SUNDHED.DK - SENTINEL

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 15. NOVEMBER 2023 OM BESKRIVELSEN AF SENTINEL OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 15. NOVEMBER 2023 OM BESKRIVELSEN AF SENTINEL OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Sundhed.dk - Sentinel
Sundhed.dk – Sentinels' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Sundhed.dk - Sentinel (databehandleren) pr. 15. november 2023 udarbejdede beskrivelse i sektion 3 af Sentinel og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme og implementere kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Begrænsninger i kontroller hos en databehandler

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af Sentinel, som hver enkelt dataansvarlig måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

Konklusion

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

a. at beskrivelsen af Sentinel og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 15. november 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 pr. 15. november 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 Sentinel system, 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 4. marts 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, statsautoriseret revisor

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

2. SUNDHED.DK - SENTINEL'S UDTALELSE

Sundhed.dk - Sentinel varetager behandling af personoplysninger i forbindelse med Sentinel 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 Sentinel. Beskrivelsen skal give de dataansvarlige tilstrækkelig forståelse til at vurdere om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt. Beskrivelsen skal ses i sammenhæng med de sikkerhedsforanstaltninger og kontroller som de dataansvarlige har ansvar for jf s.11: Komplementerende kontroller hos de dataansvarlige inkl. Lægepraksissystemer.

Sundhed.dk - Sentinel anvender underdatabehandler Cloudio og MedCom. De relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Sundhed.dk - Sentinel bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af Sentinel og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 15. november 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for Sentinel, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at begrænse behandling af personoplysninger.
    - De processer der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - De processer der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
    - De processer der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
    - De processer der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
    - De kontroller, som vi med henvisning til afgrænsningen af Sentinel har forudsat ville være udformet og implementeret af de dataansvarlige jf. side 11 og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

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

Sundhed.dk - Sentinel bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 15. november 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.

Sundhed.dk - Sentinel bekræfter, at der er implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Odense, den 4. marts 2024

Sundhed.dk - Sentinel

Claus Duedal Pedersen
Enhedschef, Sentinelenheden

3. SENTINEL ENHEDENS BESKRIVELSE AF PROGRAMMET SENTINEL OG BEHANDLING AF PERSONOPLYSNINGER

Sentinel Enheden er en enhed under Sundhed.dk, og enhedens kerneopgave er udvikling, drift og support af selve Sentinel programmet.

Sentinel er et program, der installeres af systemhuset i kundens praksissystem. Kunden skal bede eget systemhus om installation. På denne måde er Sentinel en forlængelse af kundens eget praksis IT-system. Sentinel tager kopi af strukturerede data i patientjournalen og gemmer kopien lokalt hos kunden i en SQL database, som benævnes kundens egen lokale Sentinel databank. Herfra er det muligt for Sentinel programmet at opsamle de journaldata, som kunden giver tilladelse til, med henblik på behandling i sundhed.dk databanken i Sentinel Enheden. I Sundhed.dk databanken behandles de data kunden har givet tilladelse til og de returneres til kunden i struktureret form. I sundhed.dk databank har hver kunde sin egen "konto", hvor en kopi af de udvekslede oplysninger gemmes. Formålet med denne anvendelse er at lave en kvalitetsrapport, der giver den sundhedsfaglige systematiseret overblik over egne patienter og disses data, med henblik på kvalitetsudvikling og egen læring.

I kvalitetsrapporten ser man samtidig egne data i forhold til aggregerede data. Det vil sige, at man kan benchmarke egen behandling med et samlet gennemsnit. En kvalitetsrapport indeholder således oplysninger genereret fra kundens egen konto i sundhed.dk databank og aggregerede oplysninger til benchmarking, der er genereret ud fra data i en statistikbank med ikke patienthenførebare oplysninger.

Fra Sundhed.dk databanken rapporteres endvidere data til godkendte landsdækkende kliniske kvalitetsdatabaser. Disse data er personhenførbare, jf. den til enhver tid gældende lovgivning om kliniske kvalitetsdatabaser. Endvidere skal regionerne i henhold til overenskomst for de praktiserende speciallæger modtage oplysning om diagnosekoder i den enkelte klinik, men uden personoplysninger, der kan spores tilbage til en konkret patient.

Følgende typer af data behandles i Sentinel systemet for praktiserende speciallæger:

Almindelige persondata
- Navn, Fødselsdato, Køn (fra CPR nr)
- Adresse
- Egen læge - Ydernummer

Fortrolige
- CPR-nummer

Følsomme Persondata
- ICD-10 koder
- Medicin
- Labsvar
- Henvisninger
- Notat
- Epikriser

For kiropraktorområdet gælder det endvidere, at der, udover de sammen data som for speciallæger, indsamles Ydelsekoder.

Sundhed.dk, Sentinel Enheden agerer som databehandler for løsningen. Alt persondata opbevares sikkert og forsvarligt indenfor Danmarks grænse og intet data overføres til 3. land.

STYRING AF PERSONDATASIKKERHED

For at kunne benytte Sentinel til kvalitetsudvikling hos kunden, kræves det, at der er indgået en gyldig databehandler aftale med Sundhed.dk. Sentinel programmet er designet med indbygget standardsikkerhedsforanstaltninger, hvilket bl.a. betyder at data ikke kan udveksles medmindre der foreligger en digital signeret databehandleraftale
Herudover kræves det at kunden tager eksplicit stilling til de projekter, og hermed de data, der sendes fra den lokale Sentinel databank til Sundhed.dk databank. Tilladelse gives af kunden i administrationsmodulet i forbindelse med projekttilmelding. Der udveksles altså kun de oplysninger, den dataansvarlige har givet tilladelse til.

Alt data sendes krypteret via sundhedsdatanettet. For mere information, se på eKVIS hjemmeside om Sentinel eller på KIVKs hjemmeside om Sentinel.

Sentinels centrale data ligger hos en dansk (IaaS) cloud leverandør, i et datacentermiljø, som er akkrediteret efter ISO 27001, ISO 22301 og SOC2. Vores underdatabehandler leverer herudover en årlig uafhængig ISAE 3402 revisor erklæring.

