AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 30. NOVEMBER 2024 OM BESKRIVELSEN AF IT-LØSNINGER 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

KIMIK IT A/S

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 30. NOVEMBER 2024 OM BESKRIVELSEN AF IT-LØSNINGER 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 KIMIK iT A/S
KIMIK iT A/S' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af KIMIK iT A/S (databehandleren) pr. 30. november 2024 udarbejdede beskrivelse i sektion 3 af IT-løsninger 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. 30. november 2024.

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

Databehandlerens ansvar

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

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

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

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens revisors

vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

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

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

Begrænsninger i kontroller hos en databehandler

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af IT-løsninger, 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 IT-løsninger 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. 30. november 2024, 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. 30. november 2024.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens IT-løsninger, 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 23. januar 2025

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. KIMIK IT A/S' UDTALELSE

KIMIK iT A/S varetager behandling af personoplysninger i forbindelse med IT-løsninger for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt IT-løsninger, 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.

KIMIK iT A/S anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

KIMIK iT A/S bekræfter, at den medfølgende beskrivelse på side 6 til 17 giver en retvisende beskrivelse af IT-løsninger og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 30. november 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for IT-løsninger, 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 IT-løsninger 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 IT-løsninger og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen

til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved IT-løsninger, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

KIMIK iT A/S 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. 30. november 2024. 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.

KIMIK iT A/S 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.

Nuuk, den 23. januar 2025

KIMIK iT A/S

Gynter Schneider
Direktør

3. KIMIK IT A/S' BESKRIVELSE AF IT-LØSNINGER

KIMIK IT A/S

KIMIK iT er en grønlandsk ejet virksomhed, der supporterer, drifter kundens IT-miljøer, udfører systemudvikling og forretningsanalyse på tværs af de fem grønlandske kommuner, departementer og Skattestyrelsen.
KIMIK iT har kontorer i Nuuk og i Viby, og har derudover medarbejdere der arbejder fast hjemmefra.
KIMIK iT beskæftiger ca. 28 medarbejdere, som er specialiserede inden for systemudvikling, serverdrift, support og informationssikkerhed, og organiseret i en udviklingsafdeling, en teknisk afdeling, en afdeling for forretningsanalyse og en administrationsafdeling.

Ledelsen styrer KIMIK iT's persondatasikkerhed i forhold til den behandling, som KIMIK iT varetager på vegne af sine kunder, herunder indgåelse og opdatering af databehandleraftaler, besvarelse af henvendelser fra den dataansvarlige, underretning om brud på persondatasikkerheden, efterlevelse af interne politikker og procedurer og lignende.

IT-LØSNINGER OG BEHANDLING AF PERSONOPLYSNINGER

Den Dataansvarlige anvender en række Fællesoffentlige it-løsninger, der udvikles og supporteres af Databehandleren med henblik på at understøtte driften af den Dataansvarliges virksomhed.
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om, at Databehandleren bistår med udvikling, implementering, support og videreudvikling af IT-systemer, som den Dataansvarlige anvender til løsning af sine opgaver indenfor administrativ sagsbehandling af borgerhenvendelser samt generel servicering- og sagsbehandling i relation til borgervendte ydelser – herunder gennem borgervendte selvbetjeningsløsninger.
IT-systemerne dækker:

- eSkat med delsystemerne Personskat, Selskabsskat, Suliffinnut, Innuttaasunut, Min Skat, Arbejdsgiverregister, Sulinal og Obligatorisk pension.
- Winformatik og selvbetjeningsløsningerne for bopælsattest, boligsikring og daginstitution.
- IT-Reg og selvbetjeningsløsningen onlineansøgningen.
- Valgoptællingssystemet og optællingssiden valg.gl.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede.
Der behandles alle typer af personoplysninger; både almindelige, fortrolige og følsomme. Herunder navn, e-mailadresse, telefonnummer, adresse, personnummer, løn, bankkonti, helbredsoplysninger, oplysninger om straffe, lægeerklæringer og socialfaglige vurderinger.

Behandlingen omfatter følgende kategorier af registrerede:

- Den Dataansvarliges ansatte
- Borgere

Behandlingen er ikke tidsbegrænset og vedvarer indtil, der ikke længere foreligger en aktiv aftale om Databehandlerens bistand til den Dataansvarlige mellem den Dataansvarlige og Databehandleren, og Databehandleren endegyldigt har slettet alle oplysninger, der er behandlet på vegne af den Dataansvarlige.

STYRING AF PERSONDATASIKKERHED

KIMIK iT har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af compliance platformen ComplyCloud for persondatasikkerhed, der sikrer opfyldelse af indgående aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.
Styring af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter.

ISO 27001-OMRÅDE	KONTROLOMRÅDE	ARTIKEL
Risikovurdering	• Risikovurdering	• Artikel 28, stk. 3, litra c
A.5: Informationssikkerhedspolitikker	• Informationssikkerhedspolitik • Gennemgang af informationssikkerhedspolitik	• Artikel 28, stk. 1
A.6: Organisering af informationssikkerhed	• Roller og ansvarsområder • Fjernarbejdspladser og fjernadgang til systemer og data	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra c
A.7: Personalesikkerhed	• Rekruttering af medarbejdere • Fratrædelse af medarbejdere • Uddannelse og awareness af medarbejdere • Tavsheds- og fortrolighedsaftale med medarbejdere	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra b
A.8: Styring af aktiver	• Fortegnelse over kategorier af behandlingsaktiviteter	• Artikel 30, stk. 2, 3 og 4
A.9: Adgangsstyring	• Logisk adgangssikkerhed, herunder autorisation og adgangskontrol	• Artikel 28, stk. 3, litra c
A.10: Kryptografi	• Kryptering af personoplysninger	• Artikel 28, stk. 3, litra c
A.11: Fysisk sikring og miljøsikring	• Fysisk adgangskontrol • Fysisk sikkerhed	• Artikel 28, stk. 3, litra c
A.12: Driftssikkerhed	• Driftsprocedurer • Antivirusprogram • Backup • Logning og overvågning • Sårbarhedsscanning og penetrationstests	• Artikel 28, stk. 3, litra c
A.13: Kommunikationssikkerhed	• Styring af netværkssikkerhed • Informationsoverførsel	• Artikel 28, stk. 3, litra c
A.14: Anskaffelse, udvikling og vedligeholdelse	• Analyse og specifikation af informationssikkerhedskrav • Udvikling og vedligeholdelse af systemer • Informationssikkerhed i ændring og udvikling • Adskillelse af udviklings-, test- og produktionsmiljø	• Artikel 25
A.15: Leverandørforhold	• Underdatabehandlere	• Artikel 28, stk. 2 og 4
A.16: Styring af informationssikkerhedsbrud	• Underretning om brud på persondatasikkerheden	• Artikel 33, stk. 2
A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring	• Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse	• Artikel 28, stk. 3, litra c
A.18: Overensstemmelse	• Databehandleraftale • Instruks for behandling af personoplysninger • Bistand til den dataansvarlige • Sletning og tilbagelevering af personoplysninger • Overførsel af personoplysninger til tredjelande • Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger	• Artikel 28, stk. 3, litra a, c, e, f, g og h • Artikel 29 • Artikel 32, stk. 4 • Artikel 28, stk. 10 • Artikel 44 - 49

RISIKOVURDERING

Ledelsen er ansvarlig for, at der iværksættes alle initiativer, der imødegår det trusselsbillede, som KIMIK iT til enhver tid står over for, således at indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

Der foretages en løbende vurdering af, hvilket sikkerhedsniveau der er passende. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller udføres der en gang årligt en risikovurdering. Risikovurderingen belyser sandsynligheden for og konsekvenserne af hændelser, der kan true persondatasikkerheden og dermed fysiske personers rettigheder og frihedsrettigheder, herunder tilfældige, forsætlige og uforsætlige hændelser. Risikovurderingen tager hensyn til det aktuelle tekniske niveau og implementeringsomkostninger.

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.

KIMIK iT modtager løbende orienteringer af risici fra forskellige leverandører samt eksterne websites.
KIMIK iT handler asap eller ifm næstkommende maintenance, alt afhængig af risici niveau.

A.5: Informationssikkerhedspolitikker

KIMIK iT har indført politikker og procedurer, der sikrer, at KIMIK iT kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
KIMIK iT har etableret en organisering af persondatasikkerheden, samt udarbejdet og implementeret en, af ledelsen godkendt, informationssikkerhedspolitik, der løbende gennemgås og opdateres.

Informationssikkerhedspolitikken gennemgås af ledelsen, minimum årligt, for at sikre at den fortsat er korrekt og fyldestgørende.
Informationssikkerhedspolitikken er gennemgået for de ansatte, og de har altid adgang til den seneste version af den. Nye ansatte får ligeledes en gennemgang af politikken.
KIMIK iT udfører egenkontrol af efterlevelse af instrukser i indgåede databehandleraftaler.

A.6: Organisering af informationssikkerhed

Roller og ansvarsområder
Politik for organisering af informationssikkerhed.

Formålet med KIMIK iT's politik og regler for organisering af informationssikkerhed er:

- at etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.
- at sikre fjernarbejdspladser og brugen af mobilt udstyr.

Roller og ansvarsområder:

- det overordnede ansvar for informationssikkerheden ved KIMIK iT ligger ved ledelsen og er underorganiseret således, at implementering og forvaltning af informationssikkerheden er ansvarsfordelt mellem afdelingsledelsen for hhv. den tekniske afdeling og udviklingsafdelingen.

Kontakt med myndigheder:

- i forbindelse med eventuelle brud på sikkerheden er der oprettet en procedure for, hvordan enheder indmelder sådanne brud. Denne proces sikrer kontakt til relevante myndigheder, eksempelvis Datatilsynet.

Styringen sker via compliance platformen ComplyCloud.

Databeskyttelsesrådgiver
Direktøren er udpeget som databeskyttelsesrådgiver, da denne har en bred viden om virksomhedens behandling af følsomme personoplysninger. Der er udarbejdet en funktionsbeskrivelse for databeskyttelsesrådgiveren, herunder beskrevet databeskyttelsesrådgiverens opgaver.

