DØGNDATA APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. SEPTEMBER 2021 TIL 31. AUGUST 2022 OM BESKRIVELSEN AF SOFUSMATCH, DAGBOGSPROGRAMMET OG SOFUSKONTAKTPERSONER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. SEPTEMBER 2021 TIL 31. AUGUST 2022 OM BESKRIVELSEN AF SOFUSMATCH, DAGBOGSPROGRAMMET OG SOFUSKONTAKTPERSONER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Døgndata ApS
Døgndata ApS kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Døgndata ApS (databehandleren) for hele perioden fra 1. september 2021 til 31. august 2022 udarbejdede beskrivelse i sektion 3 af SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER 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 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.

Oplysningerne i sektion 5 - Supplerende informationer fra Døgndata ApS, er ikke en del af Døgndata ApS´s beskrivelse af ydelser. Information i afsnit 5 har ikke været genstand for de procedurer, der udføres af BDO ved gennemgangen af beskrivelsen i sektion 3.

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 SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER, 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 SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret i hele perioden fra 1. september 2021 til 31. august 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. september 2021 til 31. august 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. september 2021 til 31. august 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 SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER, 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 databeskyttelses-forordningen og databeskyttelsesloven er overholdt.

København, den 19. september 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. DØGNDATA APS´ UDTALELSE

Døgndata ApS varetager behandling af personoplysninger i forbindelse med SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER 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 SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER, 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.

Døgndata ApS anvender underdatabehandler. Denne underdatabehandlers relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Døgndata ApS bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden fra 1. september 2021 til 31. august 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at begrænse behandling af personoplysninger.
    - De processer der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - De processer der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
    - De processer der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
    - De processer der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
    - De kontroller, som vi med henvisning til afgrænsningen af SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER 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 SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden fra 1. september 2021 til 31. august 2022.

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

Døgndata 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. september 2021 til 31. august 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. september 2021 til 31. august 2022.

Døgndata 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 databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Aarhus, den 19. september 2022

Døgndata ApS

Martin Lyngby Hansen
Administrerende direktør

3. DØGNDATA APS´ BESKRIVELSE AF SOFUSMATCH, DAGBOGSPROGRAMMET OG SOFUSKONTAKTPERSONER

DØGNDATA APS

Døgndata ApS er en virksomhed, der udvikler og driver en række online systemer til varetagelse af dokumentation og kommunikation inden for det sociale område, primært anbringelsesområdet, til såvel kommuner som forskellige brancher på det private marked. Døgndata ApS har kontor i Aarhus.

Døgndata ApS' ca. 10 medarbejdere er specialiserede inden for systemudvikling, serverdrift, support og informationssikkerhed, og organiseret i en udviklingsafdeling, drift- og supportafdeling, økonomiafdeling og en administrationsafdeling.

Administrationsafdelingen styrer Døgndata ApS' persondatasikkerhed i forhold til den behandling, som Døgndata ApS varetager på vegne af sine kunder, der er er dataansvarlige. Døgndata ApS' ansvarsområder omfatter indgåelse af databehandleraftaler, besvarelse af henvendelser fra den dataansvarlige, underretning om brud på persondatasikkerheden, efterlevelse af interne politikker og procedurer og lignende.

SOFUSMATCH, DAGBOGSPROGRAMMET OG SOFUSKONTAKTPERSONER OG BEHANDLING AF PERSONOPLYSNINGER

Døgndata ApS leverer Sofus Match, Dagbogsprogrammet og SofusKONTAKTPERSONER som en Software-as-a-Service (SaaS) løsning i henhold til indgået kontrakt med kommuner og private virksomheder. Programmerne kan tilgås fra såvel stationære som mobile enheder. Programmerne anvendes af kommuner og private aktører til dokumentation og kommunikation i forbindelse med deres varetagelse af opgaver inden for det sociale område, primært anbringelsesområdet. Opgavevaretagelsen er reguleret via Serviceloven.

Sofus Match, Dagbogsprogrammet og SofusKONTAKTPERSONER udvikles i Danmark, og afvikles hos Netic A/S´ hosting-center i Aalborg Øst. Der benyttes ikke andre underdatabehandlere. Døgndata ApS har indgået databehandleraftaler med denne underdatabehandler.

Døgndata ApS behandler personoplysninger på vegne af sine kunder, der er dataansvarlige, når disse anvender Sofus Match, Dagbogsprogrammet og/eller SofusKONTAKTPERSONER. Døgndata ApS har indgået databehandleraftaler med de dataansvarlige om denne behandling.

De personoplysninger, der behandles, henhører under databeskyttelsesforordningens artikel 6 om almindelige personoplysninger og omfatter blandt andet personnavn, e-mail, telefonnummer og identifikation. Samt databeskyttelsesforordningen artikel 9 om følsomme personoplysninger.