Sentinel informationssikkerhedsstrategi er risikostyret og med fokus på løbende forbedringer af informationssikkerheden med udgangspunkt i relevante områder og principper fra ISO 27001 og den sektorspecifikke informationssikkerhedsstrategi for sundhedsvæsnet 2019-2022. Her kan særligt fremhæves relevante initiativer indenfor områderne: Forudse, forebyg, opdage og håndtering af hændelser.

Til at støtte og supplere informationssikkerhedsarbejdet benytter Sentinel Enheden skabeloner, div. vejledninger og informations fra bl.a. initiativer fra hjemmesiden SikkerDigital omkring implementering af ISO 27001 som er et nationalt tiltag som private og offentlige myndigheder frit kan benytte. Herudover benyttes andre anerkendte kilder omkring informationssikkerhed f.eks. fra datastyrelsen.

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

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
Risikovurdering	• Risikovurdering	• Artikel 28, stk. 3, litra c
A.5: Informationssikkerhedspolitikker	• Informationssikkerhedspolitik • Gennemgang af informationssikkerhedspolitik	• Artikel 28, stk. 1
A.6: Organisering af informationssikkerhed	• Roller og ansvarsområder • Fjernarbejdspladser og fjernadgang til systemer og data	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra c
A.7: Personalesikkerhed	• Rekruttering af medarbejdere • Uddannelse og awareness af medarbejdere • Tavsheds- og fortrolighedsaftale med medarbejdere • Fratrædelse af medarbejdere	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra b
A.8: Styring af aktiver	• Fortegnelse over kategorier af behandlingsaktiviteter	• Artikel 30, stk. 2, 3 og 4
A.9: Adgangsstyring	• Logisk adgangssikkerhed, herunder autorisation og adgangskontrol	• Artikel 28, stk. 3, litra c
A.10: Kryptografi	• Kryptering af personoplysninger	• Artikel 28, stk. 3, litra c
A.11: Fysisk sikring og miljøsikring	• Fysisk adgangskontrol • Fysisk sikkerhed	• Artikel 28, stk. 3, litra c
A.12: Driftssikkerhed	• Vedligeholdelse af systemsoftware • Antivirusprogram • BackupLogning og overvågning • Sårbarhedsscanning og penetrationstests	• Artikel 28, stk. 3, litra c
A.13: Kommunikationssikkerhed	• Styring af netværkssikkerhed • Informationsoverførsel	• Artikel 28, stk. 3, litra c

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
A.14: Anskaffelse, udvikling og vedligeholdelse	• Udvikling og vedligeholdelse af systemer • Informationssikkerhed i ændring og udvikling • Adskillelse af udviklings-, test- og produktionsmiljø	• Artikel 25
A.15: Leverandørforhold	• Underdatabehandlere	• Artikel 28, stk. 2 og 4
A.16: Styring af informationssikkerhedsbrud	• Underretning om brud på persondatasikkerheden	• Artikel 33, stk. 2
A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring	• Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse	• Artikel 28, stk. 3, litra c
A.18: Overensstemmelse	• Indgåelse af databehandleraftale • Instruks for behandling af personoplysninger • Underretning af den dataansvarlige ved ulovlige instrukser fra • Sletning af personoplysninger • Overførsel af personoplysninger til tredjelande • Udpegelse af databeskyttelsesrådgiveren • Databeskyttelsesrådgiverens stilling • Databeskyttelsesrådgiverens opgaver • Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger	• Artikel 28, stk. 3, litra a, c, e, f, g og h • Artikel 29 • Artikel 32, stk. 4 • Artikel 28, stk. 10 • Artikel 44 - 49

RISIKOVURDERING

Der er foretages løbende risikovurdering ift. de registreredes rettigheder, ud fra en kortlægning af de risici, som databehandlingen medfører. Dette sker ud fra en reel og kompetent vurdering af evt. sårbarheder og truslen, i og omkring Sentinel systemet, udført af de IT-specialister, som arbejder med systemet.

Er der nogen væsentlig sandsynlighed for at en trussel og sårbarhed kan udnyttes, og at det kan kompromittere den registreredes rettigheder, igangsættes der omgående mitigerende tiltag.
Alle identificeret risici prioriteres og håndteres efter kritikalitet – højeste har første prioritet ift. at finde og implementere mitigerende tiltag.

Omdrejningspunktet for risikoarbejdet er løbende at blive bedre til at forudse, forebyg, opdage og håndtere hændelser.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

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

A.5: Informationssikkerhedspolitikker

Informationssikkerhedspolitikken opdateres årligt og godkendes endeligt af Enhedschefen for Sentinel.

Den nuværende informationssikkerhedspolitik definerer roller og ansvar i det daglige arbejde med informationssikkerhed. Informationssikkerhedsstrategien er fokuseret på sårbarheds- og risikoidentificering minimering, og er opdelt efter IT-specialisternes arbejdsområder og de relevante ISO27001 anneks A områder.

Dette fundament vil sikre at der fremadrettet arbejdes effektivt med informationssikkerhed. Dvs. at det er de rigtige procedure og politiker der fremadrettet udarbejdes, og at de har den rigtige kvalitet og bliver velimplementeret.

A.6: Organisering af informationssikkerhed

Roller og ansvarsområder
Roller og ansvarsområderne fremgår af informationssikkerhedspolitikken.

Enhedschefen er formand for den lokale informationssikkerhedsgruppe. Herudover fungere tre af IT-specialisterne som henholdsvis informationssikkerhedskoordinator, systemsikkerhedsejer og datasikkerhedsejer.

Sentinel Enheden benytter sundhed.dks central DPO-funktion. Alle medarbejdere har et ansvar i løbende at forbedre informationssikkerheden af Sentinel systemet og har et særligt fokus på deres egne arbejdsområder f.eks. applikationsudvikling, infrastrukturdrift og vedligehold osv.

