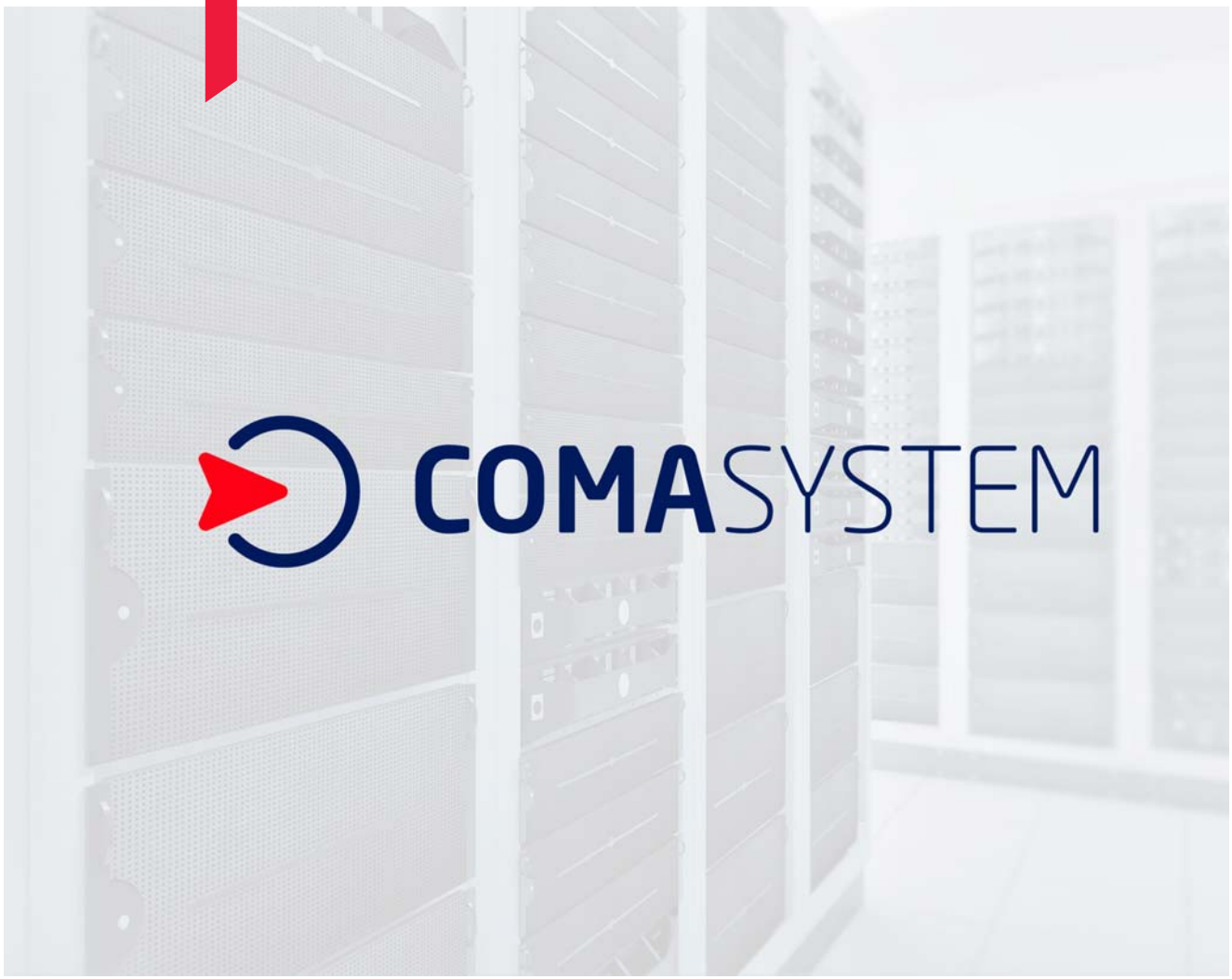

COMASYSTEM APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. OKTOBER 2021 TIL 30. SEPTEMBER 2022 OM BESKRIVELSEN AF COMASYSTEM OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. OKTOBER 2021 TIL 30. SEPTEMBER 2022 OM BESKRIVELSEN AF COMASYSTEM OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i COMAsystem ApS
COMAsystem ApS' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af COMAsystem ApS (databehandleren) for hele perioden fra 1. oktober 2021 til 30. september 2022 udarbejdede beskrivelse i sektion 3 af COMASYSTEM 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 og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen på 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, implementere og effektivt udføre 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.

Vi er underlagt den internationale standard om kvalitetsstyring ISQC 1, og vi anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen og den operationelle effektivitet 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 og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. 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 eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

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 COMASYSTEM, 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. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

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

a. at beskrivelsen af COMASYSTEM 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 i hele perioden fra 1. oktober 2021 til 30. september 2022, 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 i hele perioden fra 1. oktober 2021 til 30. september 2022, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. oktober 2021 til 30. september 2022.

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 COMASYSTEM, 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 24. oktober 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, statsautoriseret revisor

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

2. COMASYSTEM APS UDTALELSE

COMAsystem ApS varetager behandling af personoplysninger i forbindelse med COMASYSTEM 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 COMASYSTEM, 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.

COMAsystem ApS anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

COMAsystem ApS bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden fra 1. oktober 2021 til 30. september 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for COMASYSTEM, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret.
    - De processer der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - De processer der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
    - De processer der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
    - De processer der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
    - De kontroller, som vi med henvisning til afgrænsningen af COMASYSTEM 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. Indeholder relevante oplysninger om ændringer i COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden 1. oktober 2021 til 30. september 2022.

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

COMAsystem ApS 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 og fungerede effektivt i hele perioden fra 1. oktober 2021 til 30. september 2022. 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.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden fra 1. oktober 2021 til 30. september 2022.

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

Greve den 24. oktober 2022

COMAsystem ApS

Christian Richter-Pedersen
CEO

3. COMASYSTEM APS BESKRIVELSE AF COMASYSTEM OG TILHØRENDE KONTROLLER

INDLEDNING

Efterfølgende beskrivelse af COMASYSTEM er udfærdiget med det formål at kunne give retvisende oplysninger samt informationer til COMAsystem ApS' kunder og eksterne auditører.

Nedenstående forefindes en samlet beskrivelse af systemets anvendelse, formål og forhold i relation til systemets drift. Dernæst beskrives tilgangen og den løbende vedligeholdelse af risikovurderingen for systemet.

Beskrivelsen indeholder således også en gennemgang af de i organisationen implementerede kontroller for procedurer og dokumentation.

SYSTEMBESKRIVELSE

Generelt

COMASYSTEM er en Software as a Service (SaaS) webapplikation, der opbevarer og behandler kontraktdata for systemets brugere.

Anvendte kontrakttyper omfatter:

- Leverandørkontrakter
- Salgskontrakter
- Personalekontrakter
- Servicekontrakter

Systemet muliggør aktiv udnyttelse af relevante kontraktdata vha. notifikationer, der sendes til de ansvarlige brugere hos kunden.

Således sørger systemet for overholdelse af fornyelsesfrister, opsigelsesvarsler, overholdelse af forpligtelser i relation til personaler og styring af serviceaftaler.

Systemet er i den nuværende version udviklet med henblik på omfattende sikring af personhenførbare data iht. databeskyttelsesforordningens artikel 25 – "Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger".

Systemet anvendes dermed hos kunden til kontraktstyring, dokumentation ifm. compliance f.eks. ved behandling af persondata og økonomisk optimering.

Infrastruktur og drift

COMASYSTEM er hosted i Danmark, og backup opbevares ligeledes på forskellige lokationer i Danmark.

COMASYSTEM er placeret i Global Connect A/S' datacenter i Høje-Taastrup, Sjælland. Global Connect A/S varetager udelukkende housing-opgaver og optræder ikke som databehandler.

Den daglige drift af systemet, udviklingen og support gennemføres udelukkende af COMAsystem ApS og Nordicode ApS, der er databehandler.

Digital Signatur varetages af underleverandør VISMA A/S, der fungerer som databehandler for kunder, som tilvælger digital underskrift.

Backup varetages af underleverandører (FrontSafe ApS), der er databehandler.

Systemet overvåges 24/7 af både underleverandøren Nordicode ApS samt COMAsystem ApS' egne medarbejdere. Derudover overvåges backuplokationer af FrontSafe ApS.

Risikovurdering

Præmis for risikovurderingen
Risikovurderingen er udført under hensyntagen til de specifikke informationstyper som systemet behandler, mængden og følsomheden af de behandlede oplysninger.

Ligeledes vurderes systemets risiko under hensyntagen af den eller de trusler, der måtte være relevante for de brancher, som systemets kunder arbejder i.

Hændelser relateret til it eller persondatasikkerhed indgår i den løbende vurdering af risici.

Risikovurderingen er udført under antagelse af en hændelse i medfør af databeskyttelsesforordningens artikel 32, stk. 2.

Det antages i denne forbindelse, at systemet håndterer både almindelige og følsomme persondata.

Vurdering og opfølgning
Risikovurderingen er blevet foretaget systematisk igennem følgende hovedområder:

- Hardware og Systemsoftware
- Datatransmission
- Applikationer
- Ind- og uddatamaterialer
- Organisering – Intern
- Underdatabehandlere
- Diverse hændelser af mere specifik karakter (tiltag i fremtiden)

Risikovurderingen anvendes som et aktivt redskab og anses som en variabel, der skal revurderes løbende med hensyn til sikringen af, at COMASYSTEM drives og udvikles ift. det ønskede risikoniveau.

Til risikovurderingen anvendes systemet RISMA risk, og der vurderes både på konsekvensen for virksomheden og for den eller de registrerede iht. databeskyttelsesforordningen.