STYRING AF PERSONDATASIKKERHED

Døgndata ApS har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

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

DATABEHANDLERAFTALEN	KONTROLOMRÅDE	Artikel
Kontrolmål A Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.	• Instruks for behandling af personoplysninger • Efterlevelse af instruks for behandling af personoplysninger • Underretning af den dataansvarlige ved ulovlig instruks	• Artikel 28, stk. 3 • Artikel 28, stk. 3, litra a • Artikel 29 • Artikel 32, stk. 4 • Artikel 28, stk. 10 • Artikel 28, stk. 3, litra h
Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Politikker og procedure • Risikovurdering • Antivirusprogram • Firewall • Netværkssikkerhed • Logisk adgangskontrol • Overvågning • Eksterne kommunikationsforbindelser • Logning i systemer, databaser og netværk • Personoplysninger i udviklings- og testmiljø • Sårbarhedsscanninger og penetrationstest • Vedligeholdelse af systemsoftware • Fysisk sikkerhed • Sikkerhedskopiering og retablering af data • Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse	• Artikel 28, stk. 3, litra c • Artikel 25
Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Informationssikkerhedspolitik • Styring af informationssikkerhed • Rekruttering af medarbejdere • Tavsheds- og fortrolighedsaftale med medarbejdere • Fratrædelse af medarbejdere • Opretholdelse af tavshedspligt ved fratrædelse • Awareness-træning for medarbejdere • Fortegnelse over kategorier af behandlingsaktiviteter • Bistand til den dataansvarlige vedrørende artikel 32-36 • Bistand til den dataansvarlige i forhold til revision og inspektion • Udpegelse af databeskyttelsesrådgiveren	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra b • Artikel 28, stk. 3, litra f • Artikel 28, stk. 3, litra h • Artikel 30, stk. 2, 3 og 4
Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.	• Sletning af personoplysninger • Opbevaring • Ophør af aftalen med den dataansvarlige	• Artikel 28, stk. 3, litra g
Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	• Opbevaring af personoplysninger • Lokation for opbevaring af personoplysninger	• Artikel 28, stk. 3, litra c
Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.	• Underdatabehandleraftaler og instruks • Godkendelse af underdatabehandlere • Ændringer i godkendte underdatabehandlere • Underdatabehandlerens databeskyttelsesforpligtelser • Oversigt over godkendte underdatabehandlere • Tilsyn med underdatabehandlere	• Artikel 28, stk. 2 og 4

DATABEHANDLERAFTALEN	KONTROLOMRÅDE	Artikel
Kontrolmål H Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.	• Bistand til den dataansvarlige i forhold til de registreredes rettigheder	• Artikel 28, stk. 3, litra e
Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.	• Underretning om brud på persondatasikkerheden • Identifikation af brud på persondatasikkerheden • Registrering af brud på persondatasikkerheden • Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden	• Artikel 33, stk. 2 • Artikel 28, stk. 3, litra f

RISIKOVURDERING

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

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

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

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

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

Databehandleraftale

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

Instruks for behandling af personoplysninger

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

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering
Døgndata ApS har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom.

Fysisk sikkerhed
Døgndata ApS har outsourcet drift af servere og databaser til underleverandøren Netic A/S. Døgndata har indført procedurer, der sikrer, at der føres periodisk kontrol med Døgndata ApS' krav til fysisk sikkerhed. Døgndata ApS indhenter årligt en ISAE 3402 type 2-erklæring fra Netic A/S. Erklæringen gennemgås og vurderes på møder i Døgndata ApS' sikkerhedsudvalg.

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

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

Eksterne kommunikationsforbindelser
Døgndata ApS har indført procedurer, der sikrer, at ekstern adgang til applikationerne er krypterede med SSL-kryptering.

Kryptering af personoplysninger
Døgndata ApS har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

Døgndata ApS har indført procedurer, der sikrer, at data på personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, er krypteret ved ibrugtagning, så adgang til data alene er mulig for autoriserede brugere. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

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

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

Netværkssikkerhed
Døgndata ApS har indført procedurer, der sikrer, at produktions-, udviklings- og testmiljøerne er adskilte fra hinanden for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.

Døgndata ApS har outsourcet driften af servere og databaser til underleverandøren Netic A/S. Døgndata ApS indhenter årligt relevante revisionserklæringer fra underleverandøren for at sikre, at Netic A/S har fået udført sårbarhedsscanninger og penetrationstest på netværk.

Antivirusprogram
Døgndata ApS har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselsniveau, og der er opsat en løbende overvågning af disse systemer, herunder periodisk test for funktionalitet.

Vedligeholdelse af systemsoftware
Døgndata ApS har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og software installeret på arbejdsstationer.

Logning i systemer, databaser og netværk
Døgndata ApS har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret mod tab og sletning.

Overvågning
Døgndata ApS har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Afprøvning, vurdering og evaluering
Døgndata ApS har indført procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden. Dette sker på møder i Døgndata ApS' sikkerhedsudvalg.

Sikkerhedskopiering og reetablering af data
Døgndata ApS har outsourcet driften af sikkerhedskopiering af systemer og databaser til underleverandøren Netic A/S. Døgndata ApS udfører restore-test to gange årligt af sikkerhedskopier for at sikre, at sikkerhedskopier kan indlæses.

Beredskabsplaner
Døgndata ApS har etableret beredskabsplaner, således at Døgndata ApS rettidigt kan oprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. Beredskabsplanerne afprøves og revideres løbende i forbindelse med ændringer i systemer mv.

Databeskyttelse gennem design og standardindstillinger

Døgndata ApS har indført politikker og procedurer for udvikling og vedligeholdelse af SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER, der sikrer en styret ændringsproces. Der anvendes et Change Management system til styring af udviklings- og ændringsopgaver, og enhver opgave følger en ensartet proces, der indledes med risikovurdering i overensstemmelse med kravene om databeskyttelse gennem design og standardindstillinger.