Funktionsadskillelse
Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug af privilegier minimeres. Hvor funktionsadskillelse ikke er muligt, skal der implementeres kompenserende tiltag.
Der bør sikres funktionsadskillelse blandt IT-ansatte så vidt muligt således, at de, der har adgang til evt. logning, ikke er de samme, som dem der har adgang til data. De, der har adgang til at administrere data, behøver ikke nødvendigvis at have læserettigheder. Dette skal sikre, at der ikke kan manipuleres med loggen.

Politik for mobilt udstyr
Fortrolige informationer skal krypteres, når de opbevares eller transporteres på bærbare medier, f.eks. USB-hukommelse. Manglende kryptering tillades, hvis medierne, der benyttes til transport af fortrolige data, under transporten er overvåget af betroede personer. Bærbare medier, som er overleveret til samarbejdspartnere, skal sikres returnering eller destruering ved projektets afslutning.

Fjernarbejdspladser og fjernadgang til systemer og data
KIMIK iT har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for KIMIK iT's lokaler og fjernadgang til systemer og data sker via VPN-forbindelser.
Der installeres automatisk Microsoft Defender P2 på KIMIK iT's maskiner, når de bliver indlemmet i KIMIK iT's domæne.

Der bruges MFA, når der laves VPN. Dette sker via DUO på KIMIK iT's Palo Alto firewall.

A.7: Personalesikkerhed

Rekruttering og fratrædelse af medarbejdere
Der forefindes procedure for rekruttering og fratrædelse af medarbejdere.

Uddannelse og instruktion af medarbejdere, der behandler personoplysninger og Awareness og oplysningskampagner for medarbejdere
Der foretages gennemgang af politikker og procedurer for nuværende og nye medarbejdere.

Produktet Pistachio anvendes til awareness træning i cybersikkerhed samt tests i form af simulerede cyberangreb.

Fortrolighed og lovbestemt tavshedspligt
KIMIK iT har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over kategorier af behandlings-aktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

Alle medarbejdere har underskrevet en ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt.

Fratrædelse af medarbejdere kan deles op i to scenarier, hvor til der handles forskelligt.
Den ene situation er, at den ansatte selv siger op, den anden situation er, at der sker afskedigelse.
Ved afskedigelse kræves der øjeblikkelig handling fra ledelsen.

Ved ophør af ansættelsesforhold sikrer den daglige leder, at alle rettigheder og adgange til fysiske og tekniske aktiver inddrages. Ved fratrædelse af ledelse, sikrer kædens ledelse, alternativt bestyrelsen, de nødvendige tiltag.

A.8: Styring af aktiver

Fortegnelse over kategorier af behandlingsaktiviteter
KIMIK iT har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.
Betegnelsen ligger i compliance platformen ComplyCloud.

Når tilsynsmyndigheden anmoder om at få stillet en fortegnelse til rådighed udleveres denne.

Mærkning af information
Information af mærket.

Styring af flytbare medier
KIMIK iT opbevarer normalt ikke data på flytbare medier, og når KIMIK iT bruger flytbare medier, så er de krypteret.

Bortskaffelse af medier
It-udstyr med data bliver nulstillet og diske bliver ødelagte.
It-udstyr bliver efterfølgende kørt på genbrug af en KIMIK iT medarbejder.

Diske bliver åbnet, ulæseliggjort og lukket.

Fysiske medier under transport
Fysiske medier er krypteret under transport.

A.9: Adgangsstyring

KIMIK iT har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

A.10: Kryptografi

KIMIK iT har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis. KIMIK iT har indført procedurer, der sikrer, at data af personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, er krypteret ved ibrugtagning, således at adgang til data alene er muligt for autoriserede brugere. Genoprettelsesnøgler af certifikater opbevares på forsvarlig vis.

De algoritmer og niveauer for kryptering, der er anvendt til kryptering af enheder, servere og data, risiko-vurderes løbende i forhold til det aktuelle trusselsniveau.

A.11: Fysisk sikring og miljøsikring

KIMIK iT har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne, og særlige sikkerhedsmæssige foranstaltninger er indført for områder, hvor der foretages behandling af personoplysninger. Kunder, leverandører og andre besøgende ledsages.
KIMIK iT har indført procedurer, der sikrer, at adgang til serverrum er tildelt ud fra et arbejdsbetinget behov. Serviceleverandør, der har behov for adgang for at varetage opsyn eller vagt, er godkendt af ledelsen. Tildelte adgange til serverrum gennemgås og revideres ved ændringer og mindst én gang årligt.
KIMIK iT har indført procedurer, der sikrer, at servere er beskyttet mod uautoriseret adgang, beskadigelse, driftsafbrydelser og lignende hændelser ved særlige sikkerhedsforanstaltninger. Servere er således opbevaret i et særligt indrettet serverrum med fysisk og elektronisk adgangskontrol og logning af adgange. Serverrummet er sikret mod miljømæssige trusler som brand, vandindtrængning, fugt, overophedning, strømudfald og overspænding. Systemer til miljømæssig sikring af driftsfaciliteter er serviceret og vedligeholdt løbende efter de respektive leverandørers forskrifter. Driftsmiljøet er overvåget.

Fysisk adgangskontrol

Nuuk

Nox Systems er KIMIK iT's adgangsstyring, som fungerer via en Chip "nøgle" samt en app. Chip "nøgle" giver adgang til at åbne- og låse døre man har adgang til.

Appen giver mulighed for at fra- og tilkoble alarmer til de rum, man har adgang til samt at give adgang til at åbne- og låse døre man har adgang til.

Viby J

Telesikring Alarm er KIMIK iT's adgangsstyring, som fungerer via en Chip "nøgle" samt en app. Chip "nøgle" giver adgang til at åbne- og låse døre man har adgang til.

Appen giver mulighed for at fra- og tilkoble alarmer til de rum, man har adgang til samt at give adgang til at åbne- og låse døre, man har adgang til.

Der er fysisk nøgle til kopi-rummet samt til fordør og bagdør.

Fysisk sikkerhed

Adgang til kontorerne styres via alarmsystemet, hvor der er forskellige rettigheder til at kunne tilgå hvilke lokaler.

Vedligeholdelse af udstyr

KIMIK iT udskifter udstyr når det er blevet for gammelt, dvs. at der ikke længere findes sikkerhedsopdateringer eller/og er blevet for langsomme.

Sikring af udstyr og aktiver for organisationen

Fjernarbejdspladser kan kun tilgås via VPN.
KMIK iT efterlader ikke udstyr uden opsyn på offentlige steder.

Reparation og service samt bortskaffelse af it-udstyr

Se punkt A.8: Styring af aktiver → Bortskaffelse af medier

A.12: Driftssikkerhed

KIMIK iT har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes foranstaltninger og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og

software installeret på servere og arbejdsstationer.

Vedligeholdelse af systemsoftware
CheckMK har en klar oversigt over, hvad for en OS, samt programmer der er på servere.
På CheckMK kan man se, om der er opdateringer, der mangler på de enkelte OS'er eller programmer.

Antivirusprogram
KIMIK iT har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselniveau, og der er opsat en løbende overvågning af disse systemer, herunder periodisk test for funktionalitet.
KIMIK iT bruger Windows Defender XDR p2, som overvåger for sikkerhedsrisikoer for både servere og klienter.

Når enkelte servere, klienter eller specifikke programmer har brug for en opdatering, pga. større sikkerhedsrisiko, får Teknisk Sektion information derom via mail.

Opdateringer til Defender bliver installeret minimum 1 gang pr. måned.

Sikkerhedskopiering og retablering af data
KIMIK iT har indført procedurer, der sikrer, at systemer og data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation. Sikkerhedskopier er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde, eller at sikkerheds-kopier ødelægges ved brand, hærværk eller hændelig skade.

KIMIK iT tager dagligt backup, og der tages ugentligt backup ud af huset.
KIMIK iT laver test af restore 2 gange årligt.

Logning i systemer, databaser og netværk
KIMIK iT har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret mod tab og sletning.
KIMIK iT bruger Microsoft 365 til at holde øje med deres domæne i skyen samt administration af, hvem der har adgang til specifikke grupper.

Overvågning
KIMIK iT har indført procedure, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.
Servere bliver overvåget med CheckMK, hvor der dagligt laves rutinechecks.
Microsoft 365 har mulighed for at der kan overvåges over brugere i domænet.

Sårbarhedsscanning og penetrationstests

tekniske sårbarheder i applikationer, services og infrastruktur, således at tab af fortrolighed, integritet og tilgængelighed af systemer og data undgås.

KIMIK iT har en procedure for udførelse af sårbarhedsscanninger og penetrationstests på regelmæssig basis for at sikre, at tekniske foranstaltninger implementeres og testes.

A.13: Kommunikationssikkerhed

Netværkssikkerhed
KIMIK iT har indført procedurer, der sikrer, at netværk i forhold til anvendelse og sikkerhed er opdelt i et antal virtuelle netværk (VLAN), hvor trafik mellem enkelte virtuelle netværk kontrolleres af firewall. Servere med indbygget firewall benytter denne til at sikre, at der kun gives adgang til nødvendige services.

Firewall
KIMIK iT har indført procedurer, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Det er kun den tekniske chef samt lederen af supportafdelingen og den netværksansvarlige, som kan ændre i firewallene. Og ændringerne skal altid godkendes af enten den tekniske chef eller den netværksansvarlige.

KIMIK iT anvender Palo Alto som firewall. Disse firewalls er sat til at opdatere Antivirus og Sårbarheder hver time. Wildfire opdateres Real-time.

Eksterne kommunikationsforbindelser
KIMIK iT har indført procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med stærk kryptering, og at e-mail og anden kommunikation, der indeholder personoplysninger, er krypteret i forsendelse af TLS.

Eksterne forbindelser etableres med IPSec med shared key.

