

**AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING
MED SIKKERHED PR. 16. DECEMBER 2025 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 DATA-
BESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLØ-
VEN**

Sundhed.dk

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING	2
2. SUNDHED.DK'S UDTALELSE	4
3. SUNDHED.DK'S BESKRIVELSE AF SENTINEL	6
Sundhed.dk	6
Styring af persondatasikkerhed.....	8
Risikovurdering.....	9
Tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller	9
Komplementerende kontroller hos de dataansvarlige	12
4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST	14
Risikovurdering.....	16
A.5: Informationssikkerhedspolitikker.....	17
A.6: Organisering af informationssikkerhed.....	19
A.7: Personalesikkerhed	21
A.8: Styring af aktiver	23
A.9: Adgangsstyring.....	24
A.10: Kryptografi	25
A.11: Fysisk sikring og miljøsikring	26
A.12: Driftssikkerhed	27
A.13: Kommunikationssikkerhed.....	30
A.14: Anskaffelse, udvikling og vedligeholdelse	32
A.15: Leverandørforhold.....	34
A.16: Styring af informationssikkerhedsbrud.....	36
A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring	37
A.18: Overensstemmelse	38

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 16. DECEMBER 2025 OM BESKRIVELSE 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 – Sentinel's kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Sundhed.dk (databehandleren) pr. 16. december 2025 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 pr. 16. december 2025.

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 revisors 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 revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringsystem, 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 beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 16. december 2025, 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. 16. december.

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 16. februar 2026

BDO Statsautoriseret revisionspartnerselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. SUNDHED.DK'S UDTALELSE

Sundhed.dk 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, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt. Beskrivelsen skal ses i sammenhæng med de sikkerhedsforanstaltninger og kontroller som de dataansvarlige har ansvar for: Komplementerende kontroller hos de dataansvarlige inkl. Lægepraksissystemer.

Sundhed.dk anvender underdatabehandlere. Disse underdatabehandlers relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Sundhed.dk 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. 16. december 2025. 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 med henvisning til afgrænsningen af Sentinel har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.

- De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.
2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af 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 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. 16. december 2025.

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

Odense, den 16. februar 2026

Sundhed.dk - Sentinel

Øzlem Polat
Enhedschef, Sentinel-teamet

3. SUNDHED.DK'S BESKRIVELSE AF SENTINEL

SUNDHED.DK

Sentinel-teamet er et team under Sundhed.dk, og teamets kerneopgave er udvikling, drift og support af selve Sentinel programmet.

Sentinel kan anvendes på to måder:

1. **Installeret klientløsning**

Sentinel 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 at opsamle de journaldata, som kunden giver tilladelse til, med henblik på behandling i Sundhed.dk databanken i Sentinel-teamet.

2. **Webbaseret løsning**

For udvalgte faggrupper (fx kiropraktorer og fysioterapeuter) tilbydes en webbaseret Sentinel-løsning. Denne løsning kræver ingen lokal installation hos kunden. I stedet kommunikerer praksissystemet via webkald med en Sentinel-lokalserver, som er hostet centralt hos Sundhed.dk. Herfra behandles data på samme måde som i klientløsningen, dvs. at de journaldata, kunden har givet tilladelse til, sendes til Sundhed.dk databanken i Sentinel-teamet.

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 patienthenførbare 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

- ICPC- koder
- Medicin
- Labsvar
- Henvisninger
- Notat
- Epikriser

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

For fysioterapeutområdet gælder det tilsvarende, at der – ud over de samme data som for speciallæger – indsamles Ydelseskoder.

Sundhed.dk, Sentinel-teametagerer 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 data-behandler 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 data-behandleraftale

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 KviKs hjemmeside om Sentinel.