Alle risici styres og sammenknyttes med processer og eller kontroller, hvor disse fremtræder i det af COMAsystem ApS' anvendte compliance system.

Der er gennemført risikovurderinger ift. både konsekvenser for virksomheden og den registrerede. Risikovurderingen bliver løbende revurderet, og der er processer på plads ifm. Udvikling og nye tiltag, som skal tilsikre at risikovurderingen ajourføres.

Der tages udgangspunkt i det nuværende trusselbillede, og risikovurderingen er en del af dokumentationen til den årlige ISAE 3000-revision. På baggrund af revisionens anbefalinger kan denne danne grundlag for nye projekter eller procedurer, der skal styrke sikkerheden for COMASYSTEM.

KONTROLLER

Generelt

Kontroller oprettes og gennemføres i RISMAcontrols. Kontroller i RISMAcontrols udsender e-mails til de, som er ansvarlige for de pågældende kontroller, og det er også i RISMAcontrols, at kontrollernes gennemførsel dokumenteres.

Dokumentationen, afvigelser ift. kontroldeadline og tilknytning til risici og eller behandlingsaktiviteter fastholdes ligeledes i RISMAcontrols.

Det er på denne måde hensigtens at skabe en ensartet og kontinuerlig oversigt samt historik over COMAsystem ApS' kontrolregime.

COMAsystem ApS har en aktiv holdning til det løbende kontrolregime og tilpasser kontroller løbende til ændrede processer eller funktioner samt tilføjer nye eller arkiverer unødvendige kontroller.

A.5 Informationssikkerhedspolitikker

Der er implementeret en Informationssikkerhedspolitik i virksomheden, og den tages årligt til revision.

A.6 Organisering af informationssikkerhed

Iht. informationssikkerhedspolitikken står bestyrelsen med det overordnede ansvar for organiseringen af informationssikkerheden, og COMAsystem ApS' ledelse har defineret en informationssikkerhedsstrategi. Informationssikkerheden er udbredt i hele organisationen, og COMAsystem ApS stiller de samme krav til eksterne samarbejdspartnere.

A.7 Personalesikkerhed

Det tilsikres under ansættelsen af COMAsystem ApS' medarbejdere, at disse kan arbejde med fortroligt forhold og vurderes til at være i stand til at varetage driften og behandlingen af fortrolige samt følsomme data.
Der er ligeledes procedurer, som tilsikrer en nedlukning af ophørte medarbejdere.

A.8 Styring af aktiver

IT-chefen er udpeget som virksomhedens systemejer og driftsansvarlige. Der er taget stilling til klassificeringen af systemer, og hvilke data der behandles. Der foreligger processer for beskyttelse af mobilt IT-udstyr samt server. På arbejdsstationer (mobilt udstyr) er der etableret diskkryptering. Databærende medier destrueres iht. godkendt procedure.

A.9 Adgangsstyring

I COMAsystem ApS er der indført procedurer for adgangsstyring på arbejdsstationer, systemer og netværk. Adgang tildeles efter funktion til de pågældende medarbejdere.

Adgang til kritiske drifts- og backend-systemer er beskyttet af firewall samt VPN, som er termineret i firewall.

For VPN-brugerne er der planlagt rotation af password iht. IT politikkens minimumskrav.

Bruger, der ikke længere har et funktionsmæssigt behov eller grundet samarbejdets ophør, fratages rettigheder og/eller adgang til dele af eller alle systemer.

Der er implementeret kontroller for at overvåge, at kun personer med funktionsmæssige behov har adgang til specifikke systemer.

Der forefindes ikke fælles brugerkonti og der udleveres personlige brugernavne plus koder. Hemmelige koder styres og opbevares krypteret.

Adgang til persondatabærende enheder og/eller kritiske systemer sker efter vurdering og ifm. arbejdsbetingede behov.

Der arbejdes med transmissionskryptering ved alle loginfunktioner.

A.10 Kryptografi

Der arbejdes målrettet med kryptografering ved både transmission af data og i visse tilfælde ved opbevaring af data.

For e-mail kommunikation er der opsat krav om TLS-kommunikation.

For adgang til webbaserede tjenester bliver TLS-kryptering påtvunget til minimum TLS 1.2.

Backup transmitteres krypteret og opbevares krypteret. FrontSafe har ikke adgang til krypteringsnøglen for COMAsystems backup data.

A.11 Fysisk sikring og miljøsikring

Der anvendes ekstern housing-løsning til COMAsystem ApS' datacenter, hvor der arbejdes med 24/7 overvågning og adgangsstyring.

Det er kun COMAsystem ApS' medarbejdere, som har adgang til det fysiske materiel i datacentret. Det fysiske materiel omfatter server, switche, firewall etc. og er ejet af COMAsystem ApS.

Der forefindes procedure for sikker bortskaffelse og destruktion af databærende medier.

Hos COMAsystem ApS forefindes der alarmanlæg med alarmering og der er processer på plads, således arbejdsstationer automatisk låser.

A.12 Driftssikkerhed

Der anvendes compliance-software til styring af processer, kontroller og tilhørende risikovurderinger. Der registreres hændelser efter bestemte processer og COMAsystem ApS gennemgår årligt alle registrerede hændelser ifm. procesoptimering.

Der er opsat proces og registrering for patch management for både arbejdsstationer og server.

Der anvendes drifts- / kapacitetsovervågning og alarmering på server.

På både arbejdsstationer og server anvendes centraliseret software til imødegåelse af vira og malware.

Der er taget stilling til backup ift. Type, og hvilke data der skal tages backup af. Derudover er der også blevet vurderet, hvor ofte det er nødvendigt at gennemføre backup. Backup verificeres iht. løbende kontrol og ved anvendelse af systemets egne verifikationsindstillinger.

Logning er opsat på alle driftsenheder og opsamles centralt. Adgangen til logdata er begrænset til specifikke medarbejdere.

Change management registreres i hændelseslog, og det er udelukkende IT-chefen, der har beføjelse til installation og eller ændringer af nuværende software.

COMAsystem ApS holder sig løbende ajour i åbne medier og professionelle netværk vedr. sårbarheder.

A.13 Kommunikationssikkerhed

Der er udfærdiget politikker til kommunikationssikkerhed. Det er udelukkende medarbejdere med arbejdsbetinget behov, som kan foretage rettelser i netværksudstyr.

Driftskritisk netværk kan kun tilgås via VPN.

Der eksponeres kun relevante og ønskede services til det åbne net.

Udover tvungen TLS på alt e-mail, så anvendes der en intern mailtjeneste for comasystem.dk, som kun benyttes af applikationen comasystem.dk.

A.14 Udvikling og vedligeholdelse af systemer

Der er fastlagte processer for igangsættelse af udvikling og retningslinjer for sikkerhedskrav til udvikling, anskaffelse og vedligeholdelse.

Der arbejdes med processer til overvågning og kontrol af underleverandører.
Iht. blandet andet databeskyttelsesforordningen revurderes evt. risici løbende, og også kravet om DPIA bliver løbende revurderet.

Der anvendes en ensartet Pipeline til udvikling, og nye systemfeatures dokumenteres.

Produktion og udvikling er adskilt, og der udvikles ikke på produktionsdata.

Der er fastlagt processer for opdatering og opgradering af virtuelle maskiner samt hypervisor og baremetal.

A.15 Leverandørforhold

Der er indgået databehandleraftaler med underleverandører og der er indhentet revisionserklæringer.

Databehandler uden erklæringer auditeres fysisk af COMAsystem ApS og uden forudgående varsel.

Der er ligeledes etableret fysisk kontrol af datacenters sikkerhed og omgivende forhold.

Der udføres tilsyn med primære leverandører på følgende måde:

GlobalConnect A/S (ikke databehandler):
Leverance: Datacenter housing
- Fysisk kontrol
- Årlig revurdering af revisionserklæring med særlig fokus på fysisk sikkerhed

Nordicode ApS:
Leverance: Udvikling
- Fysisk kontrol
- Awareness tiltag
- Logning
- Activity-beskeder

FrontSafe A/S:
Leverance: Backup
- Funktionskontroller (særskilt under backup)
- Årlig revurdering af revisionserklæring med fokus på afvigelser ift. forhold, som gælder backup i transmission og under opbevaring

VISMA Consulting A/S:
Leverance: Digital signatur
- Årlig revurdering af revisionserklæring med fokus på afvigelser ift. forhold, som gælder backup i transmission og under opbevaring

A.16 Styring af informationssikkerhedsbrud

Grundlæggende anvendes forebyggende og opdagende kontroller, således brud på persondatasikkerheden kan afværges eller håndteres uden unødvendige ophold.

Der forefindes procedurer for håndtering af informationssikkerhedsbrud. Håndteringen omfatter registrering, risikovurdering, kommunikation og mitigering.

Medarbejdere og leverandører gøres løbende opmærksomme på hvordan informationssikkerhedsbrud skal håndteres.

Alle sikkerhedsbrud behandles også som databeskyttelsesforordningen ifm. registrering, orientering og anmeldelse.

I langt til fleste tilfælde optræder COMAsystem ApS som databehandler på vegne af systemets kunder. Brud på persondatasikkerheden meddeles derfor straks til den eller de pågældende dataansvarlige.

Det præciseres herved, at COMAsystem ApS' kunder er selvstændige dataansvarlige ift. COMAsystem ApS og har ansvaret for egen risikovurdering af hændelser og anmeldelse til myndigheder samt underretninger af de registrerede.

A.17 Beredskabsplan

COMAsystem ApS har procedurer på plads, der har til opgave at tilsikre en opstart af mitigerende foranstaltninger uden unødige ophold i tilfælde af systemnedbrud eller anden hændelse, som gør COMASYSTEM utilgængeligt for brugere og COMAsystem ApS' medarbejdere, eller nedsætter systemets funktionsevne eller sikkerhed.