Udviklings-, test- og produktionsmiljø er adskilte, og der er etableret funktionsadskillelse mellem medarbejdere i udviklingsafdelingen og i drifts- og supportafdelingen. Enhver udviklings- og ændringsopgave gennemløber et testforløb, og der anvendes genererede data som testdata. Der er indført procedurer for versionskontrol, logning og sikkerhedskopiering, således at det er muligt at geninstallere tidligere versioner.

Databehandlerens garantier

Døgndata ApS har indført politikker og procedurer, der sikrer, at Døgndata ApS kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. Døgndata ApS har etableret en organiseringen af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres. Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for uddannelse og instruktion af medarbejdere, der behandler personoplysninger, herunder gennemførelse af awareness og oplysningskampagner.

Fortrolighed

Døgndata ApS har indført politikker og procedure, der sikrer fortrolighed ved behandlingen af personoplysninger. Alle medarbejdere i Døgndata ApS har forpligtet sig til fortrolighed ved at underskrive en ansættelseskontrakt, der indeholder vilkår om tavshed og fortrolighed.

Døgndata ApS har etableret procedurer til sikring af, at medarbejdere underrettes om, at fortrolighedsaftalens fortsat er gyldig efter ophør af ansættelse.

Bistand til den dataansvarlige i forhold til behandlingssikkerhed og konsekvensanalyse

Døgndata ApS har indført politikker og procedurer, der sikrer, at Døgndata ApS kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed og artikel 36 om konsekvensanalyser.

Bistand til den dataansvarlige i forhold til revision og inspektion

Døgndata ApS har indført politikker og procedurer, der sikrer, at Døgndata ApS kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige. Døgndata ApS giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

Fortegnelse over kategorier af behandlingsaktiviteter

Døgndata ApS har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

Sletning og tilbagelevering af personoplysninger

Døgndata ApS har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige. Data hos kommunerne er underlagt Arkivloven, og slettereglerne i Arkivloven har forrang i forhold til sletteregleme i GDPR og Persondataloven. Det medfører, at disse data ikke må slettes, før der er lavet en arkivversion af data, hvilket skal ske senest efter fem år, eller ved kundens ophør at anvendelsen af tjenesten.

Opbevaring af personoplysninger

Døgndata ApS har indført procedurer, der sikrer, at opbevaring af personoplysninger alene foretages i overensstemmelse med kontrakten med den dataansvarlige og listen over lokationer i den tilhørende databehandleraftale.

Underdatabehandlere

Døgndata ApS har indført politikker og procedurer, sikrer, at underdatabehandlere er blevet pålagt de samme databeskyttelsesforpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og Døgndata ApS, og at underdatabehandlerne kan give tilstrækkelige garantier til beskyttelse af personoplysninger. Procedurer sikrer, at den dataansvarlige giver en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere, herunder at der sker en styring af ændringer i godkendte underdatabehandlere.

Døgndata ApS vurderer underdatabehandleren og dennes garantier, forinden der indgås aftale, for at sikre, at underdatabehandleren kan overholde de forpligtelser, som er pålagt Døgndata ApS. Døgndata ApS fører et årligt tilsyn med sine underdatabehandlere, baseret på en risikovurdering af den konkrete behandling af personoplysninger, ved blandt andet at indhente revisorerklæringer af typen ISAE 3000, ISAE 3402 eller SOC 2 eller lignende dokumentation.

Bistand til den dataansvarlige i forhold til den registreredes rettigheder

Døgndata ApS har indført politikker og procedurer, der sikrer, at Døgndata ApS kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

Underretning om brud på persondatasikkerheden

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

Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden

Døgndata ApS har indført politikker og procedurer, der sikrer, at Døgndata ApS kan bistå den dataansvarlige med artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden.

Udpegelse af databeskyttelsesrådgiveren

Døgndata ApS har på baggrund af behandlingsaktiviteterne valgt at ansætte en ekstern databeskyttelsesrådgiver. Døgndata ApS har vurderet databeskyttelsesrådgiverens kompetencer, og vurderer at denne har kompetence til at udføre sin rolle.

ÆNDRINGER I PERIODEN FRA 1. SEPTEMBER 2021 TIL 31. AUGUST 2022

Døgndata ApS har ikke foretaget væsentlige ændringer i SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i perioden fra 1. september 2021 til 31. august 2022:

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

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

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

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i Døgndata ApS´ beskrivelse af SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER 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 Døgndata 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. september 2021 til 31. august 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 Netic A/S som underdatabehandler inden for hosting, har vi modtaget ISAE 3402 og ISAE 3000 type 2-erkæringer for perioden fra 1. januar til 31. december 2021 på henholdsvis generelle it-kontroller for hosting- og driftsydelser, samt efterlevelse af databeskyttelsesloven og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger.

