et trygt samfund med it og data

Revisorerklæring

NOVAX A/S

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. januar 2021 til 31. december 2021

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

Marts 2022

Indholdsfortegnelse

Afsnit 1: NOVAX A/S' beskrivelse af behandlingsaktivitet for leverancen af elektroniske journalsystemer

Formålet med denne beskrivelse er at levere oplysninger til NOVAX A/S' kunder og deres interessenter (NOVAX A/S (herefter NOVAX) udvikler, vedligeholder og driftsafvikler IT-systemer (NOVAX-systemet) til en lang række aktører primært i den danske sundhedssektor, herunder læger og privathospitaler, samt en række af landets kommuner.

NOVAX behandler personoplysninger som databehandler i medfør af Databeskyttelsesforordningen og Databeskyttelsesloven, fx ved registrering, bearbejdning, arkivering, opbevaring og videregivelse af sundhedsdata i relevant og fornødent omfang. Behandlingen omfatter data af almindelig og fortrolig karakter samt særlige kategorier af personoplysninger (følsomme).

NOVAX-Systemet har snitflader til en lang række offentlige og private systemer og leverandører, fx Sundhedsdatanettet (Medcom), services fra Sundhedsdatastyrelsen osv., så det sikres, at NOVAX-Systemet kan opfylde kundens behov.

Uanset i hvilken sammenhæng NOVAX-Systemet benyttes eller hvem der benytter det, er den dataansvarlige altid den juridiske enhed, der udgør NOVAX' kunde.

Baseret på risikovurderingen er der udarbejdet og implementeret en informationssikkerhedspolitik med tilhørende informationssikkerhedshåndbog samt en lang række procedurer for specifikke områder.

Der gennemføres løbende drøftelse og iværksættelse af løsningstiltag af risici, som afrapporteres til NOVAX' ledelse.

Generelle tekniske og organisatoriske foranstaltninger

NOVAX har indført en række tekniske og organisatoriske foranstaltninger for at sikre, at såvel gældende lovgivning som det aftalte med kunden til enhver tid efterleves.
Der henvises afsnittet nedenfor, hvor de enkelte kontrolaktiviteter er beskrevet.

Behandlingssikkerhed

Som led i NOVAX' løbende arbejde med at sikre behørige og passende sikkerhedsforanstaltninger er NOVAX i proces med implementering af ISO/IEC 27001:2013 (herefter ISO27001) samt ISO/IEC 27002:2013 (herefter ISO27002).

Herudover kan fremhæves blandt andet følgende tiltag til iagttagelse af behørig og passende behandling af personoplysninger, som er nærmere uddybet i NOVAX' interne procedurer og kontroller:

Medarbejdere

- Medarbejdere, som har et arbejdsbetinget behov for at behandle personoplysninger, er pålagt tavshedspligt

- Medarbejdere vejledes og instrueres i sikker behandling af personoplysninger

Styring af aktiver

- Alle IT-aktiver styres, så vidt muligt, centralt i Active Directory og Managed Workplace

Adgangskontrol

- Der er etableret adgangsbegrænsning til personoplysninger, så der udelukkende gives adgang, hvis det er nødvendigt

Kryptering

- Tilgang til webservices sker krypteret, oftest via HTTPS/TLS
- Medarbejdernes eksterne tilgang til ressourcer sker via krypterede forbindelser

Fysisk sikkerhed

- Adgang til NOVAX er beskyttet med alarm- og adgangssystemer. Der er faste procedurer for gæste-adgang til NOVAX' bygninger samt for adgang til serverrum. Alene medarbejdere med arbejdsbetinget behov kan opnå adgang hertil
- Fysisk tilslutning til NOVAX' IT-infrastruktur er begrænset teknisk og via politikker
- I relation til fysisk sikkerhed for NOVAX' datacenter henvises til afsnittet "underdatabehandlere/-leverandører"

IT-sikkerhed

- Servere og klienter har aktiv, opdateret anti-virus/anti-malwaresoftware
- Servere og klienter er underlagt politikker for automatisk opdatering af styresystem og whitelistede 3. parts produkter
- Der foretages backup af alle IT-systemer, der behandler personoplysninger
- Det sikres, at default opsætning ift. logning og overvågning, password kompleksitet og udløb er defineret
- Der foretages monitorering af IT-udstyr og IT-systemer
- Der foretages patch- og vulnerability management
- SIEM-system implementeret
- Penetrations test i faste intervaller

Netværkssikkerhed

- Perimetersikring af netværk med firewall
- UTM implementeret
- Mail spam og malware scanning
- Netværksperimetersikring
- Netværkssegmentering er gennemført jf. informationssikkerhedspolitikken
- Håndtering af hændelser

Styring af hændelser med tilhørende beredskab, herunder "disaster recovery plan".