Funktionsadskillelse
Funktionsadskillelse følger medarbejdernes primære arbejdsområder i Sentinel Enheden. Da Sentinel Enheden er en mindre enhed, sker opdeling efter behov.

Politik for mobilt udstyr
Udleveret udstyr fra sundhed.dk er administrativt underlagt de restriktioner, som følger med udstyret og den brugertyper slutbrugeren er. Der må kun være krypteret persondata på mobilt udstyr og persondataene slettes så snart formålet hermed er opnået.

Fjernarbejdspladser og fjernadgang til systemer og data
Kan kun ske via krypterede og sikre adgang via VPN eller gennem dedikeret firewall.

A.7: Personalesikkerhed
Rekruttering og fratrædelse af medarbejdere
Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere.

Uddannelse og instruktion af medarbejdere, der behandler personoplysninger og Awareness og oplysningskampagner for medarbejdere
Der planlægges og arbejdes kontinuerligt med at forbedre medarbejderne viden omkring informationssikkerhed bl.a. gennem awareness træning.

Fortrolighed og lovbestemt tavshedspligt
Medarbejderne underskriver fortrolighedserklæringer, hvis de har omgange med persondata.

A.8: Styring af aktiver

Fortegnelse over kategorier af behandlingsaktiviteter
Sentinel Enheden har jf. aftale med dataansvarlige overblik, databehandleraftale og underdatabehandleraftale overblik herover. Der er udarbejdet fortegnelser over behandlingsaktiviteter for at understøtte vores forpligtigelse overfor den dataansvarlige.

A.9: Adgangsstyring

Der gives kun adgang til relevante medarbejder efter anmodning og adgangsrettighederne tildeles på laveste niveau.

Alle adgange og aktiviteter logges.

A.10: Kryptografi

Alt persondata skal sendes krypteret og opbevares sikkert bag ved tekniske sikkerhedsforanstaltninger.

A.11: Fysisk sikring og miljøsikring

Fysisk adgangskontrol
Adgangsstyring sker via medarbejder chip og retningslinjer ved brug af lokalerne.

Alle chip aktiviteter logges.

Fysisk sikkerhed
Ved egen fysisk lokation er adgangskontrollen styret af chip-adgang som er registret til medarbejderen. Kontormiljøet aflåses, når man forlader kontoret. Den sidste medarbejder låser og sætter alarmen til.

Underleverandøren som leverer infrastruktur som en service til Sentinel Enheden, benytter et datacenter som er akkrediteret efter ISO 27001, ISO 22301 og SOC2. Herudover leverer underleverandøren en årlig uafhængig ISAE 3402 revisor erklæring.

A.12: Driftssikkerhed

Vedligeholdelse af systemsoftware
Alle tekniske og administrative systemer opdateret jævnligt.

Antivirusprogram
Alle tekniske og administrative systemer opdateret jævnligt.

Sikkerhedskopiering og retablering af data
Der foretages sikkerhedskopiering af data jævnligt. Der udføres test af reetablering af data.

Logning i systemer, databaser og netværk
Der foretages logning af aktivitet i Sentinel systemet, herunder databaser og i de netværk som der benyttes.

Overvågning
Systemerne overvåges løbende medhenblik på at opdage og identificere ondsindet aktiviteter.

Sårbarhedsscanning og penetrationstests
Systemerne bliver løbende vurderet internt igennem skanning, abonnering af eksterne informationskilder omkring sårbarheder. Herudover foretages der ekstern penetrationstest hvert andet år.

A.13: Kommunikationssikkerhed

Netværkssikkerhed
Der benyttes krypteret netværk til datatrafik via VPN 2-faktor og sundhedsdatanettet.

Firewall
Firewall er restriktivt opsat og forbedres løbende. Firewall indgår også i den eksterne penetrationstest.

Eksterne kommunikationsforbindelser
Der benyttes krypteret netværk til datatrafik.

A.14: Anskaffelse, udvikling og vedligeholdelse

Analyse og specifikation af informationssikkerhedskrav
Der benyttes løbende sårbarheds- og risikovurdering af systemets komponenter og kryptering, Herudover er løbende fokus på forbedring og uddannelse i informationssikkerhed.

Udvikling og vedligeholdelse af systemer
Sentinel systemet udvikles efter ”Privacy by design” og ”Privacy by default” principperne.

Der benyttes versionsstyring af kildekode, som opbevares sikkert hos en danske cloud underleverandør. Kun relevant personale har adgang til kildekoden, databaser mv.

A.15: Leverandørforhold

Underdatabehandleraftale og instruks
Underdatabehandleraftale er indgået, og der er planlagt årligt leverandør tilsyn og deltagelse ved kommende beredskabstest.

A.16: Styring af informationssikkerhedsbrud

Gennem vores beredskabsplan håndteres informationssikkerhedsbrud. Beredskabsplanen testes og forbedres løbende.

A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring

Beredskabsplaner
Vores beredskabsplan beskriver hvordan nød-, beredskabs- og retablering styres og afvikles. Beredskabsplanen testes og forbedres løbende.

A.18: Overensstemmelse

Indgåelse af databehandleraftale med dataansvarlige
Gennem "Privacy by design" sikres det, at intet data udveksles uden forudgående indgået databehandler aftale.

Instruks for behandling af personoplysninger
Gennem "Privacy by design" sikres det, at kun godkendte data udveksles jf. indgået databehandler aftale.

Ulovlige instrukser fra den dataansvarlige
Alle relevante medarbejdere er bekendte med relevant lovgivning, herunder b.la. sundhedslovens § 196 omkring kliniske kvalitetsdatabaser. Dette sikrer den dataansvarlige imod, at ulovlige instrukser bliver udført.

Sletning og tilbagelevering af personoplysninger
Alle relevante medarbejdere kender deres forpligtigelser ift. sletning og tilbagelevering af sundhedsdata, herunder at tilbagelevering af data ikke må foretages i henhold til særlovgivning om statistiske sundhedsdata.