Derudover opfattes alle hændelser også som hændelser under databeskyttelsesforordningen og risikovurderes iht. denne.

CTO er som udgangspunkt den ansvarlige ift. alle hændelser og sørger for registrering, kommunikation, risikovurdering samt mitigering.

COO overtager denne rolle i CTO´s fravær.

Alle hændelser håndteres centralt i COMAsystem ApS' compliance software.

A.18 Overensstemmelse

Privatlivspolitik – er udarbejdet og vedligeholdes løbende igennem opsat kontrol. Politikken er tilgængelig for alle COMAsystem ApS' kunder og gæster på comasystem.dk/privatlivspolitik.

I forhold til awareness træning opererer COMAsystem ApS med en meget flad organisation, og der er opsat kontroller, som bidrager til gentagne diskussioner og vurderinger af virksomhedens forhold ift. persondata, og hvordan medarbejdere samt leverandører for COMAsystem ApS skal håndtere disse.

Databehandleraftaler med kunder bliver indgået ved indgåelse af aftale/kontrakt om leverance af COMASYSTEM software og skal underskrives inden, der gives adgang.
Databehandleraftalen er altid tilgængelig på comasystem.dk.

Databehandlerfortegnelse, opbevaring og vedligeholdelse heraf sker i compliance system RISMAgdpr samt filbaserede systemer. Fortegnelse, kontroller og risikovurdering dokumenteres i systemet og danner grundlag for den løbende dokumentation af de opstillede kontroller.

Efterlevelse af instrukser og underretning, hvis disse er i strid med lovgivningen, fastholdes ligeledes i RISMAgdpr, og der gennemføres løbende vurderinger igennem planlagte kontroller, så organisationen kan tilrettes.

Elektronisk opbevaring af databehandleraftaler for leverandører sker i RISMAgdpr og sammenholdes med de indhentede revisionserklæringer.

Sikring af, at underdatabehandlere lever op til kravene fra de dataansvarlige, sker gennem en ensartet databehandleraftale med COMAsystem ApS' kunder og et leverandørvalg, som understøtter den udarbejdede instruks omkring sikringsniveau og fysisk placering. Derudover risikovurderes databehandlerne ift. de funktioner, som disse udfører på vegne af COMAsystem ApS.

Konsekvensanalyse (DPIA) vurderes umiddelbart ikke nødvendigt at gennemføre pga. fravær af høj risiko for behandlingen, og idet behandlingen kun i mindre grad omfatter følsomme data. Der er opsat kontrol af, at behov for en DPIA for COMASYSTEM løbende revurderes.

Sletning af data sker både automatiseret i COMAsystem ApS' backup samt i automatiseret processer i applikationen, som den dataansvarlige selv har indflydelse på. Kundedata bliver slettet ved endt kundeforhold og er fastholdt i sletningsprocesserne. COMAsystem ApS opbevarer derudover kun data, som falder under anden lovgivning, som f.eks. bogføringsloven.

De registreredes rettigheder er beskrevet i procedurer for COMAsystem ApS. Det er dog sådan, at den enkelte kunde som dataansvarlige selv skal udtrække, rette eller slette egne data ift. anmodning efter databeskyttelsesforordningens artikel 15 – 20 samt artikel 7 vedr. samtykke. COMAsystem ApS vil i alle tilfælde assistere den dataansvarlige efter anmodning, og disse anmodninger vil blive registreret i hændelsesloggen for COMAsystem ApS.

Revision og inspektion udføres årligt og på egen foranledning af COMAsystem ApS. COMAsystem ApS ønsker via en ekstern revision af typen ISAE 3000 at synliggøre virksomhedens fokus på og evner til at kunne arbejde sikkert og på en professionel måde med kundernes data.

Bistand til den dataansvarlige ydes til den dataansvarlige, og de nærmere forhold fremgår af databehandleraftalen.

Der er opsat kontroller, som varetager sikringen og dokumentationen af forandringer, fjernelse eller tilføjelse af forretningsprocesserne i COMAsystem ApS. Kontrollen bliver gennemført under hensyntagen til risikovurderingen, som tager udgangspunkt i konsekvensen for de registrerede.

ÆNDRINGER I COMASYSTEM OG DE TILHØRENDE KONTROLLER

Der er i perioden ikke blevet gennemført væsentlige ændringer til applikationen, infrastrukturen eller leverandørforhold.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Det henstilles til de dataansvarlige, som COMAsystem ApS er databehandler for, at overholde følgende:

- Tilsikre egne processer til sikring af de registreredes rettigheder for de persondata, som lægges i COMASYSTEM.
- Udarbejde egne risikovurderinger for indhentning, anvendelse og opbevaring af persondata.
- Benyt de i COMASYSTEM udlagte funktioner til sletning af persondata uden formål eller manglende lovhjemmel.
- Tilsikre en brugeradministration af egne brugere i COMAsystem, så fratrådte og opsagte medarbejder ikke længere har adgang til systemet.
- Tilsikre i brugeradministrationen, at der drages omhyggeligt omsorg med tildelingen af rettigheder i COMASYSTEM.

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 COMAsystem ApS beskrivelse af COMASYSTEM samt for udformningen og den operationelle effektivitet 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 eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af COMAsystem ApS, 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 og har fungeret effektivt i hele perioden fra 1. oktober 2021 til 30. september 2022.

Udførte testhandlinger

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

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.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, der leveres af Global Connect A/S som serviceunderleverandør inden for housing af it-udstyr, har vi fra uafhængig revisor modtaget en ISAE 3402 type 2-erklæring for perioden fra 1. januar til 31. december 2021 om beskrivelsen af kontroller, deres udformning og funktionalitet i tilknytning til datacenterløsning.

Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i databehandlerens beskrivelse af COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene vurderet erklæringen og testet de kontroller hos databehandleren, der overvåger funktionaliteten af serviceunderleverandørens kontroller.

For de ydelser, der leveres af FrontSafe A/S som underdatabehandler inden for drift af it, har vi fra uafhængig revisor modtaget en ISAE 3402 type 2-erklæring for perioden fra 1. oktober 2020 til 30. november 2021 vedrørende afdækning af de tekniske og organisatoriske sikringsforanstaltninger i tilknytning til driften af Cloud backup-ydelser.

For de ydelser, der leveres af VISMA Consulting A/S som underdatabehandler inden for digital underskrift, har vi fra uafhængig revisor modtaget en ISAE 3000 erklæring for perioden fra 1. april 2021 til 31. marts 2022 om overensstemmelse med databeskyttelseslovgivningen som databehandler.
Ovennævnte underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i databehandlerens beskrivelse af COMASYSTEM og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene vurderet erklæringen og testet de kontroller hos databehandleren, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlernes 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 og implementeret eller ikke har fungeret effektivt i perioden.