Underdatabehandlere/-leverandører

NOVAX sikrer, at der alene anvendes velkvalificerede underdatabehandlere/- leverandører og NOVAX fører tilsyn med disse samt foretager løbende orientering af sine kunder (de dataansvarlige) om de anvendte underdatabehandlere. Tilsyn består blandt andet i møder, løbende rapportering samt gennemgang af revisionserklæringer i relevant omfang. Nærværende erklæring er en partiel erklæring og omfatter således ikke revisors gennemgang af underdatabehandlernes revisionserklæringer.

I relation til opbevaring af personoplysninger anvender NOVAX primært én underdatabehandler, som blandt andet har implementeret følgende sikkerhedsforanstaltninger i sit datacenter:

- Adgang til faciliteterne sker via nøglekort, der tilpasses den enkelte medarbejders behov i henhold til jobfunktion
- I tilfælde af strømafbrydelser er der installeret en uninterruptable power supply (UPS)
- I tilfælde af strømafbrydelser er der installeret en diesel generator
- Der er foretaget sikring mod indtrængning af grundvand og installeret alarmer, der overvåger grundvandsniveauet
- Der sker overvågning af indeklima 24/7, som sikrer, at foruddefinerede temperaturer og fugtighed ikke overskrides
- Bygninger er indhegnede og der foretages videoovervågning

Væsentlige ændringer i perioden

Der har ikke været væsentlige ændringer i perioden. Relevant at fremhæve er dog, at

- NOVAX har etableret eget kontor i Spanien (Malaga)
- NOVAX tog nye underdatabehandlere i brug i foråret 2021, som forinden var blevet kommunikeret til kunderne
- NOVAX er i gang med at ændre IT-setup hos Mentor IT (leverandør af datacenter), så Mentor IT fremover forestår yderligere håndtering af IT-teknisk setup. Mentor IT er fortsat databehandler

Komplementerende kontroller hos den dataansvarlige

- Den dataansvarlige har følgende bl.a. forpligtelser i medfør af databeskyttelsesreglerne:
    - At sikre, at den dataansvarliges brugere er ajourførte
    - At sikre, at personoplysningerne er ajourførte og slettes behørigt
    - At sikre, at der er indgået en kontrakt med NOVAX, der sikrer, at NOVAX alene handler efter instruks fra den enkelte kunde, og at NOVAX træffer alle nødvendige og tekniske foranstaltninger til behandling af personoplysninger
    - At sikre, at instruksen er hensigtsmæssig set i forhold hovedydelsen
    - At sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering
    - At sikre, at tilgang til terminaler, PC'ere, bærbare og andre enheder, der kan tilgå NOVAX-systemet, alene sker for autoriserede brugere, herunder tildeling af rettigheder til autoriserede bruger

Afsnit 2: NOVAX A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for NOVAX A/S' kunder, som har indgået en databehandleraftale med NOVAX A/S, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

NOVAX A/S anvender underdatabehandlerne:

NOVAX Sundhedspleje og PPR

- Datagruppen Multimed A/S
- Intermail Danmark A/S
- Link Mobility A/S
- Medcom
- Mentor IT A/S
- NOVAX Software ApS
- Nordic Software Solutions ApS
- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

NOVAX Journalsystem (Misbrugs- og rehabiliteringscentre)

- Datagruppen Multimed A/S
- Intermail Danmark A/S
- Link Mobility A/S
- Medcom
- Mentor IT A/S
- Region Syddanmark
- NOVAX Software ApS
- Nordic Software Solutions ApS
- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

NOVAX Journalsystem (Læge)