A.14: Anskaffelse, udvikling og vedligeholdelse

Analyse og specifikation af informationssikkerhedskrav
KIMIK iT inddrager Informationssikkerhedskrav og krav til behandling af personoplysninger i en tidlig vurdering af projekter/systemer.

Udvikling og vedligeholdelse af systemer
Udvikling og vedligehold af applikationer foregår primært i udviklings teams i KIMIK-iT, sekundært ved daglig drifts support af KIMIK-iT 's Tekniske Sektion der typisk supporterer IT platformen på kundernes drifts og test miljøer. Udvikling og vedligehold foregår på kundens præmisser og ønsker og vil til enhver tid foregå med kundens ønsker og behov.

Udviklingsteams i KIMIK-iT anvender overvejende SCRUM som udviklingsproces. Udviklingsteams har ansvaret for en enkelt kunde, og for hver kunde er der en navngiven Udviklingsansvarlig og Forretningsansvarlig. Den Forretningsansvarliges rolle er relationen til kunden og evt. kontraktuelle forhold, hvor den Udviklingsansvarlige har ansvaret for løsningens tekniske design, arkitektur og kvalitet, herunder sikkerhed.
Der foretages, i det omfang systemejeren ønsker det, jævnlige reviews af applikationerne, hvor evt. anbefalede tiltag tages videre til systemejeren. Disse tiltag kan være af funktions-, vedligeholdelses-, licens- eller sikkerhedsmæssig karakter.
Som en integreret del af udviklingsprocessen vil enhver nedbrydning og ethvert design af nyudviklings- og vedligeholdelsesopgaver inkludere overvejelser om evt. opgaver, der relaterer sig til vedligeholdelse og forbedring af sikkerheden.
De enkelte udviklingsteams har adgang til den kildekode, der vedrører de relevante applikationer og dermed kun adgang. Hvis udviklere eller andre tværgående funktioner (testere, projektledere el.lign.) deltager i flere teams, får de således adgangen til kildekode fra forskellige teams.

Informationssikkerhed i ændring og udvikling
Udviklingsteams anvender en række forskellige værktøjer til ALM (Application Lifecycle Management).
Til version control anvendes Microsoft Azure Repos. Der anvendes både repositories af typen GIT og TFVS. Denne version control sikrer, at vi kan genetablere (roll-back) kildekode fra et vilkårligt tidspunkt i kodens liv.
Til udviklingsprocesunderstøttelse, backlog planning, work tracking, release management anvendes der Microsoft Azure Boards.
Hos visse systemejere har vi implementeret et ITSM system (ZenDesk), hvorigennem 1./2. level support tickets oprettes. Hvis tickets ikke ender der, vil de blive oprettet i Azure Boards til videre håndtering.

Til DevOps anvendes Microsoft Azure Pipelines, der har mulighed for CI/CD og test automatisering. Dette anvendes i det omfang, det en ønsket implementeret af de enkelte systemejere.
Test Management udføres ligeledes i Microsoft Azure Test Plans. I det omfang det ern ønsket implementeret og brugt af de enkelte systemejere, anvendes dette til definition og eksekvering af manuelle test cases.
Godkendelse af udviklingsopgaver foretages af systemejer, efter gennemført acceptance test.
Som nævnt i 11.2 har de enkelte udviklingsteams adgang til den kildekode, der vedrører de relevante applikationer og dermed kun adgang. Hvis udviklere eller andre tværgående funktioner (testere, projektledere el.lign.) deltager i flere teams, får de således adgangen til kildekode fra forskellige teams.

Adskillelse af udviklings-, test- og produktionsmiljø
I de systemer hvor KIMIK iT udfører udvikling og vedligeholdelse af applikationer, er udviklings-, test- og produktionsmiljø adskilt, både når det gælder databaseservere og applikationsservere.
I alle de systemer hvor KIMIK iT ikke drifter produktionsdata, ligger produktionsservere hos systemejeren selv, typisk i deres eget domæne. Test- og general prøve systemer, der ligger hos systemejeren selv, vil typisk anvende produktionsdata, alt afhængigt af hvad anvendelsen foreskriver, og hvad systemejeren selv ønsker.
Der kan både forefindes testsystemer i KIMIK iT's domæne og i systemejerens eget domæne, i det sidste tilfælde, vil det være foranlediget af et behov for, at systemejeren kan teste funktionalitet med produktions lignende data. I alle de systemer, hvor KIMIK iT ikke drifter produktionsdata, vil data i testsystemer i KIMIK iT's eget domæne være anonymiseret.
Data i udviklingsmiljøer vil, i alle de systemer hvor KIMIK iT ikke drifter produktionsdata, være anonymiseret.
Tildeling af adgang til systemejerens domæner og miljøer, udføres udelukkende af systemejeren selv, og kun medlemmer i relevante udviklingsteams, der har behov for adgang, anmoder om adgang. Adgange revurderes ved bemandingsændringer hos KIMIK iT, adgange udløber automatisk ifølge systemejerens egne retningslinjer.

Personoplysninger i udviklings- og testmiljø
I de databasesystemer hvor KIMIK iT udfører udvikling og vedligeholdelse af applikationer, er udviklings, test og produktionsmiljø adskilt.
Udviklingsservere og testservere der er hostet hos og af KIMIK iT, vil som udgangspunkt indeholde anonymiserede data. I de tilfælde hvor KIMIK iT selv drifter produktionsmiljøer, vil disse og evt. test miljøer, der fordrer produktionslignende data, naturligvis indeholde produktionsdata.

Supportopgaver
Udviklere, supportere og andre, der tager del i 1. 2. eller 3. level support har adgang til de informationer, der leveres i supportsagen samt driftsmiljø for applikation og databaseservere.
Dedikerede supportere vil, i kraft af deres opgaver på tværs af kunder, have adgang til flere systemer for at kunne udføre deres supportopgaver.
Håndtering af personoplysninger ved supportopgaver sker altid ud fra et arbejdsbetinget behov og på opfordring af systemejeren.

A.15: Leverandørforhold

KIMIK iT benytter følgende underdatabehandlere:
Microsoft:

- Outlook og Azure DevOps anvendes til kundesupport, hvori der kan indgå persondata, som bliver slettet kontinuerligt i et givet interval.
- Outlook anvendes til fremsendelse af datagrundlag med persondata ifm. ad-hoc opgaver.

Zendesk:

- Zendesk anvendes til kundesupport med persondata.

De underdatabehandleraftaler der er indgået, vil som minimum pålægge de pågældende underdatabehandlere de samme databeskyttelsesforpligtelser som databehandleren selv er pålagt.
Databeskyttelsesforpligtelser pålagt databehandleren er specificeret i de enkelte databehandleraftaler.

Underdatabehandleraftale og instruks
Godkendelse af underdatabehandlere:
De underdatabehandleraftaler, der er indgået, vil i alle tilfælde være indgået i forbindelse med en databehandleraftale, og dermed vil godkendelse af underdatabehandlere ligeledes være specificeret i de pågældende databehandleraftaler.
I fald den konkrete databehandleraftale giver tilladelses til anvendelse af underdatabehandlere, vil databehandleren (KIMIK iT) altid følge den pågældende databehandleraftales instrukser hvad angår godkendelse af underdatabehandlere, men vil som minimum søge skriftlig godkendelse 1 måned inden aftaleindgåelse til anvendelse af en underdatabehandler. Således har dataansvarlig altid mulighed for at gøre indsigelse overfor nye og ændrede underdatabehandlere, inden de tages i brug.
Godkendelsesprocessen af underdatabehandlere forestås og gennemføres af den forretningsansvarlige og godkendes af direktøren og den dataansvarlige.

Ændringer i godkendte underdatabehandlere:
Ligesom ved godkendelse af underdatabehandlere, vil ændringer i anvendte underdatabehandlere i alle tilfælde være indgået i forbindelse med en databehandleraftale, og dermed vil godkendelse af underdatabehandlere ligeledes være specificeret i de pågældende underdatabehandleraftaler. Og i øvrigt opfylde samme forpligtelser som for godkendelsen af underdatabehandlere specificeret ovenfor.
Ændringsprocessen af underdatabehandlere forestås og gennemføres af den forretningsansvarlige og godkendes af direktøren og den dataansvarlige.

Oversigt over godkendte underdatabehandlere:
I forhold til nedenstående anførte tilsyn vil tilsynet af enhver underdatabehandler altid som minimum inkludere en underskrevet revisorerklæring, evt. ISAE3000 eller tilsvarende. Type af erklæring er anført under type af tilsyn.

Tilsyn med underdatabehandlere:
De underdatabehandlere der er indgået aftale med, vil i alle tilfælde være indgået i forbindelse med en databehandleraftale. Tilsyn og revision af underdatabehandlere bliver som minimum foretaget én gang om året på en ikke forudbestemt dato. Typen af revision for den pågældende underdatabehandler er anført i afsnittet ovenfor.
I forbindelse med enhver databehandleraftale der indeholder specifikke instrukser til, hvordan dataansvarlige udfører tilsyn og revision med databehandleren, vil instrukserne angående tilsyn og revision blive rettet videre mod evt. underdatabehandlere. Således vil enhver underdatabehandler som minimum skulle opfylde samme instrukser ifm. tilsyn og revision som databehandler gør over for dataansvarlige, dog kun i det omfang det er relevant for underdatabehandler.
I forhold til anførte tilsyn i ovenstående afsnit, vil tilsynet af enhver underdatabehandler altid som minimum inkludere en underskrevet revisorerklæring, evt. ISAE3000 eller tilsvarende.
Tilsyn og revision af underdatabehandlere forestås af den forretningsansvarlige med evt. ekstern hjælp i det omfang, underdatabehandleraftalen betinger dette.

A.16: Styring af informationssikkerhedsbrud

KIMIK iT har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at KIMIK iT er blevet opmærksomme på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at foretage vurdering af, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

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

Beredskabsplaner

KIMIK iT har etableret beredskabsplaner, således at KIMIK iT rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. KIMIK iT har etableret et kriseberedskab, der træder i kraft i disse tilfælde. Organisering af kriseberedskabsgruppe er etableret, og der er indført retningslinjer for aktivering af kriseberedskabet.