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**
Kontrol - Risikovurdering ▶ Databehandlerens informationssystemer og aktiver er risikovurderet i forhold til fortrolighed, integritet og tilgængelighed for den registrerede. ▶ Minimum én gang årligt eller ved væsentlige ændringer revurderes risikovurderingen. ▶ Virksomhedens risikolog for informationsaktiver opdateres i forhold til resultatet af risikoanalysen.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret databehandlerens system for risikostyring og politikker for risikostyring. Vi har observeret, at risikovurderingen er udarbejdet med afsæt i fortrolighed, integritet og tilgængelighed for den registrerede. Vi har observeret, at risikovurdering opdateres mindst én gang årligt. Vi har observeret, at seneste opdatering af risikovurdering er foretaget den 22. september 2022. Vi har observeret, at identificerede risici registreres og opdateres i databehandlerens risikolog.	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
Kontrol - Informationssikkerhedspolitikker - Politik for Informationssikkerhedspolitikker er fastlagt og dokumenteret. - Politikker for Informationssikkerhed bliver som minimum taget op til intern revision 1 gang årligt eller ved væsentlige ændringer hos databehandleren.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at ansvars- og gyldighedsområde er defineret. Vi har observeret, at politikker omfatter behandling af persondata. Vi har observeret, at informationssikkerhedspolitikken er opdateret og godkendt af ledelsen den 10. juni 2022. Vi har ligeledes observeret, at politikker og processer er gennemgået samlet d. 9. september 2022.	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 organisering af informationssikkerhed ▶ Politik for organisering af informationssikkerhed er fastlagt og dokumenteret.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at organisering af informationssikkerhed og ansvar er defineret i politikken.	Ingen afvigelser konstateret.
Roller og ansvarsområder ▶ Alle aktiver og informationssikkerhedsprocesser er identificeret, defineret og ansvarlig med nødvendig kompetence er udpeget. ▶ Ansvar, beføjelser og ramme for informationssikkerhedsroller er defineret og dokumenteret for hver enkelt proces eller aktiv. ▶ Databehandlerens ledelse sikrer, at der for driftskritiske funktioner er tilstrækkelig funktionsadskillelse. Hvor dette ikke er muligt, er der iværksat kompenserende kontroller.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at informationsaktiver er identificeret og ansvarlig for informationssikkerhedsaktiver er udpeget. Vi har observeret, at ansvar, rammer og beføjelser er fastlagt og dokumenteret i informationssikkerhedspolitik. Vi har desuden observeret, at igangsættelse af udviklingsopgaver skal autoriseres af virksomhedens direktion eller bestyrelse. Vi har inspiceret organisation og roller for funktionsadskillelse for driftskritiske systemer.	Ingen afvigelser konstateret.
Informationssikkerhed ved projektstyring ▶ Alle projekter risikovurderes i forhold til informationssikkerhed og persondata. ▶ Ved væsentlige ændringer i projekter, skal der ske en fornyet vurdering af informationssikkerhed.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret politikker og procedurer. Vi har observeret, at der er udformet en procedure for risikovurdering i projekter. Vi har inspiceret dokumentation for risikovurdering. Vi har observeret, at der er foretaget risikovurdering i forbindelse med væsentlige ændringer.	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 ▶ Medarbejdere kan ikke installere software på arbejdsstationer. ▶ Arbejdsstationer opdateres automatisk via central styret klient. ▶ Arbejdsstationer er krypteret. ▶ Arbejdsstationer er installeret med aktivt og opdateret antivirus software.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret login på arbejdsstation. Vi har observeret, at login kræver bruger-id og adgangskode. Vi har ligeledes observeret, at brugere ikke har adgang til installation af software. Vi har for en udvalgt stikprøve observeret, at arbejdsstation er installeret med en klient til sikring af, at der installeres opdateringer, og at der er aktiveret webskjold og antivirus-software. Vi har observeret, at klienten administreres centralt. Vi har inspiceret system for central styring af arbejdsstationer. Vi har observeret, at alle arbejdsstationer er installeret og opdateret. Vi har for en stikprøve inspiceret systemkonfiguration for arbejdsstationer. Vi har observeret, at arbejdsstationer er krypteret med BitLocker. Vi har inspiceret procedure for kontrol af klient. Vi har observeret, at der er udformet procedure for gennemgang af klient. Vi har observeret, at kontrollen senest er gennemført den d. 30. september 2022. Vi har for en stikprøve inspiceret opdateringsstatus for arbejdsstation. Vi har observeret, at arbejdsstationen er opdateret og installeret med antivirus-software.	Vi har konstateret at proceduren for kontrol af klient ikke adresserer alle relevante arbejdsstationer, hvorfor design af kontrollen ikke er hensigtsmæssigt udformet. 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
Fjernarbejdspladser ▶ Ved arbejde fra fjernarbejdspladser anvendes der krypteret VPN. ▶ Dokumenter og enheder skal beskyttes mod tyveri, tab og hærværk. ▶ Medarbejdere er informeret om informationssikkerhed ved arbejde på fjernarbejdsplads.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for VPN. Vi har observeret, at der er konfigureret kryptering af VPN-forbindelse. Vi har observeret, at VPN-klient autentificeres vha. certifikat samt unik bruger-id og password. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udformet retningslinjer for opbevaring og anvendelse af it-udstyr. Vi har ved forespørgsel fået bekræftet, at medarbejdere er informeret om informationssikkerhed ved anvendelse af fjernarbejdsplads.	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
Politik for personalesikkerhed ▶ Politik for personalesikkerhed er fastlagt og dokumenteret. ▶ Politik for personalesikkerhed revideres årligt.	Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker for personalesikkerhed. Vi har observeret, at politikker revideres årligt som en del af opdatering af informationssikkerhedspolitikken. Vi har observeret, at politikker er revideret den 10. juni 2022, og vi har ligeledes observeret, at politikker og processer er gennemgået samlet d. 9. september 2022.	Ingen afvigelser konstateret.
Før ansættelse ▶ Alle kandidater bliver før ansættelse screenet og vurderet i forhold til referencer, bekræftelse af uddannelse og faglige kvalifikationer, sikring af identitet og i særlige tilfælde, strafferetslige forhold. ▶ Alle medarbejdere underskriver en fortrolighedserklæring ved ansættelse, heraf fremgår medarbejderens juridiske ansvar og sanktioner ved brud af fortrolighed. ▶ Medarbejdere informeres om informationssikkerhed og andre forhold, der er gældende for stillingen, der ansættes til.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret politikker for ansættelse. Vi har observeret, at der er krav om indhentelse af straffeattest for alle medarbejdere ved ansættelse. Vi har fået bekræftet, at, der indhentes straffeattest for medarbejdere ved ansættelse. Vi har observeret, at der er udformet procedurer for vurdering af afgivelse af tavshedserklæring. Vi har inspiceret skabelon for en ansættelseskontrakt. Vi har for en stikprøve observeret, at medarbejdere i ansættelseskontrakten er pålagt tavshedspligt. Vi har observeret, at politikken indeholder sanktioner ved brud på informationssikkerhedspolitik eller fortrolighed. Vi har observeret, at der er blevet informeret om informationssikkerhed i forbindelse med ansættelse. Vi har ligeledes observeret, at der er foretaget screening og vurdering af kandidat ved ansættelse af en ny medarbejder.	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
Under ansættelsen ▶ Medarbejderen undervises i sikkerhedsforanstaltninger i forbindelse med behandling af følsomme og fortrolige data. ▶ Informationssikkerhedspolitik er tilgængelig for alle medarbejdere. ▶ Ved behov informeres der til medarbejdere om aktuelle trusler og ændringer i informationssikkerhedspolitikker.	Vi har udført forespørgsler hos passende personale. Vi har ved forespørgsel fået bekræftet, at der undervises i informationssikkerhed ved ansættelse eller indgåelse af samarbejdsaftaler. Vi har inspiceret fællesdrev. Vi har observeret, at informationssikkerhedspolitikken er tilgængelig for alle medarbejdere. Vi har ved forespørgsel fået bekræftet, at der informeres om informationssikkerhed og aktuelle trusler efter behov.	Ingen afvigelser konstateret.
Ansættelsesforholdets ophør eller ændring ▶ Alle medarbejdere er ved ansættelse informeret om ansvar, krav og sanktioner, der er gældende efter ansættelsesforholdets ophør.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker for personalesikkerhed ved fratrædelse. Vi har observeret, at der er udformet retningslinjer for tilbagelevering af informationsaktiver og fjernelse af rettigheder i systemer. Vi har for en stikprøve inspiceret dokumentation for tilbagelevering af informationsaktiver og nedlukning af adgange er foretaget for den pågældende medarbejder.	Ingen afvigelser konstateret.

A.8: Styring af aktiver

Kontrolmål

- *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 aktiver ▶ Ledelsen har udarbejdet, godkendt og kommunikeret politik for anvendelse og håndtering af enheder og medier. ▶ Databehandleren udarbejder en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af dataansvarlige. ▶ Fortegnelsen opdateres løbende og kontrolleres under den årlige gennemgang af politikker og procedurer mv. ▶ Fortegnelsen opbevares skriftligt og elektronisk. ▶ Databehandleren stiller efter anmodning fortegnelsen til rådighed for tilsynsmyndigheden. ▶ For alle systemer er der udpeget en systemejer, der er ansvarlig for daglig drift og vedligeholdelse. ▶ Data i driftssystemer er klassificeret og behandles som fortrolige data.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udarbejdet politik for anvendelse og håndtering af enheder og medier. Vi har inspiceret fortegnelse over kategorier og behandlingsaktiviteter. Vi har observeret, at indholdet heraf opfylder kravene i databeskyttelsesforordningens artikel 30, stk. 2. Vi har observeret, at fortegnelsen opdateres løbende. Vi har observeret, at fortegnelsen er opdateret den 9. september 2022. Vi har observeret, at fortegnelse over kategorier af behandlingsaktiviteter opbevares elektronisk. Vi har ved forespørgsler fået bekræftet, at fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af dataansvarlige, på anmodning stilles til rådighed for tilsynsmyndigheden. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at it-chefen er udpeget som systemejer for driftssystemer. Vi har observeret, at data i driftssystemer er klassificeret som følsomme personoplysninger.	Ingen afvigelser konstateret.
Håndtering af enheder og fysiske medier ▶ Alle enheder og medier beskyttes ved kryptering. ▶ Enheder, der udleveres til medarbejdere eller 3. mand, registreres ved udlevering og tilbagelevering. ▶ Ved udlevering er det sikret, at der ikke er fortrolige eller følsomme data på enheder.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker for håndtering af fysiske medier	Ingen afvigelser konstateret.

