøve på en fratrådt medarbejder, at rettigheder er deaktiverede eller ophørt, samt at aktiver er inddraget.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har stikprøvevis inspiceret ansættelsesaftaler, og stikprøvevis påset, at fortrolighedsaftalerne er gældende efter ansættelse.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	VI har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til løbende awarenesstræning. Vi har stikprøvevis inspiceret afholdt awarenesstræning i perioden, og stikprøvevis påset, at dette omfatter IT-sikkerhed.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver og bliver inddraget i relevante områder.	Vi har inspiceret vurderingen af behov for en databeskyttelses-rådgiver, og påset, at virksomheden har vurderet behovet for en DPO i perioden.	Ingen afvigelser konstateret.

Kontrolmål D – Tilbagelevering og sletning af personoplysninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede i perioden.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner	Vi har stikprøvevis inspiceret databehandleraftaler, og påset, at der er taget stilling til opbevaringsperioder og sletterutiner.	Vi er blevet informeret om, at der ikke har været nogle ophør af databehandleraftaler, hvorfor vi ikke har kunne verificere effektiviteten af virksomhedens relevante procedurer. Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: - Tilbageleveret til den dataansvarlige og/eller - Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har stikprøvevis inspiceret databehandleraftalen, som er ophørt, og påset, at data er blevet tilbageleveret/slettet i overensstemmelse med aftalen.	Vi er blevet informeret om, at der ikke har været nogle ophør af databehandleraftaler, hvorfor vi ikke har kunne verificere effektiviteten af virksomhedens relevante procedurer. Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at der er opsat en årlig kontrol for vurdering af hvorvidt proceduren behøver at opdateres.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har inspiceret, at data-behandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdata-behandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har inspiceret, at data-behandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har stikprøvevis inspiceret at virksomheden alene anvender underdatabehandlere som er godkendt af virksomhedens dataansvarlige partner.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har inspiceret, at der foreligger underskrevne underdata-behandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Vi har stikprøvevis inspiceret indgåede underdata-behandleraftaler og påset, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: ⎩ Navn ⎩ CVR-nr. ⎩ Adresse ⎩ Beskrivelse af behandlingen.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Vi har inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlings-aktiviteter hos underdatabe-handlerne og overholdelse af underdatabehandleraftalerne. Vi har inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Vi har inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt til, om databehandleren overfører persondata til tredjelande	Vi er blevet informeret om at der ikke overføres persondata til tredjelande Ingen afvigelser konstateret.

Kontrolmål H – De registreredes rettigheder

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har forespurgt til, om der har været anmodninger fra data-ansvarlige i perioden, og vi har inspiceret loggen over anmodninger.	Vi har observeret at KiAP ikke har modtaget persondata-anmodninger, hvorfor vi ikke har kunne verificere effektiviteten af KiAP's relevante procedurer. Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret proceduren, og påset, at denne indeholder krav om underrettelse til de dataansvarlige. Vi har inspiceret proceduren, og påset, at denne er blevet opdateret i perioden.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har stikprøvevis inspiceret awarenesstræning i perioden, og stikprøvevis påset, at medarbejdere har deltaget. Vi har inspiceret dokumentation for, at netværkstrafik overvåges, og at der sker opfølgning på uregelmæssigheder, overvågningsalarmer, overførsel af store filer mv.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret loggen over hændelser, og forespurgt til, om der har været brud på persondatasikkerheden i perioden. Vi har forespurgt til, at registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Vi har observeret at virksomheden har haft et sikkerhedsbrud og at dette er blevet meldt til Datatilsynet rettidigt. Vi har dog observeret at KiAP ikke kan dokumentere at dens dataansvarlige parter blev orienteret om sikkerhedsbruddet rettidigt. Vi er dog blevet informeret om at KiAP's dataansvarlige parter blev orienteret telefonisk. Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: - Karakteren af bruddet på persondatasikkerheden - Sandsynlige konsekvenser af bruddet på persondatasikkerheden - Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	VI har inspiceret proceduren for sikkerhedsbrud, og påset, at der er taget stilling til bistand til de dataansvarlige.	Ingen afvigelser konstateret

Kontrolmål J – Betingelser for samtykke og oplysningspligt

Der efterleves procedurer og kontroller, som sikrer, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger, og hvori det sikres, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt anden information, der er nødvendig for opfyldelse af oplysningspligten.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
J.1	Der foreligger skriftlige procedurer for indhentelse af skriftligt samtykke til behandling af personoplysninger. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt til, om virksomheden indhenter samtykke på vegne af de dataansvarlige.	Vi er blevet oplyst, at virksomheden ikke indhenter samtykke på vegne af de dataansvarlige. Ingen afvigelser konstateret.

Kontrolmål K – Fortegnelse over behandlingsaktiviteter

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
K.1	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret fortegnelsen, og påset, at fortegnelsen indeholder relevante punkter.	Ingen afvigelser konstateret.
K.2	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	Vi har inspiceret fortegnelsen, og påset, at denne er blevet opdateret i perioden.	Ingen afvigelser konstateret.
K.3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Vi har inspiceret fortegnelsen, og påset, at denne er blevet godkendt af ledelsen i perioden.	Ingen afvigelser konstateret.