KIMIK iT har udformet detaljerede beredskabsplaner og planer for retablering af systemer og data, der blandt andet sikrer personuafhængighed i forbindelse med aktivering af beredskabet og retableringen. Planerne er i kopi opbevaret sikret uden for KIMIK iT's it-systemer. Planerne afprøves og revideres løbende i forbindelse med ændringer i systemer mv.

A.18: Overensstemmelse

Indgåelse af databehandleraftale med dataansvarlige
Databehandleraftaler ligger i ComplyCloud platformen.

KIMIK iT har indført politikker og procedurer for indgåelse af databehandlingsaftaler, der sikrer, at KIMIK iT i tilknytning til kundekontrakten indgår en databehandleraftale, der angiver betingelserne for behandling af personoplysninger på vegne af den dataansvarlige. KIMIK iT anvender en skabelon for databehandleraftaler i overensstemmelse med de tjenester, der leveres, herunder information om brugen af underdatabehandlere. Databehandleraftalerne er underskrevet og opbevares elektronisk.

Instruks for behandling af personoplysninger
KIMIK iT har indført politikker og procedure, der sikrer, at KIMIK iT handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedure, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske, herunder hvem der hos den dataansvarlige kan give bindende instruks til KIMIK iT. Proceduren sikrer desuden, at KIMIK iT informerer den dataansvarlige, når denne instruks er i strid med databeskyttelseslovgivningen.

Bistand til den dataansvarlige
KIMIK iT har indført politikker og procedurer, der sikrer, at KIMIK iT kan bistå den dataansvarlige med at opfylde denne forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.
KIMIK iT har indført politikker og procedurer, der sikrer, at KIMIK iT kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 34-36 om konsekvensanalyser.
KIMIK iT har indført politikker og procedurer, der sikrer, at KIMIK iT kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige. KIMIK iT giver desuden mulighed for at bidrage til revisor, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

Sletning og tilbagelevering af personoplysninger
KIMIK iT har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Overførsel af personoplysninger til tredjelande
KIMIK iT har indført politikker og procedurer, der sikrer, at overførslen af personoplysninger til underdatabehandlere i lande uden for EU sker i henhold til EU-US Privacy, standardkontrakt eller andet gyldigt overførselsgrundlag og ifølge instruks fra den dataansvarlige.

Afprøvning, vurdering og evaluering
KIMIK iT har indført procedurer og regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerhed.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Den dataansvarlige er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed opfylde databeskyttelseslovgivningen:

- Den dataansvarlige har ansvaret for at sikre, at administratorernes brug af relevante systemer og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen.
- Den dataansvarlige styrer brugerrettighederne i relevante systemer, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.

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 KIMIK iT A/S' beskrivelse af IT-løsninger 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 KIMIK iT A/S, 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. 30. november 2024.

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

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

For de ydelser, som Microsoft leverer, har vi modtaget SOC 2 rapport fra uafhængig revisor for perioden 1. april 2023 til 31. marts 2024 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Zendesk leverer, har vi modtaget SOC 2 rapport fra uafhængig revisor for perioden 1. april 2023 til 31. marts 2024 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Denne underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i KIMIK iT A/S' beskrivelse af IT-løsninger og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos KIMIK iT A/S, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

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

En afvigelse foreligger, når:

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

Risikovurdering

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af KIMIK iT baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har foretaget inspektion af KIMIK iT's risikovurdering og observeret, at der er taget stilling til en række trusler, heriblandt trusler mod persondatasikkerheden og de registreredes rettigheder. Vi har yderligere observeret, at risikovurdering er opdateret 12. juli 2024. Vi har inspiceret KIMIK iT's risikovurdering og observeret, at KIMIK iT's IT-systemer og processer er inkluderet. Yderligere har vi observeret, at risikovurderinger mitigeres ud fra en betragtning af konsekvens, sandsynlighed og implementerings-omkostninger.	Ingen afvigelser konstateret.

A.5: Informationssikkerhedspolitikker

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politikker for informationssikkerhed og databeskyttelse ▶ KIMIK iT har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ KIMIK iT har udarbejdet og implementeret politikker, indeholdende en forpligtelse til, at opnå overholdelse af relevante krav, love og forskrifter i forhold til anvendelse af Persondata. ▶ KIMIK iT har udarbejdet følgende Persondatapolitikker: o Persondatapolitik for ansøgere og rekruttering o Persondatapolitik til brug for hjemmeside o Persondatapolitik til medarbejdere	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's informationssikkerhedspolitik. Vi har observeret, at KIMIK iT's politik er ledelsesgodkendt af KIMIK iT's ledelse. Vi er på forespørgsel blevet informeret om, at KIMIK iT's medarbejdere er bekendt med informationssikkerhedspolitikken, men at den endnu ikke er gennemgået af alle medarbejdere. Vi har inspiceret KIMIK iT's persondatapolitik og observeret, at der er krav om overholdelse af gældende lovgivning. Yderligere har vi observeret, at persondatapolitikken for medarbejdere og hjemmeside er implementeret og opdateret, samt at persondatapolitikken for ansøgere og rekruttering af medarbejdere er implementeret.	Vi har konstateret, at KIMIK iT har udarbejdet en informationssikkerhedspolitik, men at den ikke er gennemgået af alle medarbejdere. Ingen yderligere afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ KIMIK iT's informationssikkerhedspolitik bliver gennemgået og, hvis nødvendigt, opdateret minimum en gang årligt. ▶ KIMIK iT's informationssikkerhedspolitik er tilgængelig for alle medarbejdere. ▶ KIMIK iT's KIMIK iT holder minimum årligt alle Persondatapolitikker opdaterede.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's informationssikkerhedspolitik og observeret, at den skal gennemgås årligt. Vi har inspiceret informationssikkerhedspolitikken og observe-ret, at den senest er gennemgået og opdateret i september 2024. Vi har observeret, at informationssikkerhedspolitikken er til-gængelig for KIMIK iT's medarbejdere. Vi har inspiceret KIMIK iT's persondatapolitikker og observeret, at de bliver revideret årligt, og at de senest er opdateret i juni og juli 2024.	Ingen afvigelser konstateret.

A.6: Organisering af informationssikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Roller og ansvarsområder ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed. ▶ Databehandler har dokumenteret og etableret ledelsesstyring af databeskyttelse(politikken. ▶ 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.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's ISMS-opsætning og observeret, at der er etableret ledelsesstyring af informationssikkerhed og databeskyttelse. Vi har inspiceret KIMIK iT's ISMS-opsætning og observeret, at roller og ansvar relevant for informationssikkerhed og databe-skyttelse er defineret og uddelegeret. Vi har inspiceret KIMIK iT's skabelon for databehandleraftaler og observeret, at der er angivet en kontaktperson hos KIMIK iT. Vi har stikprøvevis inspiceret databehandleraftaler og observe-ret, at der er angivet en kontaktperson hos KIMIK iT.	Ingen afvigelser konstateret.
Udpegelse af databeskyttelsesrådgiveren ▶ KIMIK iT har udpeget en databeskyttelsesrådgiver.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi er på forespørgsel blevet informeret om, at KIMIK iT har udpeget en databeskyttelsesrådgiver. Vi har inspiceret, at databeskyttelsesrådgiveren er underlagt en fortrolighed og tavshedspligt.	Ingen afvigelser konstateret.
Databeskyttelsesrådgiverens stilling ▶ Databehandleren har udarbejdet og implementeret en beskrivelse af databeskyttelsesrådgiverens stilling. ▶ Databehandleren inddrager databeskyttelsesrådgiveren vedrørende beskyttelse af personoplysninger.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret beskrivelsen af databeskyttelsesrådgiverens opgavebeskrivelse.	Vi har konstateret, at databeskyttelsesrådgiveren er den samme person, som er direktør, hvorfor databeskyttelsesrådgiveren ikke er uafhængig. Ingen yderligere afvigelser konstateret.

A.6: Organisering af informationssikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Databeskyttelsesrådgiveren er underlagt tavshedspligt/fortrolighed.	Vi har observeret, at KIMIK iT's databeskyttelsesrådgiver er involveret i en række informationssikkerhedsområder samt ansvarlig i databehandleraftaler. Vi har inspiceret, at databeskyttelsesrådgiveren er underlagt en fortrolighed og tavshedspligt. Vi har observeret at databeskyttelsesrådgiveren er den samme person, som er direktør, hvorfor databeskyttelsesrådgiveren ikke er uafhængig.	
Databeskyttelsesrådgiverens opgaver ▶ Databehandleren har udarbejdet og implementeret en opgavebeskrivelse af databeskyttelsesrådgiverens opgaver.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret beskrivelsen af databeskyttelsesrådgiverens opgavebeskrivelse. Vi har inspiceret, at databeskyttelsesrådgiveren er den samme person, som er direktør, hvorfor databeskyttelsesrådgiveren ikke er uafhængig.	Vi har konstateret, at databeskyttelsesrådgiveren er den samme person, som er direktør, hvorfor databeskyttelsesrådgiveren ikke er uafhængig. Ingen yderligere afvigelser konstateret.
Funktionsadskillelse ▶ Databehandlerens modstridende funktioner og ansvarsområder er adskilt for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af data.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret en oversigt over brugere og deres rettigheder i relevante systemer og observeret, at KIMIK iT begrænser adgang og rettigheder i forhold til et arbejdsbetinget behov.	Ingen afvigelser konstateret.