Sentinelns 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 sundhedsvæsenet 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-teamet 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	KONTOLOMRÅDE	ARTIKEL
Risikovurdering	<ul style="list-style-type: none"> Risikovurdering 	<ul style="list-style-type: none"> Artikel 28, stk. 3, litra c
A.5: Informationssikkerhedspolitikker	<ul style="list-style-type: none"> Informationssikkerhedspolitik Gennemgang af informationssikkerhedspolitik 	<ul style="list-style-type: none"> Artikel 28, stk. 1
A.6: Organisering af informationssikkerhed	<ul style="list-style-type: none"> Roller og ansvarsområder Fjernarbejdspladser og fjernadgang til systemer og data 	<ul style="list-style-type: none"> Artikel 28, stk. 1 Artikel 28, stk. 3, litra c
A.7: Personalesikkerhed	<ul style="list-style-type: none"> Rekruttering af medarbejdere Uddannelse og awareness af medarbejdere Tavsheds- og fortrolighedsaftale med medarbejdere Fratrædelse af medarbejdere 	<ul style="list-style-type: none"> Artikel 28, stk. 1 Artikel 28, stk. 3, litra b
A.8: Styring af aktiver	<ul style="list-style-type: none"> Fortegnelse over kategorier af behandlingsaktiviteter 	<ul style="list-style-type: none"> Artikel 30, stk. 2, 3 og 4
A.9: Adgangsstyring	<ul style="list-style-type: none"> Logisk adgangssikkerhed, herunder autorisation og adgangskontrol 	<ul style="list-style-type: none"> Artikel 28, stk. 3, litra c
A.10: Kryptografi	<ul style="list-style-type: none"> Kryptering af personoplysninger 	<ul style="list-style-type: none"> Artikel 28, stk. 3, litra c
A.11: Fysisk sikring og miljøsikring	<ul style="list-style-type: none"> Fysisk adgangskontrol Fysisk sikkerhed 	<ul style="list-style-type: none"> Artikel 28, stk. 3, litra c
A.12: Driftssikkerhed	<ul style="list-style-type: none"> Vedligeholdelse af systemsoftware Antivirusprogram BackupLogning og overvågning Sårbarhedsscanning og penetrationstests 	<ul style="list-style-type: none"> Artikel 28, stk. 3, litra c
A.13: Kommunikationssikkerhed	<ul style="list-style-type: none"> Styring af netværkssikkerhed Informationsoverførsel 	<ul style="list-style-type: none"> Artikel 28, stk. 3, litra c

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
A.14: Anskaffelse, udvikling og vedligeholdelse	<ul style="list-style-type: none"> • Udvikling og vedligeholdelse af systemer • Informationssikkerhed i ændring og udvikling • Adskillelse af udviklings-, test- og produktionsmiljø 	<ul style="list-style-type: none"> • Artikel 25
A.15: Leverandørforhold	<ul style="list-style-type: none"> • Underdatabehandleraftale og instruks • Ændringer i godkendte underdatabehandlere • Tilsyn med underdatabehandlere 	<ul style="list-style-type: none"> • Artikel 28, stk. 2 og 4
A.16: Styring af informationssikkerhedsbrud	<ul style="list-style-type: none"> • Underretning om brud på persondatasikkerheden • Bistand til den dataansvarlige ved brud på persondatasikkerhed 	<ul style="list-style-type: none"> • Artikel 33, stk. 2
A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring	<ul style="list-style-type: none"> • Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse 	<ul style="list-style-type: none"> • Artikel 28, stk. 3, litra c
A.18: Overensstemmelse	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 kompromitere 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 politikker 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 fungerer tre af IT-specialisterne som henholdsvis informationssikkerhedskoordinator, systemsikkerhedsejer og datasikkerhedsejer.

Sentinel-teamet benytter 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-teamet. Da Sentinel-teamet 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 omgang med persondata.

A.8: Styring af aktiver

Fortegnelse over kategorier af behandlingsaktiviteter

Sentinel-teamet har jf. aftale med dataansvarlige overblik, databehandlaftale og underdatabehandlaftale overblik herover. Der er udarbejdet fortegnelser over behandlingsaktiviteter for at understøtte vores forpligtelse 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-teamet, 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 reetablering 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 med henblik 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

Underdatabehandlereftale 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 risikoen 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'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, 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. 16. december 2025.