Overførsel af personoplysninger til tredjelande
Intet data overføres til tredjeland.

Afprøvning, vurdering og evaluering
Jf. det løbende risikoarbejde og fokus, sker der løbende afprøvning, vurdering og evaluering af de relevante områder – med henblik på at sikre en løbende forbedring af informationssikkerheden, og minimering af reelle risikoer for den registrerede.

Arbejdet er centeret omkring vurdering og evaluering af Sentinel systemets komponenter ift. sårbarheder, og test og afprøvning af beredskab ved tab af fortrolighed og integritet.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Dataansvarlige har sikkerhedsansvar for de lokale miljøer – f.eks. i forhold til roll-back og adgangsstyring til Sentinel klienten.

Den dataansvarlige er forpligtet til at implementere 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 Sentinel klienten og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen
- Den dataansvarlig styrer brugerrettighederne i Sentinel klienten, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.
- Sentinel klienten, samt lokaleserver med data, er installeret på udstyr, som den dataansvarlige har ansvar for, det er dermed den dataansvarliges ansvar at udføre backup og genetablering i tilfælde af nedbrud.

Dette svarer til den almindelige daglige brug og administration af IT-systemer i den enkelte praksis og er indeholdt i samarbejdet med systemleverandøren

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 Sundhed.dk – Sentinel's beskrivelse af Sentinel samt for udformningen af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

BDO's test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af Sundhed.dk – Sentinel, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 15. november 2023.

Udførte testhandlinger

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

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

For ydelser, som Advania (tidligere Cloudio) leverer indenfor backup, opbevaring og transmission af data for Sundhed.dk – Sentinel, har vi modtaget ISAE 3402 erklæring for perioden fra 1. juni 2022 til 31. maj 2023 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For ydelser, som MedCom leverer, via deres driftsoperatør Netic indenfor transmission af personoplysninger i Sundhedsdatanettet, har vi modtaget ISAE 3000 erklæring for perioden fra 1. januar 2022 til 31. december 2022 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i Sundhed.dk – Sentinel's beskrivelse af Sentinel og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos

Sundhed.dk – Sentinel, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

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

En afvigelse foreligger, når:

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

Risikovurdering

Kontrolmål

- *At sikre, at databehandleren udfører en årlig risikovurdering i forhold til konsekvenserne for de registrerede, der danner grundlag for de tekniske og organisatoriske sikkerhedsforanstaltninger.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af Sentinel systemet 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 proces for risikovurdering og observeret, at Sentinel systemet bliver risikovurderet ud fra risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. Vi har inspiceret trusselkatalog og observeret, at risikovurderingen udarbejdes med udgangspunkt på identificerede trusler. Vi har observeret, at risikoniveau findes ved at gange sandsynlighed med konsekvens, og at der er en proces for opfølgning på risici til vurdering af behov for mitigerende handlinger. Vi har inspiceret risikovurdering og observeret, at denne er opdateret senest september 2023. Vi har endvidere inspiceret årshjulet og observeret, at fremgår, at risikovurderingen skal gennemgås årligt.	Ingen afvigelser konstateret

A.5: Informationssikkerhedspolitikker

Kontrolmål

- *At give retningslinjer for og understøtte informationssikkerheden og behandling af personoplysninger i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter – GDPR artikel 28, stk.1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politikker for informationssikkerhed og databeskyttelse ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Databehandleren har udarbejdet og implementeret en politik, indeholdende en garanti om bistand og forpligtelse til, at opnå overholdelse af relevante krav, love og forskrifter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at denne er opdateret september 2023. Vi har observeret at informationssikkerhedspolitikken kan tilgås af de ansatte via virksomhedens sharepoint. Vi har foretaget inspektion af databehandlerens informationssikkerhedspolitik og observeret, at denne dækker en garanti om bistand og forpligtelse til at overholde relevante krav, love og forskrifter.	Ingen afvigelser konstateret
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens årshjul og observeret, at databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt. Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at den senest er blevet gennemgået og opdateret september 2023.	Ingen afvigelser konstateret

A.6: Organisering af informationssikkerhed

Kontrolmål

- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed og behandling af personoplysninger I organisationen – GDPR artikel 37, stk. 1.*
- *At sikre fjernarbejdspladser og brugen af mobilt udstyr – GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Roller og ansvarsområder ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed. ▶ Alle ansvarsområder for informationssikkerhed og databeskyttelse defineres og fordeles. ▶ Databehandleren har udpeget et kontaktpunkt for dataansvarlig med hensyn til behandling af persondata. ▶ Databehandleren har udpeget en ansvarlig medarbejder for udvikling, implementering, vedligeholdelse og styring af databeskyttelse hos databehandleren. ▶ Databehandleren har et internt team der er ansvarlig for udvikling, implementering, vedligeholdelse og styring af databeskyttelse hos databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at der er etableret ledelsesstyring af informationssikkerhedspolitikken i form af ledelsesgodkendelse. Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at ansvarsområderne for informationssikkerhed og databeskyttelse er defineret og fordelt imellem den enkelte medarbejdere. Vi har foretaget inspektion af sundhedsdatanettet eKvis hjemmeside og observeret, at Sentinel support telefonnummer og e-mail oplysninger fremgår herpå, Som dækker for kontaktpunkt for de dataansvarlige. Vi har observeret, at der blevet udpeget både en ansvarlig medarbejder og et internt team for udvikling, implementering, vedligeholdelse og styring af databeskyttelse hos databehandleren.	Ingen afvigelser konstateret.
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 observeret, at mobile enheder, der anvendes i forbindelse med Sentinel, har opdateret antivirus software installeret. Vi har observeret, at fjernadgang til databehandlerens systemer og data alene kan ske gennemgang en krypteret to-faktor autentificeret VPN-forbindelse.	Ingen afvigelser konstateret