Denne underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Døgndata ApS' beskrivelse af SofusMATCH, Dagbogsprogrammet og SofusKONTAKTPERSONER og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos Døgndata ApS, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

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

En afvigelse foreligger, når:

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

Kontrolområde A		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
A.1 - Instruks for behandling af personoplysninger ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for behandling af personoplysninger og standardskabeloner for databehandleraftaler og observeret, at der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling efter instruks fra den dataansvarlige. Vi har inspiceret sikkerhedshåndbogen og observeret, at persondatapolitikken gennemgås minimum to gange årligt. Vi har inspiceret dokumentation for gennemgang af persondatapolitikken og observeret, at persondatapolitikken er gennemgået to gange i erklæringsperioden.	Ingen afvigelser konstateret.
A.2 - Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens beskrivelse og standardskabeloner for databehandleraftaler. Vi har stikprøvevis inspiceret indgåede databehandleraftaler og observeret, at behandlingen af personoplysninger skal ske på baggrund af instruks i indgåede databehandleraftaler. Vi har inspiceret referat af afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at det kontrolleres, at behandling af personoplysninger foregår på baggrund af indgåede databehandleraftaler med dertilhørende instruks.	Ingen afvigelser konstateret.
A.3 - Underretning af den dataansvarlige ved ulovlig instruks		