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 gennemlæst med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udførte, 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 itm8 leverer inden for backup, opbevaring og transmission af data for Sundhed.dk – Sentinel, har vi modtaget ISAE 3402 erklæring for perioden fra 1. januar 2024 til 31. december 2024 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For ydelser, som MedCom leverer via deres driftoperatør Netic inden for transmission af personoplysninger i Sundhedsdatanettet, har vi modtaget ISAE 3000 erklæring for perioden fra 1. januar 2024 til 31. december 2024 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For ydelser, som Region Nordjylland leverer inden for opbevaring og behandling af personoplysninger, har vi ikke modtaget tilsynsmateriale, da der ikke er foretaget endeligt tilsyn.

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 ► <i>At sikre, at databehandleren udfører en årlig risikovurdering i forhold til konsekvenserne for de registrerede, der danner grundlag for de tekniske og organisatoriske sikkerhedsforanstaltninger.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering <ul style="list-style-type: none"> ► 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>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.</p> <p>Vi har inspiceret trusselkatalog og observeret, at risikovurderingen udarbejdes med udgangspunkt på identificerede trusler.</p> <p>Vi har observeret, at risici findes og minimeres ved stillingtagen til sandsynlighed og konsekvens.</p> <p>Vi har inspiceret risikovurdering og observeret, at denne er opdateret i september 2025. Vi har endvidere inspiceret årshjulet og observeret, at det fremgår, at risikovurderingen skal gennemgås årligt.</p>	<p>Ingen afvigelser konstateret</p>

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 <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at denne senest er opdateret i november 2025.</p> <p>Vi har inspiceret databehandlerens supplerende retningslinjedokument og observeret, at denne er godkendt i 1. december 2025.</p> <p>Vi har observeret at databehandlerens generelle informationssikkerhedspolitik kan tilgås af de ansatte via virksomhedens Share-Point.</p> <p>Vi har foretaget inspektion af skabeloner for databehandleraftaler og observeret, at databehandleren skal bistå med overholdelse af forpligtelser og krav over for dataansvarlig.</p> <p>Vi har inspiceret indgåede databehandleraftaler og observeret, at disse følger skabelonen for databehandleraftaler.</p>	Ingen afvigelser konstateret
Gennemgang af informationssikkerhedspolitik <ul style="list-style-type: none"> ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens informationssikkerhedspolitik og observeret, at den senest er blevet gennemgået og opdateret i november 2025.</p> <p>Vi har inspiceret databehandlerens supplerende retningslinjedokument og observeret, at denne er godkendt i 1. december 2025.</p>	Ingen afvigelser konstateret

A.5: Informationssikkerhedspolitikker		
Kontrolmål ▶ <i>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.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret databehandlerens årshjul og observeret, at databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum én gang årligt.	

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
<p>Roller og ansvarsområder</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens informationssikkerhedspolitikker og observeret, at der er etableret ledelsesstyring af informationssikkerhedspolitikken i form af ledelsesgodkendelse.</p> <p>Vi har inspiceret databehandlerens informationssikkerhedspolitikker og observeret, at ansvarsområderne for informationssikkerhed og databeskyttelse er defineret og fordelt.</p> <p>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.</p> <p>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.</p> <p>Vi har inspiceret referat fra informationssikkerhedsmøde og observeret, at det senest er afholdt i september 2025.</p>	<p>Ingen afvigelser konstateret.</p>
<p>Fjernarbejdspladser og fjernadgang til systemer og data</p> <ul style="list-style-type: none"> ▶ 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 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har observeret, at mobile enheder, der anvendes i forbindelse med Sentinel, har opdateret antivirus software installeret.</p>	<p>Ingen afvigelser konstateret</p>

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
	Vi har observeret, at fjernadgang til databehandlerens systemer og data alene kan ske gennem en krypteret to-faktor autentificeret VPN-forbindelse.	