A.7: Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt - GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra b og artikel 37, stk. 1.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar - GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra c.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør - GDPR artikel 28, stk. 3, litra b.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse. ▶ Databehandleren udfører baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for rekruttering, ansættelse, introduktion og fratrædelse og observeret, at denne indeholder proces for rekruttering. Vi er på forespørgsel blevet informeret om, at databehandleren foretager screening og baggrundstjek via samtale med potentielle medarbejder før ansættelse. Vi har udtaget en stikprøve på en nyansat medarbejder og har på forespørgsel fået oplyst, at der er foretaget screening og baggrundstjek.	Ingen afvigelser konstateret
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 observeret, at databehandleren afholder awareness træning for medarbejdere, og vi er blevet informeret om at disse bl.a. omfatter databeskyttelse, herunder reglerne for behandling af dataansvarliges personoplysninger, og informationssikkerhed. Vi har foretaget inspektion af procedure for rekruttering, ansættelse, introduktion og fratrædelse og observeret, at introduktionskursus for nye medarbejdere er en del af introforløbet. Vi har inspiceret dokumentation for awareness-træning for nye medarbejdere og verificeret at træning er blevet afholdt.	Ingen afvigelser konstateret

A.7: Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt – GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra b og artikel 37, stk. 1.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar – GDPR artikel 28, stk. 1, artikel 28, stk. 3, litra c.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør – GDPR artikel 28, stk. 3, litra b.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret databehandlerens årshjul og herfra observeret, at der er opsat regelmæssig træning i databeskyttelse og informationssikkerhed. Vi har yderligere observeret, at træning er afholdt.	
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet ansættelseskontrakt ▶ 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 for en stikprøve observeret, at medarbejderne hos databehandleren har underskrevet en ansættelseskontrakt. Vi har for en stikprøve observeret, at medarbejderne hos, databehandleren har underskrevet en tavshedserklæring. Vi har på forespørgsel blevet informeret om, at der ikke er indgået aftaler med eksterne leverandører/konsulenter i 2023, hvorfor kontrollen om tavshedspligt ved indgåelse af kontrakt ikke kan efterprøves.	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 procedure for rekruttering, ansættelse, introduktion og fratrædelse og observeret, at denne indeholder proces for hvis en medarbejder siger op eller bliver afskediget. Vi er for en stikprøve blevet oplyst, at medarbejderen er orienteret om at tavshedspligt forsat er gældende. Vi har foretaget inspektion af underskrevet tavshedserklæring, som fastsætter at tavshedspligten forsat er gældende efter ansættelses ophør.	Ingen afvigelser konstateret

A.8: Styring af aktiver

Kontrolmål

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf. GDPR artikel 30, stk. 2, artikel 30, stk. 3 og artikel 32, stk. 2.*
- *At sikre passende beskyttelse af information og personoplysninger, der står i forhold til informationens og personoplysningernes betydning for organisationen og de registrerede - GDPR artikel 30, stk. 3 og artikel 30, stk. 4.*
- *At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information og personoplysninger lagret på medier - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret fortegnelse over behandlingsaktiviteter og observeret, at den indeholder de krævede oplysninger. Vi har inspiceret fortegnelsen over behandlingsaktiviteter og observeret, at den opdateres løbende ved væsentlige ændringer og som minimum årligt, senest november 2023.	Ingen afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester - GDPR artikel, 28, stk. 3, litra c.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre uautoriseret adgang til systemer og applikationer - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Logisk adgangssikkerhed, herunder autorisation og adgangskontrol ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitikken og observeret, at der er retningslinjer for tildeling af adgang til relevante data i forhold til Sentinel med arbejdsbetingede behov. Vi har inspiceret at det kræves to-faktor autentifikation for at tilgå systemer med personoplysninger.	Ingen afvigelser konstateret

A.10: Kryptografi

Kontrolmål

- *At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers og personoplysningers fortrolighed, autenticitet og/eller integritet - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik for anvendelse af kryptografi - Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. Politikken definerer styrken og protokollen for kryptering. - Bærbare medier med personlysninger er krypteret. - Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitikken og observeret, at denne fastsætter at dataudveksling skal krypteres. Vi har inspiceret dokumentation for alt dataudveksling sker krypteret med TLS 1.2. Vi har inspiceret dokumentation for at bærbare medier i form af pc'er er krypteret. Vi har på forespørgsel blevet informeret om, at bærbare medier som udgangspunkt ikke må indeholde personoplysninger, men i særtilfælde må personoplysninger hentes ned på krypterede enheder, men slettes så snart formålet er opfyldt. Vi har inspiceret dokumentation for at data er krypteret i form af VPN. Vi har observeret, at der bliver brugt specifikke krypterings standarter for at sikre fortrolighed og integritet af data.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og personoplysninger, herunder informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang. ▶ Alle adgange registreres og logges.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren anvender låsebrik for at få fysiske adgang til kontorer med formål at forbygge sandsynligheden for uautoriseret adgang. Vi har for udtaget stikprøve observeret log af adgange til kontorlokaler registreres med dato, klokkeslæt, sted og medarbejdere. Vi har inspiceret Advania Danmark A/S' ISAE 3402 erklæring dækkende for perioden 1. juni 2022 til 31. maj 2023 og observeret, at denne ikke indeholder nogle afvigelser. Som hoster Sentinel's servere.	Ingen afvigelser konstateret
Fysisk sikkerhed ▶ Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. Den fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav. ▶ Databehandleren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret Advania Danmark A/S' ISAE 3402 erklæring dækkende for perioden 1. juni 2022 til 31. maj 2023 og observeret, at denne ikke indeholder nogle afvigelser.	Ingen afvigelser konstateret