Kontrolområde A		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevis inspiceret indgåede databehandleraftaler og observeret, at databehandleren er forpligtet til at underrette den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. Vi har på forespørgsel fået oplyst, at der ved revisionens afslutning ikke har været hændelser vedrørende ulovlig instruks. Vi har derfor ikke kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
B.1 - Politikker og procedurer ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standardskabeloner for databehandleraftaler, informationssikkerhedspolitik og sikkerhedshåndbog. Vi har observeret, at der foreligger skriftlige procedurer, som indeholder krav om, at der etableres de aftalte sikringsforanstaltning i overensstemmelse med indgåede databehandleraftaler. Vi har inspiceret seneste referat fra møde i databehandlerens sikkerhedsudvalg og observeret, at databehandleren foretager vurdering af, om procedurerne skal opdateres.	Ingen afvigelser konstateret.
B.2 - Risikovurdering ▶ Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens risikovurdering og observeret, at databehandleren har vurderet identificerede risici ud fra sandsynlighed og konsekvenser. Vi har ved en udvalgt stikprøve observeret, at der er implementeret de tekniske sikkerhedsforanstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, samt de aftalte sikkerhedsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret.
B.3 - Antivirusprogram ▶ Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har på forespørgsel fået oplyst, at databehandleren har opsat overvågning til sikring af, at arbejdsstationer, der anvendes til behandling af personoplysninger, har installeret antivirusprogram, som løbende opdateres. Vi har inspiceret dokumentation for overvågning i værktøjet Kolide og observeret, at arbejdsstationer har installeret opdateret antivirusprogram. Vi har på forespørgsel fået oplyst, at opdatering af antivirusprogram på systemer og databaser er outsourcet til hosting-leverandøren Netic A/S. Vi har inspiceret indgået aftale om it-driftsydelser mellem databehandleren og Netic A/S og observeret, at Netic A/S er forpligtet til at foretage patching. Vi har inspiceret ISAE 3402 type 2-erklæring fra Netic A/S for perioden fra 1. januar til 31. december 2021. Vi har inspiceret, at databehandleren har tilkøbt antivirusservice på databehandlerens servere hos Netic A/S.	
B.4 - Firewall ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværksdiagram og observeret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall. Vi har inspiceret databehandlerens opsætning af jumphosts, og observeret, at tilgang til servere kræver SSH-nøgle.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret listen over medarbejdere med SSH-krypteringsnøgler, og observeret at kun et begrænset antal medarbejdere hos databehandleren har adgang.	
B.5 - Netværkssikkerhed ▶ Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværksoversigt og observeret, at databehandlerens produktions-, test- og udviklingsmiljøer er segmenterede på forskellige servere. Vi har inspiceret, at databehandleren har opsat produktions-, test- og udviklingsmiljøer på segmenterede servere.	Ingen afvigelser konstateret.
B.6 - Logisk adgangskontrol ▶ Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor. ▶ Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov. ▶ Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker ved minimum ved anvendelse af to-faktor autentifikation.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedshåndbog og observeret, at adgang til personoplysninger kun må tildeles medarbejdere med et arbejdsbetinget behov, og at disses adgange skal revurderes minimum én gang årligt. Vi har inspiceret databehandlerens liste over medarbejdere og adgangsrettigheder. Vi har på forespørgsel fået bekræftet, at adgange kan begrundes i arbejdsbetingede behov. Vi har inspiceret referat af afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at medarbejdernes adgangsrettigheder er blevet gennemgået på mødet.	Vi har konstateret, at kravet om to-faktor autentifikation i ca. 3 måneder i erklæringsperioden har være deaktiveret for administrative brugere. Det er oplyst, at traditionelt login med anvendelse af bruger-id og password har været anvendt i perioden. Ingen yderligere afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret databehandlerens liste over medarbejdere og observeret, at der ikke er fratrådt medarbejdere i erklæringsperioden. Vi har observeret, at kravet om to-faktor autentifikation har været deaktiveret i erklæringsperioden i ca. 3 måneder for administrative brugere. Vi har inspiceret, at to-faktor autentifikation er blevet genetableret straks efter at databehandleren er blevet opmærksom på kontrolsvagheden.	
B.7 - Overvågning ▶ Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: ○ Overvågning af systemanvendelse ○ Auditlogning ○ Fejllogning	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren modtager notifikationer på e-mail i tilfælde af problemer i relation til systemanvendelsen fra hosting-leverandøren Netic A/S. Vi har inspiceret dokumentation på notifikationer og observeret, at databehandleren alarmeres i tilfælde af problemer i relation til systemanvendelsen. Vi har inspiceret dokumentation for opsætning af auditlogning og observeret, at databehandleren foretager logning af alle aktiviteter på serveren. Vi har på forespørgsel fået oplyst, at databehandleren anvender værktøjet Sentry til fejllogning på produktionsserveren, og at loggen gennemgås på møder i sikkerhedsudvalget. Vi har inspiceret referat fra mødet i sikkerhedsudvalget observeret, at audit- og fejllogning er gennemgået på mødet.	Ingen afvigelser konstateret.
B.8 - Eksterne kommunikationsforbindelser	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har på forespørgsel fået oplyst, at databehandleren ikke anvender e-mail til transmission af fortrolige og følsomme personoplysninger. Vi har inspiceret dokumentation for kryptering ved transmission via internettet og observeret, at databehandlerens system er krypteret med SSL-kryptering.	
B.9 - Logning i systemer, databaser og netværk ▶ Der er etableret logning i systemer, databaser og netværk af følgende forhold: ○ Aktiviteter der udføres af brugeren i databehandlerens systemer. ○ Ændring i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk ▶ Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for opsætning af logning i systemer, databaser og netværk og observeret, at alle aktiviteter i databehandlerens systemer logges. Vi har inspiceret, at logfiler blev gennemgået på afholdte sikkerhedsmøde.	Ingen afvigelser konstateret.
B.10 - Personoplysninger i udviklings- og testmiljø ▶ Der anvendes ikke personoplysninger til udvikling, test eller lignende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren ikke anvender personoplysninger til udvikling, test eller lignende. Vi har inspiceret databehandlerens script til generering af testdata og observeret, at der genereres fiktive data.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
B.11 - Sårbarhedsscanning ▶ De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren har outsourcet driften af servere og databaser til Netic A/S. Vi har inspiceret ISAE 3402 og 3000 type 2-erklæring fra Netic A/S for perioden fra 1. januar til 31. december 2021, omhandlende de generelle it-kontroller med henblik på at observere, om der er udført sårbarhedsscanninger på databehandlerens netværk hos underdatabehandleren. Vi har inspiceret, at databehandleren har fået gennemført løbende sårbarhedsscanninger af Visma.	Ingen afvigelser konstateret.
B.12 - Vedligeholdelse af systemsoftware ▶ Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren anvender værktøjet Kolide til overvågning af, at arbejdsstationer, der anvendes til behandling af personoplysninger, modtager relevantes opdateringer og patches. Vi har inspiceret udtræk fra Kolide og observeret, at arbejdsstationer løbende modtager opdateringer og patches. Vi har på forespørgsel fået oplyst, at opdateringer og patching af servere og databaser, der anvendes til behandling af personoplysninger, er outsourcet til hosting-leverandøren Netic A/S. Vi har inspiceret indgået aftale om it-driftsydelser mellem databehandleren og Netic A/S og observeret, at Netic A/S er forpligtet til at opdatere og patche servere og databaser.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret ISAE 3402 og 3000 type 2-erklæring fra Netic A/S for perioden fra 1. januar til 31. december 2021.	
B.13 – Fysisk sikkerhed ▶ Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren har outsourcet drift af servere og databaser hvori personoplysninger opbevares og behandles til hosting-leverandøren Netic A/S. Vi har inspiceret indgået aftale om it-driftsydelser mellem databehandleren og hosting-leverandøren og observeret, at der er indgået aftale om drift af servere og databaser. Vi har inspiceret ISAE 3402 og 3000 type 2-erklæring fra Netic A/S for perioden fra 1. januar til 31. december 2021.	Ingen afvigelser konstateret.
B.14 – Sikkerhedskopiering og retablering af data ▶ Drift og opbevaring af backup er outsourcet til underdatabehandler. ▶ Der udføres restore-tests to gange årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret indgået driftsaftale med hosting-leverandøren Netic A/S og observeret, at drift og opbevaring af backup er outsourcet til leverandøren. Vi har inspiceret ISAE 3402 og 3000 type 2-erklæring fra Netic A/S for perioden fra 1. januar til 31. december 2021. Vi har på forespørgsel fået oplyst, at databehandleren foretager restore-tests to gange årligt i forbindelse med møder i databehandlerens sikkerhedsudvalg.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret, at databehandleren har gennemført to restore test i erklæringsperioden.	
B.15 - Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret en periodisk afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedshåndbog og observeret, at databehandleren har etableret en beredskabsplan. Vi har inspiceret, at beredskabsplanen er blevet afprøvet i forbindelse med afholdt undervisning i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
C.1 - Informationssikkerhedspolitik ▶ Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedspolitik og procedure for uddannelse af medarbejdere. Vi har observeret, at databehandlerens informationssikkerhedspolitik indgår i uddannelsen af nye medarbejdere. Vi har inspiceret oversigt over medarbejdere, der har gennemført uddannelse og observeret, at alle databehandlerens medarbejdere har gennemført uddannelse. Vi har inspiceret referat fra møde i databehandlerens sikkerhedsudvalg og observeret, at informationssikkerhedspolitikken er gennemgået og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
C.2 - Styring informationssikkerhed ▶ Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret referat fra møde i databehandlerens sikkerhedsudvalg og observeret, at databehandleren gennemgår informationssikkerhedspolitikken for at sikre, at den ikke er i modstrid med indgåede databehandleraftaler.	Ingen afvigelser konstateret.
C.3 - Rekruttering af medarbejdere ▶ Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvning omfatter i relevant omfang: o Straffeattester	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret databehandlerens procedure for ansættelse af nye medarbejdere og observeret, at der indhentes straffeattest fra nye medarbejdere. Vi har observeret, at databehandleren har ansat to nye medarbejdere i erklæringsperioden. Vi har inspiceret, at proceduren for nye medarbejdere er fulgt i forbindelse med ansættelsen.	
C.4 - Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for ansættelse af nye medarbejdere og observeret, at nye medarbejdere skal underskrive en fortrolighedsaftale. Vi har inspiceret databehandlerens liste over medarbejdere, og vi har stikprøvevis observeret, at medarbejderne har underskrevet en fortrolighedsaftale. Vi har inspiceret databehandlerens procedure for uddannelse af medarbejdere og observeret, at nye medarbejdere introduceres til databehandlerens informationssikkerhedspolitik og procedurer vedrørende databehandleren samt anden relevant information. Vi har inspiceret listen over medarbejdere, der har gennemført uddannelse, og observeret, at alle medarbejdere har gennemført uddannelse.	Ingen afvigelser konstateret.
C.5 - Fratrædelse af medarbejdere	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret databehandlerens procedure for ophør af ansættelse og observeret, at databehandleren har implementeret en proces, som sikrer, at medarbejderens adgange til databehandlerens systemer lukkes ved ansættelsesforholdets ophør. Vi har inspiceret databehandlerens procedure for gennemgang af tildelte adgangsrettigheder og observeret, at adgangsrettigheder gennemgås halvårligt i forbindelse med møder i databehandlerens sikkerhedsudvalg. Vi har inspiceret referat for afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at sikkerhedsudvalget har gennemgået tildelte adgangsrettigheder. Vi har inspiceret, at der ikke er fratrådt medarbejdere i erklæringsperioden. Vi har derfor ikke kunnet efterprøve kontrollen.	
C.6 - Opretholdelse af tavshedspligt ved fratrædelse ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for ophør af ansættelse og observeret, at fratrådte medarbejdere skal gøres opmærksomme på, at den indgåede fortrolighedsaftale fortsat er gældende efter ophørt ansættelse. Vi har inspiceret databehandlerens fortrolighedsaftale og observeret, at det fremgår af aftalen, at aftalen fortsat er gældende efter ophørt ansættelse.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
C.7 - Awareness-træning for medarbejdere ▶ Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for løbende uddannelse af medarbejdere og observeret, at databehandleren afholder awareness-træning for alle medarbejdere én gang årligt. Vi har inspiceret dokumentation for afholdt awareness-træning i erklæringsperioden.	Ingen afvigelser konstateret.
C.8 - Fortegnelse over kategorier af behandlingsaktiviteter ▶ Der er etableret en fortegnelse over kategorier af behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review. ▶ Fortegnelsen opbevares elektronisk. ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens fortegnelse over kategorier af behandlingsaktiviteter som databehandler. Vi har inspiceret databehandlerens procedure for løbende opdatering af fortegnelsen og observeret, at fortegnelsen gennemgås og opdateres løbende i forbindelse med databehandlerens halvårlige møder i sikkerhedsudvalget. Vi har inspiceret referat fra afholdt møde i sikkerhedsudvalget og observeret, at fortegnelsen er blevet gennemgået. Vi har observeret, at databehandlerens fortegnelse over kategorier af behandlingsaktiviteter som databehandler opbevares elektronisk. Vi har på forespørgsel fået oplyst, at databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har på forespørgsel fået oplyst, at der ikke findes tidligere eksempler på anmodning fra Datatilsynet, hvorfor vi ikke har kunnet efterprøve kontrollen.	
C.9 - Bistand til den dataansvarlige vedrørende artikel 32-36 ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for bistand til den dataansvarlige og observeret, at databehandleren har udarbejdet procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36. Vi har på forespørgsel fået oplyst, at der er ingen dataansvarlige der har anmodet om bistand vedr. Artikel 32 til 36. Vi har derfor ikke kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
C.10 - Bistand til den dataansvarlige i forhold til revision og inspektion ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren. ▶ Databehandleren skal en gang årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af indgået databehandleraftale med dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevis inspiceret indgåede databehandleraftaler med databehandlerens kunder og observeret, at de indeholder forpligtelser om, at databehandleren skal stille den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren. Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation.	Ingen afvigelser konstateret.