A.7: Personalesikkerhed		
<p>Kontrolmål</p> <ul style="list-style-type: none"> ▶ <i>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.</i> ▶ <i>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.</i> ▶ <i>At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør – GDPR-artikel 28, stk. 3, litra b.</i> 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Rekruttering af medarbejdere</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret procedure for rekruttering, ansættelse, introduktion og fratrædelse og observeret, at denne indeholder proces for rekruttering.</p> <p>Vi er på forespørgsel blevet informeret om, at databehandleren foretager screening og baggrundstjek via samtale med potentielle medarbejder før ansættelse.</p> <p>Vi har stikprøvevist inspiceret dokumentation for, at databehandleren udfører screening af medarbejdere før ansættelse.</p>	<p>Ingen afvigelser konstateret</p>
<p>Uddannelse og instruktion af medarbejdere, der behandler personoplysninger</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>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.</p> <p>Vi har foretaget inspektion af procedure for onboarding og observeret, at nye medarbejdere skal deltage i møder vedrørende orientering om GDPR.</p> <p>Vi har inspiceret awareness-værktøj og observeret, at der bliver afholdt løbende træning.</p>	<p>Ingen afvigelser konstateret</p>

A.7: Personalesikkerhed		
Kontrolmål ▶ At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tildelt – 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
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 foretaget inspektion af informationssikkerhedspolitikker og observeret, at der står beskrevet at nye medarbejder som skal arbejde med personfølsomme data, skal være underlagt en tavshedserklæring. Vi har inspiceret skabelon for underskrivelse af tavshedserklæring og observeret, at medarbejdere orienteres om stadig gældende tavshedspligt efter ansættelsens ophør. Vi har inspiceret tavsheds- og fortrolighedsaftale for seneste ansættelse og observeret, at denne er underskrevet af pågældende medarbejder. Vi har på forespørgsel fået oplyst, at der ikke anvendt eksterne med adgang til persondata.	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 har på forespørgsel fået oplyst, at der ikke har været fratrædelser af medarbejdere med adgang til persondata. Vi har derfor ikke testet kontrollens implementering.	Vi har konstateret, at der ikke har været fratrædelser siden sidste revision. Vi har derfor ikke testet kontrollens implementering. 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 <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret fortegnelse over behandlingsaktiviteter og observeret, at den indeholder de krævede oplysninger udover at én underdatabehandler ikke fremgår af fortegnelsen.</p> <p>Vi har inspiceret fortegnelsen over behandlingsaktiviteter og observeret, at den opdateres løbende ved væsentlige ændringer og som minimum årligt, senest august 2025.</p> <p>Vi har inspiceret databehandlerens årshjul og observeret, at der løbende sker opdatering af fortegnelsen.</p>	<p>Vi har konstateret, at Region Nordjylland ikke fremgår som underdatabehandlere i fortegnelsen over behandlingsaktiviteter.</p> <p>Ingen yderligere afvigelser konstateret.</p>

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
<p>Logisk adgangssikkerhed, herunder autorisation og adgangskontrol</p> <ul style="list-style-type: none"> ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret retningslinjer for tildeling af adgang til relevante data i forhold til Sentinel med arbejdsbetingede behov.</p> <p>Vi har inspiceret dokumentation for, at der kræves to-faktor autentifikation for at tilgå systemer med personoplysninger.</p>	<p>Ingen afvigelser konstateret</p>

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
<p>Politik for anvendelse af kryptografi</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens retningslinjer for informationsikkerhed og observeret, at denne fastsætter at dataudveksling skal krypteres. Vi har inspiceret dokumentation for alt dataudveksling sker krypteret med TLS.</p> <p>Vi er på forespørgsel blevet informeret om, at bærbare medier ikke må indeholde personoplysninger.</p> <p>Vi har inspiceret dokumentation for at data er krypteret i form af VPN. Vi har observeret, at der bliver brugt specifikke krypteringsstandarder for at sikre fortrolighed og integritet af data.</p> <p>Vi er på forespørgsel blevet oplyst om, at der ikke bliver sendt e-mails indeholdende personoplysninger.</p>	<p>Ingen afvigelser konstateret.</p>