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter - GDPR artikel 25 og artikel 28, stk. 3, litra c.*
- *At sikre, at information og personoplysninger, herunder informations- og databehandlingsfaciliteter er beskyttet mod malware - GDPR artikel 28, stk. 3, litra c.*
- *At beskytte mod tab af data - GDPR artikel 28, stk. 3, litra c.*
- *At registrere hændelser og tilvejebringe bevis - GDPR artikel 33, stk. 2.*
- *At sikre integriteten af driftssystemer - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre, at tekniske sårbarheder udnyttes - GDPR artikel 28, stk. 3, litra c.*
- *At minimere virkningen af auditaktiviteter på driftssystemer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Vedligeholdelse af systemsoftware ▶ 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 databehandlerens informationssikkerhedspolitik og observeret, at patching sker efter behov. Vi er på forespørgsel blevet informeret om, at en tilbagevendende manuel opgave sikrer, at systemsoftware opdateres regelmæssigt. Vi har inspiceret, at systemsoftwaren er opdateret.	Ingen afvigelser konstateret
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateret med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitikken og observeret, at denne fastsætter at antivirus bliver opdateret løbende. Vi har for en stikprøve observeret, at der er installeret opdateret antivirus-software på databehandlerens arbejdsstationer og servere. Vi har observeret, at antivirus-software er sat til automatisk opdatering.	Ingen afvigelser konstateret

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter - GDPR artikel 25 og artikel 28, stk. 3, litra c.*
- *At sikre, at information og personoplysninger, herunder informations- og databehandlingsfaciliteter er beskyttet mod malware - GDPR artikel 28, stk. 3, litra c.*
- *At beskytte mod tab af data - GDPR artikel 28, stk. 3, litra c.*
- *At registrere hændelser og tilvejebringe bevis - GDPR artikel 33, stk. 2.*
- *At sikre integriteten af driftssystemer - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre, at tekniske sårbarheder udnyttes - GDPR artikel 28, stk. 3, litra c.*
- *At minimere virkningen af auditaktiviteter på driftssystemer - GDPR artikel 28, stk. 1.*

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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitikken og observeret, at denne fastsætter at der skal udføres daglig backup af databehandlerens systemer og data. Vi har inspiceret aftale med underdatabehandler og observeret, at drift og opbevaring af backup er outsourcet til databehandlerens underdatabehandler. Vi har inspiceret underdatabehandlers ISAE 3402 erklæring dækkende for perioden 1. juni 2022 til 31. maj 2023 og observeret, at denne ikke indeholder nogle afvigelser.	Ingen afvigelser konstateret
Logning og overvågning ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har for en stikprøve observeret, at der føres log over succesfulde og mislykkedes adgangsforsøg til databehandlerens systemer og data. Vi har observeret, at der føres log over brugerændringer i systemer og databaser.	Ingen afvigelser konstateret

A.12: Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informations- og databehandlingsfaciliteter - GDPR artikel 25 og artikel 28, stk. 3, litra c.*
- *At sikre, at information og personoplysninger, herunder informations- og databehandlingsfaciliteter er beskyttet mod malware - GDPR artikel 28, stk. 3, litra c.*
- *At beskytte mod tab af data - GDPR artikel 28, stk. 3, litra c.*
- *At registrere hændelser og tilvejebringe bevis - GDPR artikel 33, stk. 2.*
- *At sikre integriteten af driftssystemer - GDPR artikel 28, stk. 3, litra c.*
- *At forhindre, at tekniske sårbarheder udnyttes - GDPR artikel 28, stk. 3, litra c.*
- *At minimere virkningen af auditaktiviteter på driftssystemer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sårbarhedsscanning og penetrationstests ▶ Hvert andet år foretages der en penetrationstest af databehandlerens netværk. Resultatet dokumenteres i en rapport. ▶ Databehandleren gennemgår rapporten og følger op på konstateret svagheder. ▶ Databehandler håndtere/mitigere eventuelle sårbarheder ud fra en risikovurdering. ▶ Databehandler har dokumenteret deres håndtering/mitigering af fundne sårbarheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret den senest udførte penetrationstestrapport af oktober 2023. Vi har inspiceret penetrationstestrapporten og observeret, at databehandleren følger op på de konstaterede svagheder. Vi har inspiceret risikoanalysen og observeret, at databehandleren har et system, hvori håndtering/mitigering af fundne sårbarheder dokumenteres.	Ingen afvigelser konstateret

A.13: Kommunikationssikkerhed

Kontrolmål

- *At sikre beskyttelse af informationer og personoplysninger i netværk og af understøttende informationsbehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*
- *At opretholde informationssikkerhed og databeskyttelse ved overførsel internt i en organisation og til en ekstern entitet - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Netværkssikkerhed ▶ Netværks topologien er struktureret efter best-practice principper, hvilket betyder at servere som driver applikationer ikke kan nås direkte fra internettet. ▶ Databehandlers netværk er segmenteret så interne services/servere ikke kan kommunikere direkte med internettet. ▶ Databehandleren anvender kendte netværksteknologier og mekanismer for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret netværks topologi og observeret, at det er struktureret således at databehandlerens server ikke kan nås direkte fra internettet. Vi har observeret, at databehandlerens netværk er segmenteret således at interne services/servere ikke kan kommunikere direkte med internettet. Vi har observeret, at databehandleren har gjort brugt af kendt netværksteknologi og mekanismer for at beskytte det interne netværk.	Ingen afvigelser konstateret
Informationsoverførelse ▶ Ekstern adgang 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 observeret, at fjernadgang til databehandlerens systemer og data alene kan ske gennemgang en krypteret to-faktor autentificeret VPN-og firewall. Vi har observeret, at eksterne kommunikationsforbindelser er krypteret. Vi har foretaget inspektion af ISAE3000 og 3402 erklæring for Netic og observeret, at den er uden forbehold. Vi er blevet informeret om at den eneste eksterne kommunikationsforbindelse, der må tilgå databehandlerens netværk, er Sundhedsdatanettet.	Ingen afvigelser konstateret.