A.8: Styring af aktiver

Kontrolmål

- *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
▶ Medarbejdere, som anvender enheder eller medier uden for organisationen, er ansvarlig for at sikre disse mod tyveri, tab eller hærværk.	og enheder. Vi har ligeledes observeret, at der er fastlagt retningslinjer for beskyttelse af mobilt udstyr og enheder, der anvendes uden for organisationen. Vi har for en stikprøve inspiceret systemkonfiguration for en arbejdsstation. Vi har observeret, at enheder er krypteret. Vi har inspiceret politikker for anvendelse af enheder uden for organisationen. Vi har ved forespørgsler fået bekræftet medarbejdernes forståelse for kontrollen.	
Bortskaffelse ▶ Diske og medier destrueres, når de tages ud af drift. ▶ Diske og medier slettes og formateres før genanvendelse.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret procedurer for bortskaffelse og sletning af diske. Vi vurderer at disse er passende udformet. Vi har ved forespørgsel fået oplyst, at der ikke har været hændelser i erklæringsperioden til brug for test af kontrollens effektivitet, hvorfor vi ikke kan udtale os herom. Vi har ved forespørgsel fået bekræftet medarbejderens forståelse for kontrollen.	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
Politik for adgangsstyring ▶ Politik for adgangsstyring til systemer og data er fastlagt og dokumenteret. ▶ Politik for adgangsstyring revideres årligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker for adgangsstyring. Vi har observeret, at politikker revideres årligt som en del af opdatering af informationssikkerhedspolitikken. Vi har observeret, at politikker er revideret den 10. juni 2022. Vi har observeret, at politikker og processer er gennemgået og vurderet samlet d. 1. juli 2022.	Ingen afvigelser konstateret.
Adgang til netværk og netværkstjenester ▶ Adgang til netværk og netværkstjenester kræver gyldigt bruger-id. ▶ Ved adgang til virksomhedsnetværket kræves det, at der oprettes VPN. ▶ Adgang gives til systemer og data, og tildeles brugere med et arbejdsrelateret behov.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udformet krav til sikkerhed ved adgang til netværk og netværksservices. Vi har inspiceret systemdokumentation og systemkonfiguration for firewall. Vi har observeret, at adgang til netværk kræver gyldigt bruger-id, og at der er begrænset adgang til netværk. Vi har observeret, at alle forbindelser til driftssystemer sker via VPN eller HTTPS. Vi har inspiceret direkte adgang til webservices og observeret, at forbindelse afvises. Vi har inspiceret liste over brugere med adgang til VPN. Vi har observeret, at kun medarbejdere med arbejdsbetinget behov er tildelt adgang.	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
Oprettelse, ændring og afmelding af brugere ▶ Der er udformet en procedure for ændring og ophør af samarbejdsforhold. ▶ Oprettelse af brugere og tildeling af rettigheder autoriseres af nærmeste leder. ▶ Tildeling af brugeradgang vurderes individuelt og baseres på brugerens funktionsområde. ▶ Bruger tildeles et midlertidigt password ved oprettelse, som skiftes ved første log-on. ▶ Ved ophør af et samarbejdsforhold, deaktiveres brugeren i alle tildelte systemer, så adgang til Virksomhedens systemer forhindres.	Vi har udført forespørgsler hos passende personale. Vi har ved forespørgsler fået bekræftet, at oprettelse af brugere sker ved indgåelse af kontrakt med medarbejder. Vi har inspiceret procedure for gennemgang af brugerrettigheder. Vi har observeret, at der sker gennemgang af rettigheder for kritiske driftssystemer og adgang til personoplysninger. Vi har observeret, at kontrollen er gennemført den 1. juli 2022. Vi har udtaget en stikprøve på en fratrådt medarbejder og observeret, at han har fået fjernet sine adgange.	Ingen afvigelser konstateret.
Styring af privilegerede adgangsrettigheder. ▶ Tildeling af privilegerede adgangsrettigheder sker ud fra et arbejdsbetinget behov. ▶ Privilegerede adgangsrettigheder sker på en særlig bruger-id.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udformet politikker for administration af privilegerede adgange. Vi har observeret, at der er foretaget gennemgang af rettigheder for kritiske driftssystemer og adgang til persondata. Vi har observeret, at kontrollen er gennemført den 1. juli 2022, og vi har inspiceret dokumentationen herfor. Vi har inspiceret dokumentation for, at privligerede adgangsrettigheder tilgås ved brug af unik bruger-id.	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
Gennemgang af brugeradgangsrettigheder ▶ Tildelte adgange gennemgås to gange årligt af systemejer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret procedure for gennemgang af brugerrettigheder. Vi har observeret, at der sker gennemgang af rettigheder for kritiske driftssystemer og adgang til personoplysninger. Vi har inspiceret system for registrering af kontroller. Vi har observeret, at der er gennemført revidering af tildelte rettigheder den 1. juli 2022, og vi har inspiceret dokumentation herfor.	Ingen afvigelser konstateret.
Styring af hemmelig autentifikationsinformation ▶ Hemmelig autentifikationsinformation for system- og servicebrugere opbevares krypteret og adgangskodebeskyttet. ▶ Kun brugere med særligt arbejdsbetinget behov har adgang til adgangskoder.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for opbevaring af hemmelige autentificeringsoplysninger. Vi har observeret, at koder og login-oplysninger opbevares, krypteret og er beskyttet med adgangskode. Vi har ved forespørgsel fået bekræftet, at kun medarbejdere med arbejdsbetinget behov har adgang til autentificeringsoplysninger.	Ingen afvigelser konstateret.
Begrænset adgang til informationer ▶ Adgang til systemer og filsystem er bestemt af arbejdsbetinget behov. Tildeling af adgang autoriseres af virksomhedens ledelse og/eller systemejer og gennemgås minimum én gang årligt.	Vi har udført forespørgsler hos passende personale. Vi har ved forespørgsel fået oplyst, at der ikke er tildelt adgange i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollernes effektivitet. Vi har ved forespørgsler fået bekræf-	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
	tet, at adgang til informationsaktiver og data sker efter bestilling fra ledelsen, og at tildeling sker efter vurdering af det arbejdsbetingede behov. Vi har observeret, at kun medarbejdere med et arbejdsbetinget behov er tildelt adgang. Vi har inspiceret procedure for gennemgang af adgangsrettigheder. Vi har observeret, at der sker gennemgang af rettigheder for kritiske driftssystemer og adgang til persondata. Vi har observeret, at kontrollen er gennemført den 1. juli 2022, og vi har inspiceret dokumentation herfor.	
Procedurer for sikkert log-on - Ved flere fejlede log-on forsøg låses brugerkonto automatisk - Ved låsning af konto, der ikke kan tilskrives brugeren, registreres dette i hændelseslog. - Password transmitteres krypteret.	Vi har udført forespørgsler hos passende personale. Vi har for en stikprøve inspiceret systemkonfiguration af servere. Vi har observeret, at der er automatisk låsning af brugerkonti ved fejlede loginforsøg. Vi har ved forespørgsel fået bekræftet, at der sker registrering af informationssikkerhedshændelser ved låsning af brugerkonti, men at der i erklæringsperioden ikke har været en hændelse, hvorfor vi ikke har kunnet teste kontrollernes effektivitet Vi har observeret, at login til system sker via HTTPS VPN, og at password er krypteret i transmission.	Ingen afvigelser konstateret.
System for administration af adgangskoder - Brugere tildeles personlige bruger-id. - Brugere kan vælge og skifte egne password.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret systemkonfiguration for en udvalgt server. Vi har observeret, at brugere er oprettet med individuelle bruger-id.	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
▶ Der er udformet politikker og procedurer for adgangskoder, der sikrer, at password lever op til de til enhver tid gældende anbefalinger om sikre password, med hensyn til blandt andet, længde, kompleksitet og udskiftning. Alle medarbejdere har modtaget instruktion i udformning og skift af password. ▶ Adgangskoder transmitteres mellem klient og server i krypteret form. ▶ Brugere skal skifte password ved første log-on.	Vi har inspiceret system for brugeradministration. Vi har observeret, at brugere har adgang til at skifte password. Vi har ligeledes observeret, at der er mulighed for at tvinge brugere til skift af password ved næste login. Vi har inspiceret politikker og procedurer for adgangskoder. Vi har observeret, at der er udsendt instruktion til skift af password til alle brugere. Vi har observeret, at instruktionen indeholder krav til udformning og skift af password. Vi har inspiceret dokumentation for udført kontrol og observeret, at seneste udsendte mail vedrørende skift af password er foretaget 8. august 2022. Vi har inspiceret system for autentificering. Vi har observeret, at password transmitteres krypteret. Vi har inspiceret meddelelse til bruger ved opstart. Vi har observeret, at brugere meddeles skriftligt ved opstart, at password skal skiftet ved første login.	
Brug af privilegerede systemprogrammer ▶ Anvendelse af privilegerede systemprogrammer på servere kræver administrative rettigheder. ▶ Kun medarbejdere med arbejdsbetinget behov har adgang til at anvende privilegerede systemprogrammer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret systemkonfiguration for en udvalgt server. Vi har observeret, at anvendelse af administrative applikationer kræver medlemskab af privilegeret gruppe på servere. Vi har inspiceret udskrift af rettighedsgrupper for en udvalgt server. Vi har observeret, at adgang til privilegeret gruppe er tildelt medarbejdere med et arbejdsbetinget behov.	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
Styring af adgang til kildekoder til programmer ▶ Adgang til kildekode tildeles efter et arbejdsbetinget behov. ▶ Kildekode versionsstyres i centralt opbevaringssystem. ▶ Adgang til kildekode tildeles af IT-ledelsen. ▶ Adgang til opbevaringssystem gennemgås minimum én gang årligt eller ved oprettelse/nedlæggelse af projekter.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for opbevaring og versionering af kildekode. Vi har observeret, at kun medarbejdere med et arbejdsbetinget behov er tildelt adgang til kildekoden og udviklingssystemet. Vi har observeret, at kildekode versionsstyres i centralt system. Vi har observeret, at der er foretaget gennemgang af brugere den 1. juli 2022, og vi har inspiceret dokumentation herfor.	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 - Politik for anvendelse af kryptografi er fastlagt og dokumenteret - Politik for anvendelse af kryptografi revideres minimum én gang årligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker for anvendelse af kryptering. Vi har observeret, at politikker revideres årligt som en del af opdatering af informationssikkerhedspolitikken. Vi har observeret, at politikker og processer er gennemgået og vurderet samlet d. 9. september 2022.	Ingen afvigelser konstateret.
Beskyttelse og kryptering af information - Følsomme personoplysninger beskyttes ved kryptering under arkivering. - Alle arbejdsstationer og udleverede enheder er krypteret. - Virksomhedens kommunikationsforbindelser mellem virksomheden, kunder og samarbejdspartnere sikres med kryptering.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udformet retningslinjer for kryptering af data ud fra krav til fortrolighed og integritet. Vi har observeret, at politikker revideres årligt som en del af opdatering af informationssikkerhedspolitikken. Vi har inspiceret filsystem og system for sikkerhedskopiering. Vi har observeret, at data er krypteret under opbevaring. Vi har for en udvalgt stikprøve inspiceret arbejdsstation. Vi har observeret, at denne er krypteret. Vi har inspiceret test af TLS-kryptering af dataforbindelser til driftssystemer. Vi har observeret, at der er konfigureret kryptering TLS 1.3 for oprettelse af forbindelse. Vi har inspiceret systemkonfiguration for at følsomme oplysninger beskyttes ved kryptering under arkivering. Vi har observe-	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
	ret, at der er tvunget kryptering ved opbevaring af adgangskoder. Vi har inspiceret logning for anvendt kryptering. Vi har observeret, at alle adgangskoder er krypteret under arkivering.	