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 databehandlers 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 fysisk adgang til kontorer med det formål at forebygge sandsynligheden for uautoriseret adgang. Vi har inspiceret udtræk over log fra låsesystemet og observeret, at dato, klokkeslæt, sted og medarbejdere registreres når kontoret tilgås. Vi har på forespørgsel fået oplyst, at servere opbevares hos fysisk hos itm8. Vi har inspiceret itm8 ISAE 3402 dækkende for perioden 1. januar 2024 til 31. december 2025 og observeret, at denne ikke indeholder afvigelser.	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 på forespørgsel fået oplyst, at servere opbevares hos fysisk hos itm8. Vi har inspiceret itm8 ISAE 3402 dækkende for perioden 1. januar 2024 til 31. december 2024 og observeret, at denne ikke indeholder 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 <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens retningslinjer for informationsikkerhed og observeret, at patching sker efter behov.</p> <p>Vi har stikprøvevist inspiceret, at arbejdsstationer er opdateret med operativsystem-software.</p> <p>Vi har inspiceret serveroversigt og observeret, at relevante servere er opdateret.</p>	Ingen afvigelser konstateret
Antivirusprogram <ul style="list-style-type: none"> ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateret med seneste version. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens informationssikkerhedspolitikker og observeret, at denne fastsætter at antivirus bliver opdateret løbende.</p> <p>Vi har stikprøvevist observeret, at der er installeret opdateret antivirus-software på databehandlerens arbejdsstationer og servere.</p>	Ingen afvigelser konstateret
Sikkerhedskopiering og reetablering af data <ul style="list-style-type: none"> ▶ Der foretages dagligt backup af systemer og data. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p>	Ingen afvigelser konstateret

A.12: Driftssikkerhed		
Kontrolmål <ul style="list-style-type: none"> ▶ 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
<ul style="list-style-type: none"> ▶ Drift og opbevaring af backup er outsourcet til underdatabehandler. 	<p>Vi har på forespørgsel fået oplyst, at der dagligt foretages backup af systemer og data.</p> <p>Vi har inspiceret udtræk over gennemførte backups og observeret, at der dagligt er foretaget backup.</p> <p>Vi har inspiceret aftale med underdatabehandler og observeret, at drift og opbevaring af backup er outsourcet til databehandlerens underdatabehandler.</p> <p>Vi har inspiceret underdatabehandlers ISAE 3402 erklæring dækkende for perioden 1. januar 2024 til 31. december 2024 og observeret, at denne ikke indeholder nogle afvigelser.</p>	
Logning og overvågning <ul style="list-style-type: none"> ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har for en inspiceret, at der føres log over succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data.</p>	Ingen afvigelser konstateret
Sårbarhedsscanning og penetrationstests <ul style="list-style-type: none"> ▶ Hvert andet år foretages der en penetrationstest af databehandlerens netværk. Resultatet dokumenteres i en rapport. ▶ Databehandleren gennemgår rapporten og følger op på konstaterede svagheder. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret den senest udførte penetrationstestrapport af oktober 2025.</p>	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
<ul style="list-style-type: none"> ▶ Databehandler har dokumenteret deres håndtering/mitigering af fundne sårbarheder. 	<p>Vi har inspiceret, at databehandleren har fået gennemført en penetrationstest, og observeret, at databehandleren følger op på de konstaterede svagheder.</p> <p>Vi har inspiceret dokumentation for seneste sårbarhedsscanning.</p> <p>Vi har på forespørgsel fået oplyst, at håndtering af fundne sårbarheder i sårbarhedsscanningerne løses ad hoc.</p>	

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 <ul style="list-style-type: none"> ▶ Netværkstopologien 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret netværkstopologi og observeret, at det er struktureret således at databehandlers server ikke kan nås direkte fra internettet.</p> <p>Vi har observeret, at databehandlers netværk er segmenteret således at interne services/servere ikke kan kommunikere direkte med internettet.</p> <p>Vi har observeret, at databehandleren anvender kendt netværksteknologi og mekanismer for at beskytte det interne netværk.</p>	Ingen afvigelser konstateret
Informationsoverførsel <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har observeret, at fjernadgang til databehandlers systemer og data alene kan ske gennemgang en krypteret to-faktor autentificeret VPN-og firewall.</p> <p>Vi har inspiceret dokument for beskrivelse af VPN og observeret, at eksterne kommunikationsforbindelser er krypteret.</p> <p>Vi har stikprøvet observeret, at der kræves login med VPN for at tilgå systemer.</p> <p>Vi har foretaget inspektion af ISAE 3000 erklæring for MedCom dækkende perioden 1. januar til 31. december 2024.</p> <p>Vi har observeret, at denne er uden afvigelser.</p>	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
	Vi hr inspiceret udtræk over adgange til udviklingsservere samt log over tilslutninger til VPN hos databehandleren og observeret, at kun personer med et arbejdsbetinget behov har adgang.	