Kontrolområde C

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
C.11 – Udpegelse af databeskyttelsesrådgiveren ▶ Databehandleren har vurderet behovet for en databeskyttelsesrådgiver og har sikret, at denne har kompetence til at udføre sin rolle. ▶ Databeskyttelsesrådgiveren inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger. ▶ Databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver. ▶ Databeskyttelsesrådgiveren overvåger databehandlerens overholdelse af databeskyttelseslovgivningen og politikker om beskyttelse af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren har vurderet, at der er et behov for ansættelse af en databeskyttelsesrådgiver. Vi har inspiceret dokumentation for, at databeskyttelsesrådgiveren inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger. Vi har inspiceret indgået aftale med databeskyttelsesrådgiveren og observeret, at databeskyttelsesrådgiveren er underlagt fortrolighed vedrørende udførelsen af sine opgaver. Vi har på forespørgsel fået oplyst, at databehandlerens databeskyttelsesrådgiver fører årligt tilsyn med databehandlerens overholdelse af databeskyttelseslovgivningen og politikker og beskyttelse af personoplysninger. Vi har inspiceret, at databehandlerens DPO har gennemført tilsyn med databehandlerens overholdelse af databeskyttelseslovgivningen og politikker om beskyttelse af personoplysninger.	Ingen afvigelser konstateret.