A.6: Organisering af informationssikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik for mobilt udstyr ▶ KIMIK iT, databehandleren har udarbejdet og implementeret en politik og understøttende sikkerhedsforanstaltninger til styring af risici for personoplysninger, der opstår ved anvendelse af mobilt udstyr.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's informationssikkerhedspolitik og observeret, at beskyttelse af mobilt udstyr bliver administreret af tredje part. Vi har inspiceret KIMIK iT's VPN-opsætning og observeret at der er implementeret to-faktor autentifikation på mobilt udstyr.	Ingen afvigelser konstateret.
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. ▶ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse ([SHA-2 & 256 bit]) ▶ Fjernadgang skal foregå via to-faktor autentifikation ([SMS Passcode])	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's informationssikkerhedspolitik og observeret, at it-udstyr skal have installeret nyeste version af antivirus software. Vi har stikprøvevis inspiceret mobile enheder og observeret, at der er installeret anti-virus beskyttelse på enhederne. Vi har inspiceret dokumentation for KIMIK iT's VPN-konfiguration og observeret, at der er installeret passende kryptering. Vi har inspiceret KIMIK iT's VPN-opsætning og observeret, at der er implementeret to-faktor autentifikation.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Rekruttering af medarbejdere ▶ Databehandleren har implementeret screening af potentielle medarbejdere før ansættelse. ▶ Databehandleren har implementeret baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's beskrivelse for rekruttering og observeret, at der er formaliseret krav til baggrundstjek af kandidater. Vi er på forespørgsel blevet informeret om, at KIMIK iT ikke har haft nogle nyansættelser siden udarbejdelsen af deres procedure, hvorfor kontrolaktiviteten ikke har været mulig at teste.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for rekruttering af medarbejdere. Der har dog ikke været ansættelser siden udarbejdelse af proceduren. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og informationssikkerhed, i forlængelse af ansættelsen. ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. ▶ Databehandleren foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's informationssikkerhedspolitik og observeret at der er formelle krav til løbende træning i sikkerhed og persondata herunder introduktion til nye medarbejdere. Vi er på forespørgsel blevet informeret om, at KIMIK iT ikke har haft nogen nyansættelser siden deres implementering af proceduren, hvorfor kontrolaktiviteten ikke kunne testes. Vi har inspiceret interne referater og observeret, at træning i persondatasikkerhed har været på dagsordenen. Vi har observeret, at KIMIK iT har implementeret et system til løbende træning i IT- og persondatasikkerhed, som medarbejderne løbende gennemfører.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for uddannelse og instruktion af medarbejdere. Der har dog ikke været ansættelser siden udarbejdelse af proceduren. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren udfører løbende awareness-kampagner i form af, tests, mail og fællesmøder om databeskyttelse og informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret interne referater og observeret, at træning i persondatasikkerhed har været på dagsordenen. Vi har observeret, at KIMIK iT har implementeret et system til løbende træning i IT- og persondatasikkerhed, som medarbejderne løbende har gennemført diverse relevante tests i.	Ingen afvigelser konstateret.
Lovbestemt tavshedspligt ▶ Alle medarbejdere er underlagt lovbestemt tavshedspligt efter straffelovens bestemmelser.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's ansættelsesskabelon og observeret, at den indeholder et område om tavshedspligt, under og efter ansættelse. Vi har stikprøvevis inspiceret, at medarbejderne er underlagt tavshedspligt.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Alle medarbejdere har underskrevet en tavshedsaftale. ▶ Eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's ansættelsesskabelon og observeret, at den indeholder et område om tavshedspligt, under og efter ansættelse. Vi har stikprøvevis inspiceret, at medarbejderne er underlagt tavshedspligt. Vi er på forespørgsel blevet oplyst, at eksterne konsulenter og leverandører er underlagt tavshedspligt.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har stikprøvevis inspiceret, at eksterne leverandører er underlagt tavshedspligt.	
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Databehandleren har udarbejdet og implementeret en procedure for off-boarding af fratrådte medarbejdere. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's informationssikkerhedspolitik og observeret, at der er krav om returnering af fysiske aktiver med adgang til personoplysninger, samt fjernelse af adgange til systemer og services ved ophør af ansættelsesforholdet. Vi er på forespørgsel blevet informeret om, at KIMIK iT benytter en standard tjekliste ved ansættelsesstop. Vi har inspiceret dokumentation for KIMIK iT's off-boarding tjekliste og observeret, at den er udfyldt samt, at medarbejderens adgange er nedlagt i systemerne. Vi har observeret, at medarbejderne ved ansættelsesstop underskriver et fratrædelsesbrev, hvori der orienteres om gældende krav for fortrolighed og tavspligt efter ansættelse.	Ingen afvigelser konstateret.

A.8: Styring af aktiver

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's fortegnelse over behandlingsaktiviteter og observeret, at den indeholder ydelser samt dataansvarlige. Vi er på forespørgsel blevet informeret om, at fortegnelser over behandlingsaktiviteter opdateres løbende. Vi har inspiceret KIMIK iT's årshjul og observeret, at fortegnelser over behandlingsaktiviteter opdateres som minimum én gang årligt. Vi har inspiceret, at fortegnelsen er opdateret inden for det seneste år.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens ComplyCloud løsning.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's placering af fortegnelser over behandlingsaktiviteter og observeret, at de opbevares elektronisk.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi er på forespørgsel blevet informeret om, at KIMIK iT udleverer deres fortegnelse over behandlingsaktiviteter til Datatilsynet efter anmodning. Vi er på forespørgsel blevet informeret om, at der ikke har været nogen forespørgsel fra Datatilsynet om udlevering af fortegnelse	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for adgang til fortegnelsen. Der har dog ikke været nogen henvendelser fra datatilsynet i erklæringsperioden. Vi kan derfor ikke teste 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
	over behandlingsaktiviteter, hvorfor kontrolaktiviteten ikke har kunnet testes.	
Klassifikation af information ▶ Databehandleren informerer relevante medarbejdere om definitionen af personoplysninger, og hvordan de identificeres i forbindelse med awareness-træning/uddannelse samt i procedure for klassifikation af information.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for data klassifikation og observeret, at personoplysninger er defineret, og at dette kommunikeres ud til medarbejderne. Vi har observeret KIMIK iT's awarness træningsplatform og observeret, at der er træning vedrørende definition af personoplysninger. Vi har inspiceret KIMIK iT's awareness dokumentation og observeret, at medarbejderne har gennemført træning som omfatter dataklassifikation af personoplysninger.	Ingen afvigelser konstateret.
Styring af flytbare medier ▶ Databehandleren har udarbejdet og implementeret en procedure til styring af flytbare medier, herunder dokumenterer om der opbevares personoplysninger på flytbare medier. ▶ Databehandleren anvender krypteret flytbare medier til opbevaring af personoplysninger.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's politik for styring af flytbare medier og observeret, at der er krav om kryptering på enheder, der indeholder personoplysninger. Vi har inspiceret KIMIK iT's opsætning af kryptering på flytbare medier og observeret, at enheder, der indeholder personoplysninger, er krypteret.	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
Bortskaffelse af medier ▶ Databehandleren har udarbejdet og implementeret en procedure for bortskaffelse af medier, hvor der opbevares personoplysninger på forsvarlig vis. ▶ Databehandleren bortskaffelse selv medier på forsvarlig vis, herunder medier hvor personoplysninger er opbevaret, som sikrer at opbevaret personoplysninger ikke kan tilgås.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's politik for bortskaffelse af medier og observeret, at der er krav om sikker bortskaffelse på medier med personoplysninger. Vi er på forespørgsel blevet informeret om, at der ikke har været tilfælde med bortskaffelse af medier med personoplysninger efter implementeringen af KIMIK iT's politik, hvorfor kontrolaktiviteten ikke kunne testes.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for bortskaffelse af medier med personoplysninger. Der har dog siden udarbejdelse af proceduren ikke været nogen tilfælde af bortskaffelse. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
Fysiske medier under transport ▶ Databehandleren anvender et system for registrering af ind- og udgående fysiske medier indeholdende personoplysninger. ▶ Databehandleren krypterer fysiske medier der indeholder personoplysninger under transport.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's katalog over IT-aktiver og observeret at KIMIK iT har implementeret en oversigt over aktiver, hvortil der er placeret en ejer. Vi har inspiceret KIMIK iT's aktiver og observeret, at der er installeret passende kryptering på enheder, der flyttes.	Ingen afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Brugerregistrering og -afmelding ▶ Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for brugeroprettelse og observeret, at brugere oprettes med autoriseret godkendelse, og at adgange tildeles ud fra et arbejdsbetinget behov. Vi har inspiceret KIMIK iT's procedure for sletning af brugere og observeret, at, at brugere nedlægges ved fratrædelse, eller når der er væsentlige ændringer i arbejdsforholdet. Vi er på forespørgsel blevet informeret om, at KIMIK iT ikke har ansat nye medarbejdere siden deres implementering af procedure for brugeroprettelser, hvorfor kontrolaktiviteten ikke kunne testes. Vi er på forespørgsel blevet informeret om, at KIMIK iT udfylder en kontrolliste for nedlæggelse af brugeradgange ved fratrædelser. Vi har inspiceret dokumentationen for brugernedlæggelser og observeret, at kontrollisten er sendt til ansvarlige vedkommende, udfyldt, og at brugeren er nedlagt i alle systemer og services.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for brugerregistrering. Der har dog ikke været ansættelser siden udarbejdelse af proceduren. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
Tildeling af brugeradgange ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for brugeroprettelse og observeret, at brugere oprettes med autoriseret godkendelse, og at adgange tildeles ud fra et arbejdsbetinget behov.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for brugerregistrering. Der har dog ikke været ansættelser siden udarbejdelse af proceduren. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.9: Adgangsstyring

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi er på forespørgsel blevet informeret om, at KIMIK iT ikke har ansat nye medarbejdere siden deres implementering af brugeroprettelser, hvorfor kontrolaktiviteten ikke kunne testes.	
Styring af privilegerede adgangsrettigheder ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for brugeroprettelse og observeret, at brugere oprettes med autoriseret godkendelse, og at adgange tildeles ud fra et arbejdsbetinget behov. Vi er på forespørgsel blevet informeret om, at KIMIK iT ikke har ansat nye medarbejdere siden deres implementering af brugeroprettelser, hvorfor kontrolaktiviteten ikke kunne testes. Vi har inspiceret KIMIK iT's udtræk over brugere med privilegerede adgange og observeret, at listen er begrænset og kun til medarbejdere med et arbejdsbetinget behov.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for styring af privilegerede adgangsrettigheder. Der har dog ikke været nogle nye brugere med privilegerede adgangsrettigheder siden udarbejdelse af proceduren. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
Gennemgang af brugeradgangsrettigheder ▶ Der foretages kvartalsvis gennemgang af brugere og brugerrettigheder.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har observeret KIMIK iT's politik for adgangsstyring og observeret, at brugeradgange skal revideres hvert halve år. Vi har inspiceret KIMIK iT's gennemgang af brugere og observeret at KIMIK iT har gennemgået brugeradgange i deres systemer indenfor det sidste halve år.	Ingen afvigelser konstateret.
Brug af hemmelig autentifikationsinformation		

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
▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's konfiguration for adgangskoder og observeret, at der er sat passende minimumskrav for adgangskoder. Vi har observeret, at brugere med privilegerede adgange bruger to faktor autentifikation for at logge på systemer.	Ingen afvigelser konstateret.
Procedure for sikkert log-on ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's konfiguration for adgangskoder og observeret, at der er sat passende minimumskrav for adgangskoder. Vi har observeret, at brugere med privilegerede adgange bruger to faktor autentifikation for at logge på systemer.	Ingen afvigelser konstateret.