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 <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har en procedure for privacy-by-design principper i udvikling og vedligeholdelses opgaver herunder risikovurdering og test af alle ændringer</p> <p>Vi har på forespørgsel fået oplyst, at databehandleren ikke har implementeret proceduren.</p>	<p>Vi har konstateret, at databehandlerens procedure udvikling og vedligeholdelses opgaver ikke er implementeret, herunder dokumentation for arbejdet med privacy-by-design principper og gennemførelse af risikovurdering af systemændringer.</p> <p>Ingen yderligere afvigelser konstateret.</p>
Informationssikkerhed i udvikling og ændringer <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har en procedure for privacy-by-design principper i udvikling og vedligeholdelses opgaver herunder risikovurdering og test af ændringer</p> <p>Vi har på forespørgsel fået oplyst, at databehandleren ikke har implementeret proceduren.</p> <p>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.</p> <p>Vi har inspiceret, at tildeling af rettigheder sker med laveste mulige brugerrettighedsniveau.</p> <p>Vi har observeret, at kun databehandlerens udviklere kan tilgå kildekoden.</p>	<p>Vi har konstateret, at databehandlerens procedure udvikling og vedligeholdelses opgaver ikke er implementeret, herunder dokumentation for test og godkendelse af ændringer.</p> <p>Ingen yderligere afvigelser konstateret.</p>

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
<p>Adskillelse af udviklings-, test og produktionsmiljø</p> <ul style="list-style-type: none"> ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. ▶ Der benyttes et versionsstyringssystem som registrerer alle ændringer i kildekode. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at udviklings- test- og produktionsmiljøet er logisk adskilt fra hinanden.</p> <p>Vi har inspiceret, at testdata er anonymiseret.</p> <p>Vi har observeret, at et versionsstyringssystem, som registrerer alle ændringer i kildekoden, anvendes.</p>	<p>Ingen afvigelser konstateret.</p>

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 inspiceret indgåede underdatabehandleraftaler og observeret, at disse videregiver instrukser fra dataansvarlige til underdatabehandleren. Vi har observeret, at de indgåede underdatabehandleraftaler opbevares elektronisk. Vi har inspiceret skabelon for databehandleraftaler og observeret, at databehandleraftalen med anvendt underdatabehandler indeholder information om dennes potentielle brug af underdatabehandlere.	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere ▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at ITM8 og Region Nordjylland er taget i brug som nye underdatabehandlere. Vi har på forespørgsel fået oplyst, at databehandleren ikke kan dokumentere, at der er sket underretning til de dataansvarlige i overensstemmelse med de indgået databehandleraftaler. Vi har på forespørgsel fået oplyst, at man har underrettet de dataansvarlige i forhold til ITM8 efter de er taget i brug.	Vi har konstateret, at databehandleren ikke kan dokumentere, at der er sket underretning om ibrugtagning af ITM8 og Region Nordjylland til de dataansvarlige i overensstemmelse med de indgåede databehandleraftaler. Ingen yderligere 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
Tilsyn med underdatabehandlere <ul style="list-style-type: none"> ▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens årshjul og observeret at der udføres årligt tilsyn med underdatabehandlere.</p> <p>Vi har inspiceret ISAE 3000 erklæring for Medcom for perioden 1. januar til 31. december 2024 og observeret, at erklæringen er uden afvigelser.</p> <p>Vi har inspiceret ISAE 3402 erklæringen for itm8 for perioden 1. januar 2024 til 31. december 2024 og observeret, at erklæringen er uden afvigelser.</p> <p>Vi har på forespørgsel fået oplyst, at tilsynet for Region Nordjylland ikke var afsluttet pr. 16. december 2025.</p>	<p>Vi har konstateret, at databehandleren ikke har foretaget tilsyn af Region Nordjylland</p> <p>Ingen yderligere afvigelser konstateret.</p>