Kontrolområde D		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
D.1 - Sletning 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 forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler og observeret, at tilbagelevering og sletning af data skal ske efter aftale med den dataansvarlige. Vi har inspiceret databehandlerens procedure for sletning af data og observeret, at dette sker i henhold til databehandlerens standarddatabehandleraftalerne. Vi har inspiceret referat fra senest møde i databehandlerens sikkerhedsudvalg og observeret, at proceduren er gennemgået. Vi har inspiceret databehandlerens kundeoversigt og observeret, at der er sket ophør af samarbejde med én dataansvarlig. Vi har på forespørgsel fået oplyst, at det er aftalt med den dataansvarlige, at de skal have adgang til data i en periode efter ophør af aftale.	Ingen afvigelser konstateret.
D.2 - Opbevaring ▶ Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: ○ Data slettes kun ved forespørgsel	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler. Vi har inspiceret databehandlerens procedure for sletning af data og observeret, at sletningen af data kun sker efter instruktion fra den dataansvarlige. Vi har inspiceret databehandlerens kundeoversigt og observeret, at der er sket ophør af samarbejde med én dataansvarlig.	Ingen afvigelser konstateret.

Kontrolområde D		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har på forespørgsel fået oplyst, at det er aftalt med den dataansvarlige, at de skal have adgang til data i en periode efter ophør af aftale.	
D.3 – Ophør af aftalen med den dataansvarlige ▶ Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: ○ Tilbageleveret til den dataansvarlige og/eller ○ Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler. Vi har inspiceret databehandlerens procedure for tilbagelevering og sletning af data og observeret, at ved ophør af hovedaftale skal databehandleren kontakte den dataansvarlige angående tilbagelevering og sletning af data. Vi har inspiceret databehandlerens kundeoversigt og observeret, at der er sket ophør af samarbejde med én dataansvarlig. Vi har på forespørgsel fået oplyst, at det er aftalt med den dataansvarlige, at de skal have adgang til data i en periode efter ophør af aftale.	Ingen afvigelser konstateret.

Kontrolområde E		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
E.1 - Opbevaring af personoplysninger ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler. Vi har inspiceret databehandlerens procedure for opbevaring af data og observeret, at data kun må opbevares i overensstemmelse med formålene i indgåede databehandleraftale. Vi har inspiceret referat for afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at proceduren er blevet gennemgået.	Ingen afvigelser konstateret.
E.2 - Lokation for opbevaring af personoplysninger ▶ Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler og observeret, at den dataansvarlige adviseres minimum seks måneder før ændringer i lokation for opbevaring af personoplysninger. Vi har observeret, at den dataansvarlige skal godkende enhver ændring i brugen af underdatabehandlere. Vi har på forespørgsel fået oplyst, at der ikke er sket ændring af allerede, godkendte lokationer, lande eller landområder, hvor der foretages behandling eller opbevaring af personoplysninger.	Ingen afvigelser konstateret.

Kontrolområde F		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
F.1 - Underdatabehandleraftaler og instruks ▶ Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler og observeret, at databehandleren skal pålægge underdatabehandlere de samme databeskyttelsesforpligtelser som databehandleren selv. Databehandleren skal ligeledes indgå databehandleraftaler med tilhørende instruks. Vi har inspiceret indgået databehandleraftale med underdatabehandleren Netic A/S og observeret, der er indgået en databehandleraftale med tilhørende instruks. Vi har inspiceret dokumentation for afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at proceduren er blevet gennemgået på mødet.	Ingen afvigelser konstateret.
F.2 - Godkendelse af underdatabehandlere ▶ Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler og observeret, at den dataansvarlige specifikt godkender Netic A/S som underdatabehandler. Vi har observeret, at databehandleren alene anvender Netic A/S som underdatabehandler. Vi har inspiceret, at Netic A/S ikke anvender underunderdatabehandlere i relation til behandlingen af databehandlerens persondata.	Ingen afvigelser konstateret.

Kontrolområde F		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
F.3 - Ændringer i godkendte underdatabehandlere ▶ Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler og observeret, at de dataansvarlige godkender anvendelsen af underdatabehandleren Netic A/S. Vi har på forespørgsel fået oplyst, at der ikke er foretaget ændringer i brugen af generelt, godkendte underdatabehandlere. Vi har derfor ikke kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
F.4 - Underdatabehandlers databeskyttelsesforpligtelser ▶ Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standard databehandleraftaler og observeret, at databehandleren skal pålægge underdatabehandlere de samme databeskyttelsesforpligtelser, der er forudsat i databehandleraftalen. Vi har inspiceret indgået databehandleraftaler med underdatabehandleren Netic A/S og observeret, at underdatabehandleren pålægges de samme databeskyttelsesforpligtelser, der er forudsat i databehandleraftalen.	Ingen afvigelser konstateret.
F.5 - Oversigt over godkendte underdatabehandlere ▶ Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: ○ Navn ○ CVR-nr. ○ Adresse	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabeloner for databehandleraftaler og sikkerhedshåndbog. Vi har observeret, at begge indeholder en oversigt over godkendte underdatabehandlere med	Ingen afvigelser konstateret.