A.14: Anskaffelse, udvikling og vedligeholdelse

Kontrolmål

- *At sikre, at informationssikkerhed og databeskyttelse er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk - GDPR artikel 25.*
- *At sikre, at informationssikkerhed og databeskyttelse tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus - GDPR artikel 25.*
- *At sikre beskyttelse af data, som anvendes til test - GDPR artikel 25.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Udvikling og vedligeholdelse af systemer ▶ Databehandleren arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelses opgaver. ▶ 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 dokumentation for, at privacy-by-design principper bliver brugt i henhold til det enkelte projekt, herunder hvordan information skal præsenteres for brugere af systemet. Vi er på forespørgsel blevet informeret, at ændringer til Sentinel systemet bliver testet i et testmiljø før det bliver sat i produktion.	Ingen afvigelser konstateret.
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. ▶ Bruger oprettelse sker som udgangspunkt med laveste brugerrettighedsniveau. ▶ Kun databehandlerens udviklere har adgang til kildekode.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren følger security-by-design princippet. Vi har observeret at Sentinels kildekode er versionsstyret og er blevet informeret om at et Roll-back ville kunne udføres såfremt en fejl skulle forekomme. Vi er på forespørgsel blevet informeret om, at brugeroprettelser sker med laveste brugerrettighedsniveau. Vi har inspiceret at Sundhed.dk – sentinel's brugere med adgang til sentinel løsningen alene har de adgange som er nødvendige i forbindelse med arbejdsmæssigt behov. Vi har observeret at kun databehandlerens udviklere kan tilgå kildekoden.	Ingen afvigelser konstateret.

A.14: Anskaffelse, udvikling og vedligeholdelse

Kontrolmål

- *At sikre, at informationssikkerhed og databeskyttelse er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk - GDPR artikel 25.*
- *At sikre, at informationssikkerhed og databeskyttelse tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus - GDPR artikel 25.*
- *At sikre beskyttelse af data, som anvendes til test - GDPR artikel 25.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at der er indført funktionsadskille mellem udvikling og drift i forbindelse med medarbejderes adgang. Vi er på forespørgsel blevet informeret, at ændringer til Sentinel systemet bliver testet i et testmiljø før det bliver sat i produktion. Vi har inspiceret en netværkstopologi over infrastrukturen, og observeret, at udviklings- og testmiljø er adskilt fra produktion. Vi har inspiceret, at testdata er anonymiseret. Vi har observeret, at et versionsstyringssystem som registrerer alle ændringer i kildekoden anvendes.	Ingen afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

- *At sikre beskyttelse af organisationens aktiver og personoplysninger, som leverandører har adgang til - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*
- *At opretholde et aftalt niveau af informationssikkerhed, databeskyttelse og levering af ydelser i henhold til leverandøraftalerne - GDPR artikel 28, stk. 2, artikel 28, stk. 3, litra d og artikel 28, stk. 4.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandlers indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at underdatabehandleraftaler indgås ved anvendelse af underdatabehandlere og at forpligtelser, som databehandleren er blevet pålagt, videregives. Vi har for en stikprøve inspiceret indgået underdatabehandleraftale og observeret, at denne videregiver instrukser fra dataansvarlige til underdatabehandleren. Vi har observeret, at de indgåede underdatabehandleraftaler opbevares elektronisk. Vi har inspiceret skabelon for indgåede af databehandleraftale og observeret, at databehandleraftalen med anvendt underdatabehandler indeholder information om dennes potentielle brug af underdatabehandlere.	Ingen afvigelser konstateret.

A.16: Styring af informationssikkerhedsbrud

Kontrolmål

- *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud og brud på persondatasikkerheden, herunder kommunikation om sikkerhedshændelser og -svagheder - GDPR artikel 33, stk. 2.*

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 en stikprøve af indgået databehandleraftaler og observeret, at databehandler heri forpligter sig til uden unødig forsinkelse at underrette den dataansvarlige om sikkerhedsbrud. Vi har inspiceret beredskabsplanen og observeret, at denne indeholder en procedure for håndtering af brud på persondatasikkerheden, hvorfra det fremgår at dataansvarlige parter skal orienteres om persondatasikkerheds brud uden unødvendig forsinkelse. Vi er på forespørgsel blevet informeret om, at der ikke har været persondatasikkerhedsbrud i 2023, hvorfor procedurer og kontroller i forbindelse med brud på persondatasikkerhed ikke kan efterprøves.	Ingen afvigelser konstateret

A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring

Kontrolmål

- *Informationssikkerheds- og databeskyttelseskontinuiteten skal være forankret I organisationens ledelsessystemer for nød-, beredskabs- og retableringsstyring - GDPR artikel 28, stk. 3, litra c.*
- *At sikre tilgængelighed af informations- og databehandlingsfaciliteter - GDPR artikel 28, stk. 3, litra c.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
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, beredskabsplanerne er tidssvarende og effektive i kritiske situationer. ▶ Beredskabstest dokumenteres og evalueres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beredskabsplanen og observeret, at en Recovery Time Objective (RTO), og den maksimalt acceptable tidsperiode for datatab før aktivering af beredskab, betegnet Recovery Point Objective (RPO), er blevet defineret. Vi har observeret, at beredskabsplanen definerer, at der skal foretages en årlig test af beredskabsplanen. Vi har observeret, at test af beredskabsplanen foretaget i september 2023 er blevet dokumenteret og evalueret.	Ingen afvigelser konstateret

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

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 observeret, at databehandleren har sat et system op for at sikre at en databehandleraftale altid indgås med dataansvarlige parter gennem eKvis, på bais af databehandlerens standard databehandleraftale. Vi har inspiceret databehandler skabelon for indgåelse af databehandler aftaler og observeret, at den dækker relevante områder. Vi har for en stikprøve udpeget databehandleraftale observeret, at den er i overensstemmelse med de ydelser databehandleren leverer. Vi har observeret, at indgåede databehandleraftaler underskrives og opbevares elektronisk. Vi har observeret, at databehandlerens standarddatabehandleraftale indeholder information om brugen af underdatabehandler, men ved forespørgsel blevet informeret om at de opdaterede skabeloner ikke er taget i brug endnu.	Vi har konstateret at nyeste skabeloner ikke er taget i anvendelse og observeret, at information om brugen af underdatabehandler MedCom, således ikke er kommunikeret til dataansvarlige via databehandleraftalerne. Ingen yderligere 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 observeret, at databehandlerens standarddatabehandleraftale og den stikprøve udvalgte indgåede databehandleraftale indeholder instrukser fra den dataansvarlige part.	Ingen afvigelser konstateret