A.16: Styring af informationssikkerhedsbrud		
Kontrolmål		
<p>▶ 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.</p>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Underretning om brud på persondatasikkerheden</p> <ul style="list-style-type: none"> ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødigt 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret databehandlerens skabelon for databehandleraf-taler og observeret, at databehandler heri forpligter sig til uden unødigt forsinkelse at underrette den dataansvarlige om sikkerhedsbrud.</p> <p>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.</p> <p>Vi er på forespørgsel blevet informeret om, at der ikke har været persondatasikkerhedsbrud relateret til Sentinel.</p>	<p>Vi har konstateret, at der ikke har været persondatabrud siden sidste revision, hvorfor vi ikke har kunnet teste kontrollens implementering.</p> <p>Ingen afvigelser konstateret.</p>
<p>Bistand til den dataansvarlige ved brud på persondatasikkerhed</p> <ul style="list-style-type: none"> ▶ Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret, at databehandleren har en procedure for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet.</p> <p>Vi er på forespørgsel blevet informeret om, at der ikke har været nogle anmodninger om bistand til den dataansvarlige vedr. persondatasikkerhed.</p>	<p>Vi har konstateret, at der ikke har været nogle anmodninger om bistand til den dataansvarlige vedr. persondatasikkerhed siden sidste revision, hvorfor vi ikke har kunnet teste kontrollens implementering.</p> <p>Ingen afvigelser konstateret.</p>

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
<p>Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret beredskabsplanen og observeret, at en Recovery Time Objective (RTO), og den maksimalt acceptable tidsperiode for database før aktivering af beredskab, betegnet Recovery Point Objective (RPO), er blevet defineret.</p> <p>Vi har observeret, at beredskabsplanen definerer, at der skal foretages en årlig test af beredskabsplanen.</p> <p>Vi har inspiceret dokumentation for udført test og opfølgning af beredskabsplan i august 2025 og observeret, at den er dokumenteret og evalueret.</p>	<p>Ingen afvigelser konstateret.</p>

A.18: Overensstemmelse		
<p>Kontrolmål</p> <ul style="list-style-type: none"> ▶ <i>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. 10, artikel 29, artikel 32, stk. 4 og artikel 33, stk. 2.</i> ▶ <i>At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives i overensstemmelse med organisationens politikker og procedurer - GDPR-artikel 28, stk. 1.</i> 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Indgåelse af databehandleraftale med den dataansvarlige</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har observeret, at databehandleren har sat et system op for at sikre at en databehandleraftale altid indgås med dataansvarlige parter gennem eKvis, på basis af databehandlerens standard databehandleraftale.</p> <p>Vi har inspiceret databehandlereskabeloner for indgåelse af databehandleraftaler og observeret, at de dækker relevante områder, herunder brugen af underdatabehandlere.</p> <p>Vi har foretaget inspektion af databehandleraftaleskabeloner og observeret, at aftalerne indeholder informationer om brugen af underdatabehandlere.</p> <p>Vi har inspiceret, at seneste indgået databehandleraftaler er baseret på databehandlerens skabelon for databehandleraftaler.</p> <p>Vi har observeret, at indgåede databehandleraftaler er underskrevet og at de opbevares elektronisk.</p>	<p>Ingen afvigelser konstateret</p>
<p>Instruks for behandling af personoplysninger</p> <ul style="list-style-type: none"> ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har observeret, at databehandlerens standarddatabehandleraftaler indeholder instrukser fra den dataansvarlige part.</p> <p>Vi har inspiceret processen for, hvordan det sikres at databehandler kun behandler personoplysninger, som dataansvarlig har givet tilladelse til via deres "projekt tilmeldings bank".</p>	<p>Ingen afvigelser konstateret</p>

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, at seneste indgået databehandleraftaler er baseret på databehandlers skabelon for databehandleraftaler.	
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.	Vi har konstateret, at der ikke har været tilfælde af ulovlig instruks, hvorfor vi ikke har kunnet teste kontrollens implementering. 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 skabelon for databehandleraftaler og observeret, at personoplysninger skal slettes eller tilbageleveres, hvis aftalen ophører. Vi har inspiceret procedure for sletning af personoplysninger og observeret, at data slettes og at dataansvarlige informeres om, at dette sker inden for 30 dage. Vi har inspiceret dokumentation for, at der ikke behandles data på ikke aktive databehandleraftaler.	Ingen afvigelser konstateret.