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
Politik for fysisk sikring og miljøsikring ▶ Politik for fysisk sikring og miljøsikring er fastlagt og dokumenteret. ▶ Politik for fysisk sikring og miljøsikring revideres minimum én gang årligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker og retningslinjer for fysisk sikkerhed. Vi har observeret, at politikker revideres årligt som en del af opdatering af informationssikkerhedspolitikken. Vi har observeret, at politikker er revideret den 10. juni 2022. Vi har observeret, at politikker og processer er gennemgået og vurderet samlet d. 9. september 2022.	Ingen afvigelser konstateret.
Fysisk adgangskontrol – datacenter ▶ Adgang til sikrede lokationer er alene tildelt CEO og IT-chef.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret adgangsliste for personer med adgang til databehandlerens udstyr i datacenter. Alene COO og it-chef er tildelt adgang. Vi har observeret, at ledelsen har foretaget revidering af tildelte adgange den 9. september 2022.	Ingen afvigelser konstateret.
Sikker bortskaffelse, vedligehold eller genbrug af udstyr ▶ Ved bortskaffelse, genbrug eller reparation, sikres det, at data er slettet og gendannelse ikke er muligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret kontroller for bortskaffelse og sletning af diske. Vi har inspiceret kontroller for bortskaffelse og sletning af diske. Vi har observeret, at diske er bortskaffet via serviceleverandør. Vi har inspiceret dokumentation for aflevering af diske. Vi har observeret, at der er foretaget aflevering af diske til serviceleverandør for makulering d. 26. december 2021.	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
Politik for ryddeligt skrivebord og blank skærm ▶ PC låses med skærmlås, når arbejdspladsen forlades.	Vi har udført forespørgsler hos passende personale. Vi har ved forespørgsel af relevante medarbejdere fået bekræftet, at der ikke opbevares personoplysninger i fysisk form. Vi har observeret, at der er implementeret automatisk skærmlås, når arbejdspladsen forlades.	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
Politik driftssikkerhed ▶ Politik for driftssikkerhed er fastlagt og dokumenteret ▶ Politik for driftssikkerhed revideres årligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt politikker og retningslinjer for driftssikkerhed. Vi har observeret, at politikker for driftssikkerhed revideres årligt i forbindelse med revidering af informationssikkerhedspolitik. Vi har observeret, at politikker og processer er gennemgået og vurderet samlet d. 9. september 2022.	Ingen afvigelser konstateret.
Dokumenterede driftsprocedurer ▶ Der er udarbejdet procedurebeskrivelser eller arbejdsinstrukser for rutinemæssige opgaver. ▶ Væsentlige driftsforstyrrelser og -uregelmæssigheder, som påvirker forretningskritiske applikationer, registreres i hændelseslog. ▶ Der er udarbejdet instruktioner til genetablering af driftskritiske systemer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for registrering af kontroller. Vi har observeret, at der er udarbejdet procedurer for tilbagevendende driftsopgaver. Vi har inspiceret procedure for registrering af væsentlige driftsforstyrrelser og uregelmæssigheder. Vi har inspiceret hændelseslog. Vi har observeret, at væsentlige driftsforstyrrelser registreres i hændelseslog. Vi har inspiceret procedure for genetablering af drift/beredskabsplan. Vi har observeret, at der er udformet en overordnet plan for reetablering af drift efter kritiske nedbrud. Vi har observeret, at beredskabsplan er opdateret i august 2022.	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
Patchmanagement – systemsoftware ▶ Alle væsentlige ændringer identificeres, styres og dokumenteres i Patch Management System. ▶ Der foretages planlægning af test og deployment som en del af patchmanagement proceduren. ▶ Alle væsentlige ændringer godkendes før implementering. ▶ Informationssikkerhed sikres som en del af patchmanagement. ▶ Alle væsentlige ændringer risikovurderes før implementering. ▶ Nødprocedurer og fail-back planlægges som en del af patchmanagement.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for kontroldokumentation. Vi har observeret, at der er udformet procedure for opdatering af operativsystemer og databaser. Vi har observeret, at opdateringer installeres og testes i Staging-miljø, forinden disse installeres i driftsmiljø. Vi har for en stikprøve inspiceret dokumentation for opdatering. Vi har observeret, at der er gennemført opdatering af driftssystemer den 2. september 2022. Vi har observeret, at opdateringer foretages i et fastlagt opdateringsvindue. Vi har observeret, at der er udformet en procedure for opdatering, herunder risikovurdering og fall-back planlægning.	Ingen afvigelser konstateret.
Kapacitetsstyring ▶ Driftskritiske systemer overvåges i realtid for kapacitetsudnyttelse og ressourceknaphed.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for kapacitetsovervågning. Vi har for en stikprøve observeret, at der foretages overvågning af servere og systemer for kapacitets overvågning. Vi har inspiceret dokumentation for at mails med alarmer modtages, og at der sker opfølgning herpå.	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
Kontroller mod malware ▶ Servere og arbejdsstationer er beskyttet med Antivirus. ▶ Antivirus software opdateres regelmæssigt. ▶ Procedure for håndtering af malwareudbrud er beskrevet og implementeret.	Vi har udført forespørgsler hos passende personale. Vi har for en stikprøve inspiceret arbejdsstationer. Vi har observeret, at der er installeret antivirus-software. Vi har ligeledes observeret, at software er opdateret. Vi har for en stikprøve inspiceret systemkonfiguration for server. Vi har observeret, at der er installeret antivirus-software. Vi har observeret, at der er udformet procedure for brugernes håndtering af malwareudbrud, og inspiceret dokumentation for at proceduren er fulgt.	Ingen afvigelser konstateret
Backup af information ▶ Der tages backup af alle kritiske servere og datadrev. ▶ Der foretages backup hver time. ▶ Backup kontrolleres ugentligt. ▶ Der modtages statusnotifikation ved fejl i backup. ▶ Der gennemføres én gang årligt restore test af driftskritiske systemer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret systemkonfiguration for sikkerhedskopiering. Vi har observeret, at der foretages sikkerhedskopiering af driftskritiske systemer og servere. Vi har observeret, at der foretages sikkerhedskopiering hver time. Vi har inspiceret system for dokumentation af kontroller. Vi har observeret, at der foretages ugentlig kontrol af korrekt sikkerhedskopiering. Vi har observeret, at der sendes notifikation til driftsansvarlig ved afvigelser i sikkerhedskopiering. Vi har observeret, at der er foretaget systemgendannelse af server den 9. september 2022.	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
Hændelseslogning, beskyttelse af logoplysninger, administrator- og operatørlog ▶ Der logges på driftskritisk netværk og servere, logning opsamles og analyseres. ▶ Logning opsamles og sikres i central database. ▶ Alarmer monitoreres og håndteres af IT-ansvarlig. ▶ Kun medarbejdere med arbejdsbetinget behov har adgang til logning. ▶ Systemer er tidssynkroniseret.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for logning. Vi har observeret, at der foretages logning på kritiske servere. Vi har observeret, at logning konsolideres og analyseres i centralt logsystem. Vi har inspiceret e-mailmeddelelser fra logningssystem. Vi har observeret, at der ved væsentlige afvigelser sendes e-mailnotifikationer til it-chef. Vi har inspiceret system for logning. Vi har observeret, at kun medarbejdere med arbejdsbetinget behov har adgang til logsystem. Vi har inspiceret system for logning. Vi har observeret, at der logges på ændringer i kritiske systemfiler. Vi har observeret, at ændringer i system eller oprettelse af brugere udløser notifikation. Vi har inspiceret systemkonfiguration for SQL server og NTP-server. Vi har observeret, at der er konfigureret tidssynkronisering for disse.	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
Softwareinstallation på driftssystemer ▶ Softwareinstallation på driftssystemer er underlagt ændringsstyring.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for ændringsstyring. Vi har observeret, at der er udformet procedure for risikovurdering og reetableringsplan ved implementering af ændringer i driftsmiljø. Vi har inspiceret hændelseslog og observeret, at der er foretaget risikovurdering af ændring før installation af software.	Ingen afvigelser konstateret.
Styring af tekniske sårbarheder ▶ Der indhentes løbende information om sårbarheder i anvendte systemer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret dokumentation for indsamling af oplysninger om sårbarheder og for deltagelse i aktiviteter omkring aktuelle trusler og sårbarheder.	Ingen afvigelser konstateret.