- Datagruppen Multimed A/S
- Flexfone A/S
- Intermail Danmark A/S
- Link Mobility A/S
- Medcom
- Mentor IT A/S
- PLSP A/S
- Region Syddanmark
- Tier 1 Asset A/S
- NOVAX Software ApS
- Nordic Software Solutions ApS

- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

Underdatabehandlere via koncernforbundne selskaber (for NOVAX Journalsystem Læge)

- Microsoft Ireland

NOVAX Journalsystem (Pleje)

- Link Mobility A/S
- Medcom
- Mentor IT A/S
- Region Syddanmark
- NOVAX Software ApS
- Nordic Software Solutions ApS
- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

Underdatabehandlere via koncernforbundne selskaber (for NOVAX Journalsystem Pleje)

- Datagruppen Multimed A/S
- Microsoft Ireland

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos NOVAX A/S' underleverandører og underdatabehandlere.

NOVAX A/S bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af, hvordan NOVAX A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 1. januar 2021 til 31. december 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan NOVAX A/S' processer og kontroller relateret til databeskyttelse var udformet og implementeret, herunder redegør for:

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

som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

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

(ii) Indeholder relevante oplysninger om ændringer ved databehandlerens elektroniske journalsystemer til behandling af personoplysninger foretaget i hele perioden fra 1. januar 2021 til 31. december 2021

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

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2021 til 31. december 2021.

Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2021 til 31. december 2021

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

Lystrup, den 16. marts 2022
NOVAX A/S

Ole Abildgaard
Adm. direktør

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. januar 2021 til 31. december 2021

Til NOVAX A/S og NOVAX A/S' kunder i rollen som dataansvarlige.

Omfang

Vi har fået til opgave at afgive erklæring med høj grad af sikkerhed om NOVAX A/S' beskrivelse i "Afsnit 1" af elektroniske journalsystemer i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig i hele perioden fra 1. januar 2021 til 31. december 2021 og b+c) om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

NOVAX A/S anvender underdatabehandlerne:

NOVAX Sundhedspleje og PPR

- Datagruppen Multimed A/S
- Intermail Danmark A/S
- Link Mobility A/S
- Medcom
- Mentor IT A/S
- NOVAX Software ApS
- Nordic Software Solutions ApS
- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

NOVAX Journalsystem (Misbrugs- og rehabiliteringscentre)

- Datagruppen Multimed A/S
- Intermail Danmark A/S
- Link Mobility A/S
- Medcom
- Mentor IT A/S
- Region Syddanmark
- NOVAX Software ApS
- Nordic Software Solutions ApS
- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

NOVAX Journalsystem (Læge)

- Datagruppen Multimed A/S
- Flexfone A/S
- Intermail Danmark A/S
- Link Mobility A/S
- Medcom
- Mentor IT A/S

- PLSP A/S
- Region Syddanmark
- Tier 1 Asset A/S
- NOVAX Software ApS
- Nordic Software Solutions ApS
- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

Underdatabehandlere via koncernforbundne selskaber (for NOVAX Journalsystem Læge)

- Microsoft Ireland

NOVAX Journalsystem (Pleje)

- Link Mobility A/S
- Medcom
- Mentor IT A/S
- Region Syddanmark
- NOVAX Software ApS
- Nordic Software Solutions ApS
- Nordic Software Solutions S.L.
- Medicinsk Data Distribution ApS

Underdatabehandlere via koncernforbundne selskaber (for NOVAX Journalsystem Pleje)

- Datagruppen Multimed A/S
- Microsoft Ireland

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos NOVAX A/S' underleverandører og underdatabehandlere.

Vores konklusion udtrykkes med høj grad af sikkerhed.

NOVAX A/S' ansvar

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

Vores 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.

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

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af elektroniske journalsystemer samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "Afsnit 1".

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

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

Begrænsninger i kontroller hos en databehandler

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

Konklusion

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

(a) at beskrivelsen af elektroniske journalsystemer, således som denne var udformet og implementeret i perioden fra 1. januar 2021 til 31. december 2021, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra 1. januar 2021 til 31. december 2021, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i perioden fra 1. januar 2021 til 31. december 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt NOVAX A/S' elektroniske journalsystemer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, 28. marts 2022

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Christian H. Riis
Partner, CISA

Michael Marseen
Statsautoriseret revisor

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

Vores arbejde er udført i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-I nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden fra 1. januar 2021 til 31. december 2021.