A.10: Kryptografi

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Politik for anvendelse af kryptografi - Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. Politikken definerer styrken og protokollen for kryptering. - Bærbare medier med personlysninger er krypteret. - Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's krypteringspolitik og observeret, at der er defineret krav til styrke samt protokol for kryptering. Vi har observeret, at KIMIK iT's har krypteret deres enheder med kryptering i overensstemmelse med deres krypteringspolitik. Vi har inspiceret dokumentation for at KIMIK iT anvender kryptering ved transmission af personoplysninger via e-mail.	Ingen afvigelser konstateret.
Administration af nøgler - Krypteringsnøgler opbevares på en lokation der er forskellig fra hvor krypteret data er lagret.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi er på forespørgsel blevet informeret om, at krypteringsnøgler er placeret så autoriserede medarbejdere kan tilgå dem, samt at der er redundans i opsætningen således, at krypteringsnøglerne altid er tilgængelige. Vi har inspiceret dokumentation for, at krypteringsnøgler opbevares på anden lokation, end hvor data er lagret.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang. ▶ Alle adgange registreres og logges. ▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's sikkerhedsbeskrivelse for fysisk sikkerhed og observeret, at der er krav om fysisk adgangskontrol, samt at deres lokation er opdelt i forskellige adgangszoner. Vi har inspiceret dokumentation for at medarbejdere registreres når de får udleveret adgangsmuligheder til KIMIK iT's lokationer. Vi har inspiceret KIMIK iT's log overvågning for den fysiske adgangskontrol og observeret, at adgange logges. Vi har inspiceret, at KIMIK iT har opsat halvårlig kontrol for fysisk adgang.	Ingen afvigelser konstateret.
Fysisk sikkerhed ▶ Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. ▶ Databehandleren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum omfattende følgende forhold: ○ Bygning ○ Gulve ○ Klima ○ Strøm ○ Adgang ○ Alarmmonitorering ○ Brandslukning ○ Kabling	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har på forespørgsel fået oplyst, at KIMIK iT kun opbevarer personoplysninger på servere i Nuuk. Vi har inspiceret, at KIMIK iT har indgået aftale med ekstern virksomhed om vagt og overvågning. Vi har inspiceret dokumentation for, at KIMIK iT's serverrum efterlever krav i forhold til beskyttelse mod eksterne og miljømæssige trusler.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring		
Kontrolmål ▶ *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og personoplysninger, herunder informations- og databehandlingsfaciliteter – GDPR, artikel 28, stk. 3, litra c.* ▶ *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen – GDPR, artikel 28, stk. 3, litra c.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Vedligeholdelse af udstyr ▶ Vedligeholdelse af udstyr følger en vedligeholdelsesplan og udføres af autoriseret personale.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's vedligeholdelsesplan og observeret, at der forekommer opgaver for både medarbejderes enheder samt fysiske servere, som løses løbende. Vi har observeret, at vedligeholdelsesplanen bliver gennemgået årligt. Vi har inspiceret dokumentation for, at KIMIK iT vedligeholder deres udstyr.	Ingen afvigelser konstateret.
Sikring af udstyr og aktiver for organisationen ▶ Udstyr uden for organisationen må ikke efterlades uden opsyn på offentlige steder. ▶ Adgang til organisationens server fra fjernarbejdspladser, kan kun tilgås via VPN-adgang.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for it-udstyr og observeret, at der er krav om fjernadgang samt observering af it-udstyr i offentlige rum. Vi har observeret, at adgang til KIMIK iT's infrastruktur på deres netværk sker igennem en sikret VPN-forbindelse.	Ingen afvigelser konstateret.
Reparation og service samt bortskaffelse af it-udstyr ▶ Databehandleren bortskaffer it-udstyr ved fysisk destruktion af databærende medier. ▶ Databehandleren foretager sikker sletning af data på databærende medier (overskrivning/forvanskning, kryptering...)	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for bortskaffelse af IT-udstyr og observeret, at der er krav til sikker sletning og destruering af IT-udstyr.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for reparation, service og bortskaffelse af medier med personoplysninger. Der har dog siden udarbejdelse af proceduren ikke været tilfælde af bortskaffelse. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har på forespørgsel fået oplyst, at KIMIK iT foretager en sikker sletning af IT-udstyr med personoplysninger når det ikke længere skal anvendes. Vi har på forespørgsel fået oplyst, at KIMIK iT ikke har bortskaffet IT-udstyr siden implementering af deres procedure, hvorfor kontrolaktiviteten ikke kunne testes.	
Politik for ryddeligt skrivebord og blank skærm - Skærmlås aktiveres automatisk og låses efter 10 min. - Medarbejdere skal aktivere skærmlås, når klienten forlades. - Fysisk materiale med personoplysninger opbevares i aflåst skab når materialet forlades.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's politik for ryddeligt skrivebord og låst skærm og observeret, at der er opsat en automatisk skærmlås på enheder, der er inaktive. Vi har observeret, at medarbejderne er instrueret i at låse deres enheder, når de forlader deres arbejdsstation. Vi har observeret, at fysiske følsomme oplysninger opbevares i et sikret aflåst skab på KIMIK iT's lokationer.	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 ▶ Databehandler fører en oversigt over systemsoftware/tredjepartsprogrammer som vedligeholdes og opdateres løbende. ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende. ▶ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed. – automatisk- eller manuel overvågningsproces.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's vedligeholdelsesplan og observeret, at der forekommer opgaver for både medarbejderes enheder samt fysiske servere, som løses løbende og kontinuerligt. Vi har på forespørgsel fået oplyst, at opdateringer sker på fastlagte tidspunkter. Vi har inspiceret, at KIMIK iT holder en ajourført liste over systemsoftware og tredjepartsprogrammer. Vi har inspiceret KIMIK iT's konfiguration for opdateringer og stikprøvevis observeret, at systemsoftware er opdateret.	Ingen afvigelser konstateret.
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateret med seneste version.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's vedligeholdelsesplan og observeret, at der forekommer opgaver for både medarbejderes enheder samt fysiske servere, som løses løbende og kontinuerligt. Vi har inspiceret KIMIK iT's dokumentation for virus beskyttelse og observeret at der er installeret antivirus-software på både medarbejderenheder og servere.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sikkerhedskopiering og retablering af data ▶ Der foretages dagligt backup af systemer og data. ▶ Der udføres restore-tests mindst en gang årligt.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har på forespørgsel fået oplyst, at der foretages backup på daglig basis. Vi har inspiceret KIMIK iT's dokumentation for daglig backup og observeret, at backup tages dagligt. Vi har på forespørgsel fået oplyst, at der laves restore test to gange årligt. Vi er på forespørgsel blevet oplyst om, at KIMIK iT ikke kan dokumentere deres gennemførsel af genetablering af backup.	Vi har konstateret, at KIMIK iT ikke kan dokumentere at have udført restore test. Ingen yderligere afvigelser konstateret.
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges. ▶ Databehandler monitorerer og logger netværkstrafik. ▶ Loggen slettes efter den fastsatte retentionsperiode.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's politik for adgangsstyring og observeret, at der er krav om adgangslogning. Vi har observeret, at adgangsforsøg og ændringer logges. Vi har observeret, at KIMIK iT har opsat log overvågning på deres netværk. Vi har observeret at log data slettes efter den fastsatte retentionsperiode.	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
Overvågning ▶ Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. ▶ Databehandleren notificeres om identificeret alarmer og følger op herpå.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's dokumentation for log overvågning og observeret, at deres infrastruktur overvåges. Vi har observeret, at alarmer via log overvågning på servere udløser en notifikation til relevant personale, som manuelt følger op på en given alarm.	Ingen afvigelser konstateret.
Sårbarhedsscanning ▶ Der udføres årligt en sårbarhedsscanning af databehandlerens netværk. Resultatet dokumenteres i en rapport ▶ Databehandleren gennemgår rapporten og følger op på konstateret svagheder. ▶ Databehandler håndtere/mitigere eventuelle sårbarheder ud fra en risikovurdering. ▶ Databehandler har dokumenteret deres håndtering/migrering af fundne sårbarheder.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for sårbarhedsscanninger og observeret, at der foretages regelmæssige sårbarhedsscanninger. Vi har inspiceret KIMIK iT's sårbarhedsscanningsrapport og observeret, at resultater kan dokumenteres. Vi har på forespørgsel fået oplyst, at KIMIK iT har taget stilling til resultaterne i rapporten, og mitigeret de kritiske resultater, ud fra en risikovurdering. Vi har observeret, at KIMIK iT er i stand til at dokumentere deres mitigerende handlinger af sårbarheder fra deres scanninger.	Ingen afvigelser konstateret.