Begrænsninger på softwareinstallation ▶ IT-politikken fastsætter rammer for anvendelse og installation af software. ▶ Installation af software kræver forudgående godkendelse fra virksomhedens ledelse.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt retningslinjer for anvendelse og installation af software. Vi har for en stikprøve inspiceret arbejdsstationer. Vi har observeret, at brugere ikke har adgang til installation af software.	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
Politik for kommunikationssikkerhed ▶ Politik for kommunikationssikkerhed er fastlagt og dokumenteret. ▶ Politik for kommunikationssikkerhed revideres årligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udformet politikker for kommunikationssikkerhed. Vi har observeret, at politikker for kommunikationssikkerhed revideres årligt i forbindelse med revidering af informationssikkerhedspolitikken. Vi har observeret, at politik for kommunikationssikkerhed senest er revideret og godkendt af ledelsen 10. juni 2022. Vi har observeret, at politikker og processer er gennemgået og vurderet samlet d. 9. september 2022.	Ingen afvigelser konstateret.
Netværksstyring ▶ Adgang til netværksenheders konfiguration er kun tildelt medarbejdere med et arbejdsbetinget behov.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret systemkonfiguration for firewall. Vi har observeret, at adgang til konfiguration er tildelt medarbejdere med et arbejdsbetinget behov.	Ingen afvigelser konstateret.
Sikring af netværkstjenester ▶ Adgang til virksomhedens drifts-netværk er beskyttet med kryptering.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret systemkonfiguration for firewall. Vi har observeret, at kommunikation til driftssystemer er beskyttet med VPN. Vi har observeret, at forbindelse er krypteret.	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
Opdeling af netværk ▶ Services eksponeret mod internettet er beskyttet af firewall.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret systemkonfiguration for firewall. Vi har observeret, at der er implementeret trafikfiltrering for adgang til servere.	Ingen afvigelser konstateret.
Elektroniske meddelelser ▶ Databehandleren anvender e-mail til kommunikation med eksterne parter, E-mail kommunikationen er krypteret i transmissionen. ▶ Udgående E-mail kommunikation bliver indholdsscannet ved afsendelse for personfølsomme data.	Vi har udført forespørgsler hos passende personale. Vi har observeret, at databehandleren anvender Microsoft Office 365 til e-mail-kommunikation. Vi har inspiceret system for e-mail. Vi har observeret, at der er tvunget TLS-kryptering af alle udgående e-mails. Vi har inspiceret system for indholdsscanning af e-mail. Vi har observeret, at udgående e-mails bliver scannet for persondata og fortroligt materiale.	Ingen afvigelser konstateret.
Fortroligheds- og hemmeligholdelsesaftaler ▶ Der er indgået skriftlige leverandøraftaler og databehandleraftaler eller underskrevet NDA, hvis leverandør har adgang til eller behandler personoplysninger, fortrolige oplysninger eller følsomme data.	Vi har udført forespørgsler hos passende personale. Vi har ved forespørgsel fået oplyst, at der ikke er indgået nye leverandøraftaler i perioden, hvorfor det ikke har været muligt at efterprøve kontrollen. Vi har inspiceret databehandleraftaler. Vi har observeret, at der er indgået skriftlig aftale og databehandleraftale med underdatabehandler og serviceunderleverandører.	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
Politik for anskaffelse, udvikling og vedligeholdelse af systemer ▶ Politik for anskaffelse, udvikling og vedligeholdelse af systemer er fastlagt og dokumenteret. ▶ Politik for anskaffelse, udvikling og vedligeholdelse af systemer revideres årligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er fastlagt retningslinjer for sikkerhedskrav til anskaffelse, udvikling og vedligeholdelse. Vi har observeret, at politikker for sikkerhedskrav til anskaffelse, udvikling og vedligeholdelse årligt i forbindelse med revidering af informationssikkerhedspolitikken. Vi har observeret, at politikker og processer er gennemgået og vurderet samlet d. 9. september 2022.	Ingen afvigelser konstateret.
Analyse og specifikation af informationssikkerhedskrav ▶ Alle projekter omfattende udvikling eller ændringer af informationssystemer er omfattet af Databehandlerens procedure for udvikling, hvor informationssikkerhedskrav er et obligatorisk område. ▶ Informationssikkerhedskrav dokumenteres i projektdokumentationen. ▶ Ved nyanskaffelser, skift af outsourcing partner, indgåelse af aftale med ny outsourcing partner eller lign. gennemføres en risikovurdering. ▶ Systemer er designet og implementeret, så de sikrer persondatabeskyttelse ved hjælp af standardindstillinger og gennem design af processer og funktionalitet.	Vi har foretaget forespørgsler hos passende personale. Vi har for en stikprøve inspiceret dokumentation for gennemførte udviklingsopgaver. Vi har observeret, at der er foretaget risikovurdering af udviklingsopgaven i forhold til informationssikkerhed og påvirkning for den registrerede. Vi har observeret, at krav til og resultatet af risikovurderingen er dokumenteret i projektdokumentation. Vi har inspiceret procedure for udvikling og idriftsættelse. Vi har observeret, at risikovurdering opdateres ved væsentlige ændringer i organiseringen og it-systemer. Vi har observeret, at ændringer i serviceunderleverandører og underdatabehandlere medfører fornyet risikovurdering af trusler, der er identificeret	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
	i trusselskataloget og tilknyttet serviceunderleverandører og underdatabehandlere. Vi har for en stikprøve inspiceret risikovurdering af ændringer. Vi har observeret, at der er foretaget vurdering i forhold til, om der skal gennemføres risikovurdering. Vi har inspiceret procedure for projektdokumentation. Vi har observeret, at der er opsat krav til risikovurdering og informationssikkerhedskrav, herunder Privacy by default og Privacy by design.	
Sikker udviklingspolitik - Alle projekter dokumenteres.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for dokumentation af projekter. Vi har observeret, at der er procedure for dokumentation af projekter. Vi har inspiceret system for Pipeline management. Vi har observeret, at projekter, der er registreret i udvikling, er dokumenteret.	Ingen afvigelser konstateret.
Principper for udvikling af sikre systemer - Alle opgaver eller ændringer i Systemer vurderes for påvirkning i forhold til behandling af persondata. - Privacy by design og Privacy by default sikres ved ændringer, der berører persondata. - Virksomheden gennemfører systemgodkendelsestest på komponenter og integrerede systemer før idriftsættelse.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret politikker og procedurebeskrivelser. Vi har observeret, at der ved opstart af projekter foretages vurdering af projektets påvirkning i forhold til persondata. Vi har observeret, at design og standardindstillinger er obligatoriske for vurdering ved opstart af projekter.	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 observeret, at der gennemføres automatiseret test af kildekode før installation i driftsmiljø.	
Adskillelse af udviklings-, test og driftsmiljøer - Regler for overførsel af software fra udvikling til drift er beskrevet i politik for ændringsstyring. - Udviklingstest og driftsmiljøer for driftskritiske systemer er adskilt. - Ændringer testes i et adskilt miljø før idriftsættelse. - Der opbevares ikke data i udviklings- / testmiljø. - Kun IT-chef har beføjelse til installation og/eller ændringer af software. - Ved deployment af software sendes notifikation til CTO.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret overførsel af software fra udvikling til drift. Vi har observeret, at der er udformet og implementeret procedure for deployment, test af udviklingsprojekter, bugfixes samt overførsel af software fra udvikling til drift. Vi har inspiceret produktions- og testmiljø. Vi har observeret, at der er adskillelse mellem test- og produktionsmiljø. Vi har observeret, at test og udvikling sker på separate servere. Vi har for en stikprøve inspiceret system for test af kildekode. Vi har observeret, at der er gennemført automatiseret integrationstest i staging-miljø før overførsel af software fra udvikling til drift. Vi har inspiceret dokumentation for notifikation ved deployment i driftsmiljø. Vi har observeret, at it-chef bliver notificeret, når der sendes ny kildekode til driftsmiljø, før dette bliver deployment. Vi har inspiceret databaser i udviklings- og testmiljø. Vi har observeret, at data i tabeller er anonymiseret. Vi har inspiceret adgangssystemer for adgang til kildekode og udviklingsværktøjer samt privilegeret adgang til servere.	Vi har konstateret, at der ikke er implementeret funktionsadskillelse, relateret til ændring og overførsel af software fra udvikling til drift. Dette idet udviklere er tildelt privilegeret adgang til produktionsservere. Ingen yderligere afvigelser konstateret.