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos NOVAX A/S' underleverandører og underdatabehandlere.

Kontroller udført hos de dataansvarlige er ikke omfattet af vores erklæring.

Vi har udført vores tests af kontroller hos NOVAX A/S via følgende handlinger:

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

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

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

Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Nyt område ift. ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Nyt område ift. ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2

G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15, 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har forespurgt, om databehandleren har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi er blevet informeret om, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, hvorfor vi ikke har testet effektiviteten af relevante procedurer. Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har inspiceret, at der for de systemer og aktiver, der anvendes til behandling af personoplysninger, er installeret antivirus software. Vi har inspiceret, at antivirus software er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret adgange til personoplysninger, og påset, at dette sker gennem firewall.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugernes adgang til personoplysninger. Vi har stikprøvevis inspiceret, at brugernes adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har stikprøvevis inspiceret systemer, og stikprøvevis påset, at der er opsat alarmer.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevis inspiceret tilgang til personoplysninger, og stikprøvevis påset, at dette sker med krypteret forbindelse.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
B.9	Der er etableret logning i systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har stikprøvevis inspiceret systemer, og stikprøvevis påset, at der er etableret logning. Vi har inspiceret gennemgang af logfiler, herunder administratorlogs i perioden, og påset, at disse gennemgange er blevet udført.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Vi har stikprøvevis inspiceret, at personoplysninger er pseudonymiseret eller anonymiseret i udviklings- og testdatabaser.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har stikprøvevis inspiceret penetrationstest udført i perioden, og stikprøvevis påset, at dette følger de planlagte test.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Vi har stikprøvevis inspiceret ændringer I perioden, og stikprøvevis påset, at ændringerne følger den interne procedure.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har stikprøvevis inspiceret, at medarbejdernes adgange til systemer og databaser er godkendt, og at der er et arbejdsbetinget behov. Vi har stikprøvevis inspiceret, at fratrådte medarbejderes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Vi har inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Vi har stikprøvevis inspiceret adgange til personoplysninger, og stikprøvevis påset, at dette sker med tofaktor autentifikation.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret, at databehandleren har oversigt over nøgler til serverrum.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er tilgængelig for databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har stikprøvevis inspiceret, at der er dokumentation for, at der er blevet foretaget efterprøvning af medarbejdere i perioden.	Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har stikprøvevis inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale. Vi har inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har stikprøvevis inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget for fratrådte medarbejdere i erklæringsperioden.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Vi har stikprøvevis inspiceret, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt for fratrådte medarbejdere i erklæringsperioden.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	Vi har inspiceret dokumentation for, at DPO'en er blevet inddraget i relevante opgaver i erklæringsperioden.	Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret, at der foreligger fortegnelser, som er behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevis inspiceret ophørte aftaler i perioden, og stikprøvevis påset, at der er aftalt krav til opbevaring og sletterutiner.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har stikprøvevis inspiceret, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført for ophørte databehandlinger i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede politikker for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at politikker er opdaterede.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har stikprøvevis inspiceret, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede politikker for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at politikken er opdateret.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har stikprøvevis inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har stikprøvevis inspiceret dokumentation for, at dataansvarlige er blevet underrettet I forhold til nye underdatabehandlere.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har stikprøvevis inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede politikker, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Vi har inspiceret, at politikkerne er opdaterede.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er taget stilling til tredjelandsoverførsler. Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer	Vi er blevet informeret om, at personoplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er taget stilling til tredjelandsoverførsler. Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer	Vi er blevet informeret om, at personoplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Kontrolmål H – De registreredes rettigheder

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.	Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har inspiceret liste over anmodninger I perioden. Vi har forespurgt, om databehandleren har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder.	Vi er blevet informeret om, at databehandleren ikke har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	*NOVAX A/S' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har forespurgt, om der har været persondatassikkerhedsbrud i perioden.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har inspiceret proceduren for håndtering af hændelser og brud, og påset, at det håndtering brud er beskrevet.	Ingen afvigelser konstateret.