A.13: Kommunikationssikkerhed

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Netværkssikkerhed ▶ Netværks topologien er struktureret efter best-practice principper, hvilket betyder at servere, som driver applikationer ikke kan nås direkte fra internettet. ▶ Databehandlerens netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet. ▶ Databehandleren anvender kendte netværksteknologier og mekanismer (Firewall/Intrusion DetectionSystem/Intrusion Prevention System) for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's netværkstegning og observeret, at best practice standarder følges. Vi har observeret, at netværket er segmenteret. Vi har inspiceret KIMIK iT's dokumentation for netværksbeskyttelse og observeret, at netværket er beskyttet med en IPS (Intrusion Prevention System) funktion.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall korrekt efter best-practice standard. ▶ Databehandler anvender kun services/porte, som de har behov for. ▶ Firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's netværkstegning og observeret, at best practice standarder følges. Vi har observeret, at netværket er segmenteret. Vi har inspiceret dokumentation for, at KIMIK iT har opsat deres firewall hensigtsmæssigt og yderligere observeret, at KIMIK iT regelmæssigt tester deres firewall.	Ingen afvigelser konstateret.
Eksterne kommunikationsforbindelser ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og VPN. ▶ Udveksling af personoplysninger via e-mail, sker vha. SikkerMail-løsning. ▶ Eksterne kommunikationsforbindelser er krypteret.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for kommunikationsforbindelser og observeret, at fjernadgang sker via en sikret VPN-forbindelse.	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 har inspiceret KIMIK iT's krypteringspolitik og observeret, at der er krav til minimums kryptering ved eksterne kommunikationsforbindelser. Vi har observeret, at det kun er autoriserede medarbejdere, som kan tilgå KIMIK iT's netværk fra en fjerntliggende placering. Vi har inspiceret KIMIK iT's dokumentation for fjernadgang og observeret, at det sker via en sikret VPN-forbindelse. Vi har inspiceret dokumentation for, at KIMIK iT har implementeret krypteret e-mail.	

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
Analyse og specifikation af informationssikkerhedskrav ▶ Informationssikkerhedskrav og krav til behandling af personoplysninger inddrages i en tidlig vurdering af nye projekter/systemer.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har stikprøvevis inspiceret, at KIMIK iT inddrager informationssikkerhedskrav og krav til behandling af personoplysninger i udviklingsprojekter.	Ingen afvigelser konstateret.
Udvikling og vedligeholdelse af systemer ▶ KIMIK iT arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelses opgaver, der er defineret i "Politik for sikkerhedsforanstaltninger til beskyttelse af personoplysninger". ▶ Der foretages, i det omfang systemejeren ønsker det, jævnlige reviews af kundernes applikationer, hvor evt. anbefalede tiltag tages videre til systemejeren. Disse tiltag kan være af funktion, vedligehold, licens eller sikkerhedsmæssig karakter.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's politik for sikkerhedsforanstaltninger til beskyttelse af personoplysninger og observeret, at privatliv og sikkerhed er en integreret del af arkitektur, design og udvikling. Vi har inspiceret KIMIK iT's politik for personoplysninger i testmiljø og observeret, at KIMIK iT så vidt muligt undgår at bruge personoplysninger i udviklingsarbejdet. Vi har observeret, at kundernes systemer jævnligt revideres.	Vi har konstateret, at KIMIK iT's politik for personoplysninger i udviklingsarbejdet ikke udelukker brugen af personoplysninger. Ingen yderligere afvigelser konstateret.
Informationssikkerhed i udvikling og ændringer ▶ KIMIK iT 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 KIMIK iT's udviklere har adgang til kildekode.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's informationssikkerhedspolitik og observeret, at udviklingsopgaver sker ud fra et princip om privacy by design and default. Vi har inspiceret KIMIK iT's udviklingsmiljø og observeret, at det er muligt at rulle en version tilbage til en tidligere version i tilfælde af implementeringsfejl.	Ingen afvigelser konstateret.

A.14: Anskaffelse, udvikling og vedligeholdelse

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret KIMIK iT's politik for adgangsstyring og observeret, at der er krav om et arbejdsbetinget behov for adgang til systemer og services. Vi har observeret, at det kun er medarbejdere med et arbejdsbetinget behov, som har adgang til KIMIK iT's kildekode.	
Adskillelse af udviklings-, test og produktionsmiljø - Der er indført funktionsadskillelse mellem udvikling og drift. - Ændringer af funktionalitet testes, inden det sættes i drift. - Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. - Der benyttes et versionsstyringssystem som registrerer alle ændringer i kildekode.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har på forespørgsel fået oplyst, at test sker på KIMIK iT's egne servere, og at persondata aldrig forlader de dataansvarliges domæner. Vi har modtaget og inspiceret tegninger over systemmiljø og observeret, at der er adskillelse mellem test- og produktionsmiljø. Vi har modtaget og inspiceret dokumentation for, at ændringer testes inden de idriftsættes. Vi har inspiceret, at ændringer i kildekode registreres.	Ingen afvigelser konstateret.
Personoplysninger i udviklings- og testmiljø - Der anvendes som udgangspunkt anonymiseret data på udviklingsservere og testservere der er hostet hos og af KIMIK iT. I de tilfælde hvor KIMIK iT selv drifter produktionsmiljøer, vil disse og evt. test miljøer, der fordrer produktionslignede data, naturligvis kunne indeholde produktionsdata.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's dokumentation for test data, og observeret at data i udviklings- og testmiljøer er anonymiseret.	Ingen afvigelser konstateret.

A.14: Anskaffelse, udvikling og vedligeholdelse

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Supportopgaver ▶ Supporteres adgange og håndtering af personoplysninger ved supportopgaver sker ud fra support-tickets/mails og supporterens arbejdsbetingede behov.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi er på forespørgsel blevet informeret om, at alle henvendelser til KIMIK iT's support afdeling sker igennem et supportsystem. Vi har inspiceret KIMIK iT's politik for adgangsstyring og observeret, at adgange til systemer og services sker på baggrund af et arbejdsbetinget behov. Vi har inspiceret KIMIK iT's dokumentation for supportopgaver og observeret, at de behandles af autoriserede medarbejdere.	Ingen afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandlers indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret databehandleraftale med underdatabehandlere og observeret, at underdatabehandleren er underlagt de samme databeskyttelsesforpligtelser som KIMIK iT. Vi har inspiceret databehandleraftale med underdatabehandlere og observeret, at underdatabehandleraftaler er underskrevet i bedst muligt omfang. Vi har inspiceret databehandleraftale med underdatabehandlere og observeret, at der fremgår information om brugen af underdatabehandlere.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's standardskabelon for databehandleraftaler og observeret, at den indeholder brug af underdatabehandlere. Vi har stikprøvevis inspiceret, at underdatabehandlere fremgår af databehandleraftaler med kunder.	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere ▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere. ▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's standardskabelon for databehandleraftaler og observeret, at ændringer skal varsles 30 dage før, ændringer træder i kraft.	Ingen afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Dataansvarlig har mulighed for at gøre indsigelse vedr. udskiftning af underdatabehandler. ▶ Ved udskiftning af underdatabehandler skal databehandleren have en ny forudgående specifik skriftlig godkendelse fra dataansvarlig.	Vi har observeret, at KIMIK iT underretter den dataansvarlige ved ændringer af underdatabehandler. Vi har inspiceret KIMIK iT's, databehandleraftaler, med de dataansvarlige og observeret, at ændringer er dokumenteret og godkendt inden implementering af ny underdatabehandler. Vi har inspiceret KIMIK iT's standard skabelon for databehandleraftaler og observeret, at den dataansvarlige har mulighed for at gøre indsigelse ved ændring af underdatabehandler.	
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering. ▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for tilsyn af underdatabehandlere og observeret, at der skal ske et årligt tilsyn. Vi har inspiceret, at KIMIK iT udfører tilsyn ud fra en risikobaseret tilgang. Vi har observeret, at KIMIK iT har modtaget tilsynsmateriale fra deres underdatabehandlere.	Ingen afvigelser konstateret.