A.15: Leverandørforhold

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Overholdelse af aftaler/håndtering af sikkerhed i leverandøraftaler ▶ Det kræves, at leverandørernes informationssikkerhedsniveau lever op til kravene i Databehandlerens informations-sikkerhedspolitik. Dette sikres gennem kontrakter, NDA eller Databehandleraftale. ▶ Underdatabehandler skal forpligte sig til at dokumentere overholdelse af Databehandlerens informationssikkerhedspolitik. ▶ Underdatabehandler skal forpligte sig til at informere Databehandleren omkring informationssikkerhedshændelser. ▶ Databehandleren indhenter og gennemgår en gang årligt, ISAE 3000, ISAE 3402 eller SOC-2 revisor erklæring for leverandører af driftskritiske ydelser.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret samarbejdsaftale med GlobalConnect A/S, der er serviceunderleverandør. Vi har inspiceret databehandleraftale og samarbejdsaftale med Global Connect A/S, Nordicode ApS, Visma Consulting A/S og FrontSafe A/S. Vi har observeret, at databehandleren har adgang til at udføre revision af processer og kontroller relateret til den enkelte aftale. Vi har ligeledes observeret, at underdatabehandlere er forpligtet til at informere databehandleren om informationssikkerhedshændelser. Vi har desuden observeret, at underdatabehandlere er forpligtet til at lade databehandleren foretage auditering af underdatabehandlerens processer og kontroller. Vi har inspiceret dokumentation for tilsyn med underdatabehandlere. Vi har observeret, at der er ført tilsyn med underdatabehandlere, og at dette er sket ved fysisk inspektion af kontorlokaler og interview med underdatabehandlere. Vi har foretaget inspektion af dokumentation herfor. Vi har inspiceret dokumentation for indhentelse og vurdering af eksterne revisorerklæringer fra underdatabehandlere og serviceunderleverandør. Vi har inspiceret samarbejdsaftale med serviceunderleverandøren Global Connect A/S som underserviceleverandør. Vi har observeret, at der er indgået aftale om co-lokation.	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
	Vi har observeret, at der er indhentet ISAE 3402-erklæring Global Connect A/S som led i overvågningen af funktionaliteten af dennes kontroller. Vi har inspiceret ISAE 3402 erklæring fra Global Connect A/S for perioden fra 1. januar til 31. december 2021. Vi har observeret, at denne er uden væsentlige bemærkninger eller forbehold fra den afgivende revisor. Vi har inspiceret ISAE 3402-erklæring fra FrontSafe A/S for perioden fra 1. oktober 2020 til 30. november 2021. Vi har observeret, at denne er uden væsentlige bemærkninger eller forbehold fra den afgivende revisor. Vi har observeret, at der er indhentet ISAE 3000-erklæring fra Visma Consulting ApS for perioden 1. april 2021 til 31. marts 2022. Vi har observeret, at denne er uden væsentlige bemærkninger eller forbehold fra den afgivende revisor. Vi har inspiceret dokumentation for tilsyn med Nordicode ApS. Vi har observeret, at Nordicode ApS er instrueret i databehandling og informationssikkerhedspolitik. Vi har observeret, at der er foretaget fysisk inspektion den 22. april 2022. Vi har ved forespørgsel fået bekræftet, at inspektionen er sket hos Nordicode ApS i forbindelse med tilsyn.	
Styring af ændringer af leverandørydelser ▶ Ved væsentlig ændring af leverance, ejerforhold, økonomiske, organisatoriske og andre sikkerhedsmæssige forhold hos leverandøren, skal serviceydelse risikovurderes på ny af Databehandleren.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udformet politikker for leverandørstyring. Vi har inspiceret dokumentation for foretagne risikovurderinger af Global Connect, Frontsafe samt VISMA.	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
Rapportering af informationssikkerhedshændelse ▶ Alle Informationssikkerhedshændelser, svagheder og brud indrapporteres til ledelsen. ▶ Alle Informationssikkerhedshændelser, svagheder og brud registreres af ledelsen i hændelseslog. ▶ Alle informationssikkerhedshændelser vurderes i forhold til fortrolighed, integritet og tilgængelighed.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret procedure for indrapportering af informationssikkerhedshændelser. Vi har observeret, at der er udformet en procedure for rapportering af informationssikkerhedshændelser. Vi har inspiceret dokumentation for hændelser. Vi har observeret, at der i perioden er indrapporteret en informationssikkerhedshændelse, men ikke brud på informationssikkerheden. Vi har ligeledes observeret, at hændelsen er mitigeret. Vi har observeret, at der er foretaget en vurdering af den indrapporterede hændelse i forhold til, om der er sket brud på persondatasikkerhed.	Ingen afvigelser konstateret.
Håndtering af informationssikkerhedsbrud ▶ Informationssikkerhedsbrud håndteres efter en fastlagt procedure. ▶ Logning og andre beviser sikres i forbindelse med registrering af informationssikkerhedsbrud.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret informationssikkerhedspolitik. Vi har observeret, at der er udformet en procedure for håndtering af informationssikkerhedshændelser og brud, som foreskriver, at brud på persondatasikkerhed skal rapporteres uden unødig forsinkelse til dataansvarlig. Vi har inspiceret oversigt over informationssikkerhedsbrud. Vi har for en stikprøve, inspiceret dokumentation for informationssikkerhedsbrud. Vi har observeret, at informationssikkerhedsbrud er håndteret i henhold til procedure.	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
Erfaringer fra informationssikkerhedsbrud ▶ Virksomhedens ledelse gennemgår årligt hændelsesloggen og iværksætter forbedringer af informationssikkerheden.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret system for dokumentation af kontroller. Vi har observeret, at der er udformet en procedure for gennemgang af alle informationssikkerhedshændelser og evaluering af disse. Vi har inspiceret system for dokumentation af databehandlerens kontroller. Vi har inspiceret system for dokumentation af selskabets kontroller. Vi har observeret, at der er foretaget gennemgang af selskabets hændelseslog. Vi har observeret, at kontrollen er gennemført d. 10. juli 2022.	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
Planlægning af informationssikkerhedskontinuitet ▶ Der er på baggrund af risikovurdering etableret en plan for informationssikkerhedskontinuitet.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret beredskabsplan. Vi har observeret, at der er udformet og implementeret beredskabsplan ud fra en risikovurdering for drift af informationsaktiver. Vi har observeret, at beredskabsplanen er revideret i august 2022.	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
Implementering af informationssikkerhedskontinuitet ▶ Organisations- og ledelsesstruktur under nødberedskab er specificeret i procedure for nød-, beredskabs- og reetableringsstyring. ▶ Der er udarbejdet en overordnet beredskabsplan, der beskriver den overordnede procedure for iværksættelse af beredskab og organisering af beredskab. ▶ Roller og ansvar i forbindelse med aktivering af beredskab er kommunikeret til relevante personer; herunder information om placering af nødvendige beskrivelser og information. ▶ Der er udarbejdet procedure og arbejdsbeskrivelser for reetablering af driftskritiske systemer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret beredskabsplaner. Vi har observeret, at ledelsesstruktur er specificeret i beredskabsplan. Vi har observeret, at der er udarbejdet en overordnet beredskabsplan med procedure for iværksættelse og organisering af beredskab. Vi har ligeledes observeret, at roller og ansvar i forbindelse med beredskab er fastlagt og kommunikeret til relevante medarbejdere. Vi har observeret, at der er udarbejdet en arbejdsbeskrivelse for trinvis reetablering af driftssystemer.	Ingen afvigelser konstateret.
Verificering, gennemgang og evaluering af informationssikkerhedskontinuitet ▶ Beredskabsplaner revideres en gang årligt ved implementering af nye systemer eller ændringer i risikovurderingen. ▶ Beredskabsplaner afprøves efter en fastlagt rotationsplan. Afprøvning af beredskabsplaner er planlagt i årshjul.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret databehandlerens årshjul for kontroller. Vi har observeret, at der er udformet procedurer for årlig revidering af beredskabsplaner. Vi har observeret, at beredskabsplanen er revideret i august 2022. Vi har inspiceret dokumentation for test af beredskabsplan og observeret, at den er afholdt 9. december 2021.	Ingen afvigelser konstateret.
Tilgængelighed af informationsbehandlingsfaciliteter ▶ Driftskritiske systemer er virtualiseret. ▶ Beredskabsplaner opbevares på flere fysiske lokationer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret systemkonfiguration for XEN-server. Vi har observeret, at databehandlerens systemer er virtualiseret.	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
	Vi har inspiceret system for opbevaring af dokumentation. Vi har observeret, at beredskabsplaner er opbevaret i filsystem. Vi har ligeledes observeret, at beredskabsplanen opbevares i fysisk udskrift på kontoret.	

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
Kontrol - Bistand til den dataansvarlige ▶ Databehandleren har udformet og implementeret procedurer for bistand til den dataansvarlige med opfyldelse af de registreredes rettigheder. ▶ Databehandleren har udformet og implementeret procedurer for bistand til den dataansvarlige i forhold til revision og inspektion. ▶ Databehandleren har udformet og implementeret procedurer for bistand til den dataansvarlige i forhold til overholdelse af særlige krav i forordningen, herunder bistand i forhold til artikel 32 – 36.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret databehandleraftale og politikker. Vi har observeret, at der er udformet procedurer for bistand til den dataansvarlige i relation til den registreredes rettigheder. Vi har ligeledes observeret, at der er udformet standardprocedure for registrering af anmodninger fra dataansvarlige. Vi har ved forespørgsel fået oplyst, at databehandleren ikke har modtaget en anmodning fra en dataansvarlig vedrørende registreredes rettigheder i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollernes effektivitet. Vi har observeret, at der er udformet politikker og procedurer for den dataansvarliges adgang til gennemførelse af revision og inspektion. Vi har inspiceret databehandleraftale og procedurer for bistand til den dataansvarlige, jf. databeskyttelsesforordningens artikel 32 til 36, herunder behandlingssikkerhed, anmeldelse og underretning ved brud på persondatasikkerhed samt konsekvensanalyse. Vi har ved forespørgsel fået oplyst, at databehandleren ikke er blevet anmodet om at bistå med de anførte forpligtelser i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollernes effektivitet.	Ingen afvigelser konstateret.
Kontrol - Sletning og tilbagelevering af personoplysninger ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret procedure og politikker for sletning og tilbagelevering af data til dataansvarlige. Vi har observeret, at der er udarbejdet procedure for sletning af data ved ophør af kundeforhold.	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 log for sletning og foretaget inspektion af databaser for registrering af personoplysninger. Vi har observeret, at der er foretaget sletning af personoplysninger i henhold til procedure. Vi har observeret, at der er planlagt gennemgang af procedurer for sletning mindst én gang årligt.	
Kontrol - Databehandleraftaler ▶ Der er udformet og implementeret en procedure for indhentelse og vurdering af databehandleraftaler. ▶ Underdatabehandlere er angivet i databehandleraftale med dataansvarlige. ▶ Databehandleraftaler underskrives af dataansvarlige og databehandler samt arkiveres elektronisk.	Vi har udført forespørgsler hos passende personale. Vi har observeret, at der anvendes en standarddatabehandleraftale ved indgåelse af databehandleraftaler med dataansvarlige og underdatabehandlere. Vi har observeret, at underdatabehandlere er angivet i skabelon for databehandleraftale med dataansvarlige. Vi har for en stikprøve inspiceret databehandleraftaler. Vi har observeret, at databehandleraftaler er udformet i henhold til databeskyttelsesforordningens artikel 28, stk. 2. Vi har observeret, at databehandleraftale er underskrevet af dataansvarlig og databehandlerens ledelse. Vi har ligeledes observeret, at databehandleraftaler opbevares elektronisk.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 80