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret processen for hvordan det sikres at databehandler kun behandler personoplysninger, som dataansvarlig har givet tilladelse til via deres "projekt tilmeldings bank". Vi er ved forespørgsel blevet informeret om, at der ikke har været projekter med persondata i nyere tid, hvorfor vi ikke har kunne efterprøve processen.	
Ulovlige instrukser fra den dataansvarlige ▶ 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 på forespørgsel blevet informeret om, at alle relevante ansatte er orienteret om, hvordan underretning af den dataansvarlige skal ske, hvis en ulovlig instruks modtages. Vi er på forespørgsel blevet informeret om, at der ingen ulovlige instrukser er modtaget, hvorfor procedure og kontrol heraf ikke kan efterprøves.	Ingen afvigelser konstateret
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret en stikprøve udvalgt databehandleraftale og observeret, at denne definerer, hvordan sletning af personoplysninger må ske, herunder at det kun må foretages efter overdragelse til ny databehandler. Vi er på forespørgsel blevet informeret om, at ingen databehandleraftaler er ophørt i 2023, hvorfor proceduren ikke kan efterprøves.	Ingen afvigelser konstateret

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Overførsel af personoplysninger til tredjelande ▶ Der foreligger skriftlige procedurer for overførsel af personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. ▶ Databehandlerens procedure gennemgås og vurderes løbende, og som minimum en gang årligt, om proceduren skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi er på forespørgsel blevet informeret om, at persondata ikke overføres til tredjelande.	Ingen afvigelser konstateret
Udpegelse af databeskyttelsesrådgiveren ▶ Databehandleren har udpeget en databeskyttelsesrådgiver.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret Sundhed.dk – Sentinels stillingtagelse til om de skal have en DPO og observeret, at de har vurderet, at de skal have en DPO og at de har udpeget en sådan.	Ingen afvigelser konstateret
Databeskyttelsesrådgiverens stilling ▶ Databehandleren har udarbejdet og implementeret en beskrivelse af databeskyttelsesrådgiverens stilling. ▶ Databehandleren inddrager databeskyttelsesrådgiveren vedrørende beskyttelse af personoplysninger. ▶ Databeskyttelsesrådgiveren rapporterer direkte til databehandlerens ledelse. ▶ Databeskyttelsesrådgiveren er underlagt tavshedspligt/fortrolighed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret Sundhed,dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret, at der heraf fremgår en beskrivelse af DPO'ens stilling. Vi har inspiceret Sundhed,dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret, at det heraf fremgår at DPO'en skal inddrages i sager vedrørende beskyttelse af personoplysninger.	Ingen afvigelser konstateret

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret Sundhed,dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret, at det heraf fremgår at DPO'en rapportere direkte til ledelsen. Vi har inspiceret dokumentation på at DPO'en skal være underlagt tavshedspligt og observeret at DPO er underlagt tavshedspligt.	
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 Sundhed,dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og vi har inspiceret dokumentation for at databeskyttelsesrådgiven udfører de opgaver DPO'en er pålagt. Vi har inspiceret Sundhed,dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret at det er defineret i hvilke situationer DPO ikke må inddrages, idet det vil medfører at DPO vil komme i konflikt med de opgaver DPO'en udfører.	Ingen afvigelser konstateret
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurdere og evaluerer effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. De data som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at virksomheden regelmæssigt fører kontrol med sine organisatoriske sikkerhedsforanstaltninger for at vurdere om disse fungerer effektivt.	Ingen afvigelser konstateret

A.18: Overensstemmelse

Kontrolmål

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav - GDPR artikel 25, artikel 28, stk. 2, artikel 28, stk. 3, litra a, artikel 28, stk. 3, litra e, artikel 28, stk. 3, litra g, artikel 28, stk. 3, litra h, artikel 28, stk. 3, litra f, artikel 28, stk. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.*
- *At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives I overensstemmelse med organisationens politikker og procedurer - GDPR artikel 28, stk. 1.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har yderligere observeret, at databehandleren hvert andet år udfører en penetrationstest for, at evaluerer effektiviteten af dens tekniske sikkerhedsforanstaltninger, senest 2023.	

5. SUPPLERENDE INFORMATION FRA SUNDHED.DK - SENTINEL

Nedenstående supplerende information har ikke været genstand for den revision, der udføres af BDO.

På baggrund af BDO's konstaterede afvigelser i ISAE 3000-erklæringen har Sundhed.dk - Sentinel følgende supplerende information:

Handlingsplan		
Kontrolaktivitet	**Resultat af test**	**Supplerende information**
Indgåelse af databehandleraftale med den dataansvarlige	Vi har konstateret at nyeste skabeloner ikke er taget i anvendelse og observeret, at information om brugen af underdatabehandler MedCom, således ikke er kommunikeret til dataansvarlige via databehandleraftalerne.	I forhold til de gamle databehandler aftaler, har vi kontaktet eKVIS/FAPS i forhold til at underdatabehandler MedCom skulle med på listen over underdatabehandlere. eKVIS/FAPS valgt på vegne af speciallægerne, at vente med at lave ændringen til den planlagte opdatering af databehandleraftalerne i forbindelse med aflevering af data til sundhedsjournalen.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 80

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."

Claus Duedal Pedersen
Enhedschef, Sentinelenheden
På vegne af: Sundhed.dk - Sentinel
Serienummer: c65c5788-d060-431b-8318-a4c22b78ebaa
IP: 193.228.xxx.xxx
2024-03-04 14:17:09 UTC

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: 37.96.xxx.xxx
2024-03-04 14:30:33 UTC

Nicolai Tobias Visti Pedersen
Partner, statsautoriseret revisor
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-03-04 14:33:57 UTC