A.16: Styring af informationssikkerhedsbrud

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Ansvar og procedurer ▶ Der er fastlagt ledelsesansvar og roller i forbindelse med brud på persondatasikkerheden. ▶ Databehandleren har implementeret procedure for brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for styring, at informationssikkerhedsbrud og observeret, at der er etableret ledelsesansvar og rollefordeling i forbindelse med informationssikkerhedsbrud. Vi har yderligere observeret, at der er udarbejdet en procedure for håndtering af brud på persondatasikkerheden. Vi har inspiceret KIMIK iT's log over brud på persondatasikkerhed og observeret, at den er tom, og har derfor ikke kunnet teste kontrollens implementering.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for styring af informationssikkerhedsbrud. Der har dog ikke været nogle brud på persondatasikkerheden siden udarbejdelsen af deres procedure. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for underretning om brud og observeret, at der er retningslinjer for underretning til de dataansvarlige ved identifikation af brud på persondatasikkerheden. Yderligere har vi observeret, at der er krav og retningslinjer for materiale og detaljer, som skal kommunikeres til de dataansvarlige. Vi har inspiceret KIMIK iT's procedure for styring af informationssikkerhed og observeret, at kommunikation mellem KIMIK iT og de dataansvarlige dokumenteres og gemmes i et sikkert system. Vi har inspiceret KIMIK iT's log over brud på persondatasikkerhed og observeret, at den er tom, og har derfor ikke kunnet teste kontrollens implementering.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for styring af informationssikkerhedsbrud. Der har dog ikke været nogle brud på persondatasikkerheden siden udarbejdelsen af deres procedure. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.16: Styring af informationssikkerhedsbrud		
Kontrolmål ▶ *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud og brud på persondatasikkerheden, herunder kommunikation om sikkerhedshændelser og –svagheder – GDPR, artikel 33, stk. 2.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for vurdering og identifikation af brud på persondatasikkerheden og observeret, at relevante elementer af brud på persondatasikkerheden skal analyseres af KIMIK iT's Incident Manager. Vi har inspiceret KIMIK iT's log over brud på persondatasikkerhed og observeret, at den er tom og har derfor ikke kunne teste kontrollens implementering.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for styring af informationssikkerhedsbrud. Der har dog ikke været nogle brud på persondatasikkerheden siden udarbejdelsen af deres procedure. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
Registrering af brud på persondatasikkerheden ▶ Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen. ▶ Databehandleren har udarbejdet og implementeret en procedure for erfaringsopsamling ved brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's procedure for erfaringsopsamling ved brud på persondatasikkerheden og observeret, at der efter et brud bliver gennemført en erfaringsopsamling af Incident Manageren. Vi har inspiceret KIMIK iT's log over brud på persondatasikkerhed og observeret, at den er tom, og har derfor ikke kunnet teste kontrollens implementering.	Vi har konstateret, at KIMIK IT har udarbejdet en procedure for styring af informationssikkerhedsbrud. Der har dog ikke været nogle brud på persondatasikkerheden siden udarbejdelsen af deres procedure. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, beredskabsplanerne er tidssvarende og effektive i kritiske situationer. ▶ Beredskabstest dokumenteres og evalueres.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's beredskabsplan og observeret, at den omfatter tilgængelighed og adgang til personoplysninger. Vi har observeret, at beredskabsplanen opdateres minimum én gang om året. Vi har inspiceret KIMIK iT's test af beredskabsplan og vurderet, at den ikke er tilstrækkeligt dokumenteret og evalueret.	Vi har konstateret, at test af beredskabsplanen ikke er tilstrækkeligt dokumenteret og evalueret. Ingen yderligere afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige ▶ Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ▶ Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. ▶ Databehandleraftaler underskrives og opbevares elektronisk. ▶ Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har på forespørgsel fået oplyst, at når der indgås en aftale med en kunde, indgås der samtidig en databehandleraftale, der refererer til aftalen. Databehandleraftalen dækker de ydelser, der leveres. Vi har inspiceret KIMIK iT's standard skabelon for indgåelse af databehandleraftaler og stikprøvevis observeret, at den er underskrevet, opbevares elektronisk samt omfatter brugen af underdatabehandlere.	Ingen afvigelser konstateret.
Instruks for behandling af personoplysninger ▶ Indgående databehandleraftaler indeholder en instruks fra den dataansvarlige. ▶ Databehandleren indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's standard skabelon for indgåelse af databehandleraftaler og stikprøvevis observeret, at den indeholder instruks fra den dataansvarlige.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger. ▶ Databehandlerens procedurer gennemgås og opdateres løbende og minimum en gang årligt. ▶ Databehandleren har implementeret egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har stikprøvevist inspiceret KIMIK iT's, databehandleraftaler med den dataansvarlige og observeret, at der alene udføres behandling som fremgår af instruks. Vi har inspiceret KIMIK iT's fortegnelse over behandlingsaktiviteter og observeret, at behandling sker på baggrund af instruks af den dataansvarlige.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for egenkontrol for efterlevelse af instruks for behandling af personoplysninger. Den har dog ikke været udført siden udarbejdelse af proceduren. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret KIMIK iT's årshjul og observeret, at procedure, databehandleraftaleskabelon og fortegnelse over behandlingsaktiviteter opdateres årligt Vi har inspiceret KIMIK iT's årshjul og observeret, at KIMIK iT har implementeret egenkontrol for efterlevelse af instruks. Vi har inspiceret KIMIK iT's instruks til medarbejderne og observeret, at den er opdateret.	
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig, i tilfælde hvor den dataansvarliges instruks, strider mod databeskyttelseslovgivningen. ▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's standard skabelon for indgåelse af databehandleraftaler og observeret, at KIMIK iT har krav til straks at underrette den dataansvarlige om ulovlig instruks. Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde af ulovlig instruks, hvorfor kontrolaktiviteten ikke kunne testes.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for underretning af den dataansvarlige ved ulovlig instruks. Der har dog ikke været tilfælde af ulovlig instruks siden udarbejdelse af proceduren. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
De registreredes rettigheder ▶ Databehandler har i databehandleraftalen en procedure for bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder. ▶ Det er muligt at give indsigt i alle oplysninger, der er registreret i den dataansvarliges systemer.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's standard skabelon for indgåelse af databehandleraftaler og observeret, at den omfatter bistand til den dataansvarlige. Vi har stikprøvevis inspiceret indgåede databehandleraftaler og observeret, at de indeholder en sektion for bistand til den dataansvarlige opfyldelse af de registreredes rettigheder, samt overholdelse af indsigtsretten.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for bistand til den dataansvarlige. Der har dog ikke været anmodet om bistand fra den dataansvarlige. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde, hvor KIMIK iT er blevet anmodet om bistand fra den dataansvarlige, hvorfor kontrollens implementering ikke kunne testes.	
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser ▶ I databehandleraftalen er der udarbejdet procedurer for bistand til dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevis inspiceret databehandlerens, databehandleraftaler med de dataansvarlige og observeret, at databehandleren har en procedure for at yde bistand til den dataansvarlige ved opfyldelse af de registreredes rettigheder.	Ingen afvigelser konstateret.
Revision og inspektion ▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandler bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har observeret, at KIMIK iT får udarbejdet en ISAE3000 erklæring som omfatter KIMIK iT's tekniske og organisatoriske foranstaltninger. Vi har stikprøvevist inspiceret indgåede databehandleraftaler og observeret, at de indeholder en sektion for bistand til den dataansvarlige heriblandt muligheden for fysisk tilsyn. Vi har stikprøvevist inspiceret indgåede databehandleraftaler og observeret, at de indeholder en sektion for bistand til den dataansvarlige heriblandt de nødvendige informationer, som der på forespørgsel af den dataansvarlige er blevet anmodet om. Vi er på forespørgsel blevet oplyst, at KIMIK iT, på anmodning, stiller de nødvendige informationer til rådighed for dataansvarlige og tilsynsmyndigheden.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for revision og inspektion. Der har dog ikke har været revision eller inspektion fra dataansvarlige eller tilsynsmyndighed. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har på forespørgsel fået oplyst, at der ikke har været revision eller inspektion af KIMIK iT fra dataansvarlige eller tilsynsmyndighed. Vi kan derfor ikke teste kontrollens effektivitet.	
Sletning af personoplysninger - Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har stikprøvevis inspiceret indgåede databehandleraftaler og observeret, at de indeholder en sektion for sletning eller tilbagelevering af personoplysninger ved ophør af gældende aftale efter instruks. Vi har på forespørgsel fået oplyst, at der ikke har været ophør af kundeaftaler det seneste år, hvorfor kontrolaktiviteten ikke kunne testes.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for sletning af personoplysninger. Der har dog ikke har været ophør af kundeaftaler det seneste år. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.
Tilbagelevering af personoplysninger - Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har stikprøvevis inspiceret indgåede databehandleraftaler og observeret, at de indeholder en sektion for sletning eller tilbagelevering af personoplysninger ved ophørelse af gældende aftale efter instruks. Vi har på forespørgsel fået oplyst, at der ikke har været ophør af kundeaftaler det seneste år, hvorfor kontrolaktiviteten ikke kunne testes.	Vi har konstateret, at KIMIK iT har udarbejdet en procedure for tilbagelevering af personoplysninger. Der har dog ikke har været ophør af kundeaftaler det seneste år. Vi kan derfor ikke teste kontrollens implementering. Ingen afvigelser konstateret.

A.18: Overensstemmelse

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Overførsel af personoplysninger til tredjelande ▶ I databehandleraftalen foreligger der skriftlige procedurer for overførsel af personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. ▶ Databehandlerens procedure gennemgås og vurderes løbende, og som minimum en gang årligt, om proceduren skal opdateres.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har inspiceret KIMIK iT's kontrol rapport om overførsel af personoplysninger til tredje lande og observeret, at den er opdateret. Vi har stikprøvevis inspiceret KIMIK iT's databehandleraftaler med de dataansvarlige og observeret, at KIMIK iT ikke behandler eller overfører personoplysninger i andre lande uden for EU/EØS.	Ingen afvigelser konstateret.
Instruks fra den dataansvarlige ▶ Databehandleren overfører kun personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige. ▶ Databehandleren dokumenterer indhentet instruks vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer fra dataansvarlige.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har stikprøvevis inspiceret KIMIK iT's databehandleraftaler med de dataansvarlige og observeret, at KIMIK iT ikke behandler eller overfører personoplysninger i andre lande uden for EU/EØS. Yderligere har vi observeret, at KIMIK iT's underdatabehandlere alle fremkommer på EU-US Data Privacy Framework listen.	Ingen afvigelser konstateret.
Gyldigt overførselsgrundlag ▶ Databehandleren vurderer og dokumenterer, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer.	Vi har udført forespørgsel hos passende personale hos KIMIK iT. Vi har stikprøvevis inspiceret KIMIK iT's databehandleraftaler med de dataansvarlige og observeret, at KIMIK iT ikke behandler eller overfører personoplysninger i andre lande uden for EU/EØS. Yderligere har vi observeret, at KIMIK iT's underdatabehandlere alle fremkommer på EU-US Data Privacy Framework listen.	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
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger		
▶ Databehandler har implementeret en procedure for afprøvning, vurdering og evaluering af 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 KIMIK iT. Vi har ikke modtaget tilstrækkelig dokumentation for at KIMIK iT afprøver, vurderer og evaluerer effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger, som varetages på vegne af dataansvarlig	Vi har konstateret, at der ikke kan leveres tilstrækkelig dokumentation for at KIMIK iT afprøver, vurderer og evaluerer effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger som varetages på vegne af dataansvarlig. Ingen yderligere afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

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."

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2025-01-24 11:53:19 UTC

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 37.96.xxx.xxx
2025-01-24 11:58:52 UTC

Gynter Schneider
Administrerende direktør
På vegne af: Kimik IT
Serienummer: 248b026b-184c-445c-87db-c60382f13d72
IP: 194.177.xxx.xxx
2025-01-27 16:29:21 UTC