A.18: Overensstemmelse		
<p>Kontrolmål</p> <ul style="list-style-type: none"> ▶ <i>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.</i> ▶ <i>At sikre, at informationssikkerhed og databeskyttelse er implementeret og drives i overensstemmelse med organisationens politikker og procedurer - GDPR-artikel 28, stk. 1.</i> 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Overførsel af personoplysninger til tredjelande</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi er på forespørgsel blevet informeret om, at persondata ikke overføres til tredjelande.</p>	Ingen afvigelser konstateret
<p>Udpegelse af databeskyttelsesrådgiveren</p> <ul style="list-style-type: none"> ▶ Databehandleren har udpeget en databeskyttelsesrådgiver. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret dokumentation for, at databehandleren er pålagt at udpege en DPO.</p> <p>Vi har inspiceret dokumentation for, at databehandleren har udpeget en DPO og beskrevet dennes opgaver.</p>	Ingen afvigelser konstateret
<p>Databeskyttelsesrådgiverens stilling</p> <ul style="list-style-type: none"> ▶ 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. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har inspiceret Sundhed.dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret, at der heraf fremgår en beskrivelse af DPO'ens stilling.</p> <p>Vi har inspiceret Sundhed.dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret, at det heraf fremgår at</p>	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. 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
	DPO'en skal inddrages i sager vedrørende beskyttelse af personoplysninger. Vi har inspiceret Sundhed.dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret, at det heraf fremgår, at DPO'en rapporterer direkte til ledelsen. Vi har inspiceret dokumentation for, at DPO'en skal være underlagt tavshedspligt. Vi har inspiceret tavshedserklæring og observeret, at DPO'en har underskrevet denne.	
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 inspiceret dokumentation for, at databeskyttelsesrådgiveren udfører de opgaver DPO'en er pålagt. Vi har inspiceret Sundhed.dk – Sentinels beskrivelse af databeskyttelsesrådgiverens opgaver og observeret, at det er defineret, hvornår DPO'en ikke må inddrages, idet det vil medføre, 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, vurderer 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.	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
	<p>Vi har fået oplyst, at der regelmæssigt føres kontrol med de organisatoriske sikkerhedsforanstaltninger for at vurdere om disse fungerer effektivt.</p> <p>Vi har inspiceret, at der i risikovurderingen tages stilling til effektiviteten af indførte foranstaltningerne.</p> <p>Vi har inspiceret, at databehandleren har gennemført en Penetrationstest for, at evaluerer effektiviteten af deres tekniske sikkerhedsforanstaltninger.</p>	

**BDO STATSATORISERET
REVISIONSPARTNERSELSKAB**

**VESTRE RINGGADE 28
8000 AARHUS C**

www.bdo.dk

BDO Statsautoriseret Revisionspartnerselskab, en danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlemsfirmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.800 medarbejdere, mens det verdensomspændende BDO-netværk har ca. 95.000 medarbejdere i 169 lande.

*Copyright - BDO Statsautoriseret revisionspartnerselskab,
cvr.nr. 45 71 93 75.*



PENNEO

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

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

Øzlem Polat

Enhedschef, Sentinel-enheden

Serienummer: c5d89dc9-3bdc-4c00-a19f-bf1e2bab71b3

IP: 77.75.xxx.xxx

2026-02-16 10:18:32 UTC



Nicolai Tobias Visti Pedersen

BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375

Statsautoriseret revisor

Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e

IP: 77.243.xxx.xxx

2026-02-16 10:24:15 UTC



Mikkel Jon Larsen

BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375

Partner

Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6

IP: 77.215.xxx.xxx

2026-02-17 07:40:54 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.