Kontrolområde F		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
○ Beskrivelse af behandling	angivelse af navn, CVR-nr., adresse og beskrivelse af behandling.	
F.6 – Tilsyn med underdatabehandlere ▶ Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedshåndbog og observeret, at der årligt skal indhentes ISAE 3402- og 3000-erklæringer fra underdatabehandlere, som gennemgås på møder i databehandlerens sikkerhedsudvalg. Vi har inspiceret seneste offentliggjorte ISAE 3402 type 2-erklæring fra underdatabehandleren Netic A/S for perioden fra 1. januar til 31. december 2021. Vi har inspiceret seneste offentliggjorte ISAE 3000 type 2-erklæring fra underdatabehandleren Netic A/S for perioden fra 1. januar til 31. december 2021. Vi har inspiceret referat fra afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at databehandleren har gennemgået og vurderet ISAE 3402 og 3000 type 2-erklæringen fra Netic A/S. Vi har inspiceret, at databehandleren har lavet løbende opfølgning på Netic A/S.	Ingen afvigelser konstateret.

Kontrolområde H

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
H.1 - Bistand til den dataansvarlige i forhold til de registreredes rettigheder - Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede. - Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens standarddatabehandleraftaler. Vi har inspiceret databehandlerens procedurer i forbindelse med registreredes rettigheder og observeret, at databehandleren har etableret procedurer, som muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede. Vi har på forespørgsel fået oplyst, at der ikke har været eksempler på henvendelser om bistand. Vi har derfor ikke kunnet efterprøve kontrollen. Vi har inspiceret referat fra afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at databehandlerens procedurer i forbindelse med registreredes rettigheder er blevet gennemgået og vurderet.	Ingen afvigelser konstateret.

Kontrolområde I		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
I.1 - Underretning om brud på persondatasikkerheden ▶ Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden og observeret, at den dataansvarlige skal underrettes hurtigst muligt og inden for 24 timer. Vi har inspiceret databehandlerens databrudslogs og observeret at der har været tre hændelser, men ingen konstateret databrud i erklæringsperioden. Vi har inspiceret at databehandleren kontaktede den berørte dataansvarlig i henhold til proceduren. Vi har inspiceret referat fra afholdt møde i databehandlerens sikkerhedsudvalg og observeret, at databehandlerens procedurer er blevet gennemgået og vurderet.	Ingen afvigelser konstateret.
I.2 - Identifikation af brud på persondatasikkerheden ▶ Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: ○ Awareness hos medarbejdere ○ Opfølgning på logning af tilgang til personoplysninger	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for løbende uddannelse af medarbejdere og observeret, at der skal afholdes awareness-træning for alle medarbejdere én gang årligt. Vi har inspiceret dokumentation for afholdt awareness-træning i erklæringsperioden. Vi har inspiceret afholdt møde i sikkerhedsudvalget, og observeret at der senest er foretaget opfølgning på logning af tilgang til personoplysninger.	Ingen afvigelser konstateret.

Kontrolområde I		
Kontrolmål ► *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
I.3 - Registrering af brud på persondatasikkerheden ► Alle brud på persondatasikkerheden registreres og dokumenteres i en databrudslog.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for brud på persondatasikkerheden og observeret, at databehandleren har registreret ét brud på persondatasikkerheden. Vi har inspiceret databehandlerens databrudslog og observeret, at databruddet er registreret i databrudsloggen i henhold til databehandlerens procedure.	Ingen afvigelser konstateret.
I.4 - Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden ► Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: ○ Karakteren af bruddet på persondatasikkerheden ○ Sandsynlige konsekvenser af bruddet på persondatasikkerheden ○ Foranstaltninger, som er truffet eller foreslås truffet for at håndterer bruddet på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for bistand til den dataansvarlige og observeret, at databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Vi har inspiceret databehandlerens databrudslogs og observeret at der har været tre hændelser, men ingen konstateret databrud i erklæringsperioden. Vi har inspiceret, at databehandleren kontaktede den berørte dataansvarlig i henhold til proceduren.	Ingen afvigelser konstateret.

5. SUPPLERENDE INFORMATION FRA DØGNDATA APS

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

På baggrund af BDO's konstaterede afvigelser i ISAE 3000-erklæringen har Døgndata ApS følgende supplerende information:

Under kontrolaktivitet B.6 skriver BDO " Vi har konstateret, at kravet om to-faktor autentifikation i ca. 3 måneder i erklæringsperioden har være deaktiveret for administrative brugere"

Til dette angiver Døgndata, at en af Døgndatas medarbejdere i forbindelse med support havde slået to-faktor autentifikationen fra for Døgndatas medarbejdere og efterfølgende glemte at få det slået til igen. Det blev først opdaget efter tre måneder. Vi har ingen indikation på, at der i perioden har været misbrug af Døgndatas medarbejderes brugernavn/adgangskode autentifikation. Efterfølgende har vi oprettet en funktion i programmerne, som en gang i døgnet tjekker, om to-faktor autentifikation er slået til, og som sender en besked til de relevante personer i Døgndata, hvis det er tilfældet.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

PENNEO

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

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

Mikkel Jon Larssen
Partner
Serienummer: CVR:20222670-RID:52744874
IP: 77.243.xxx.xxx
2022-09-23 12:38:31 UTC
NEM ID

Martin Lyngby Hansen
Administrerende direktør
Serienummer: CVR:33771797-RID:11030354
IP: 85.184.xxx.xxx
2022-09-24 05:45:37 UTC
NEM ID

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2022-09-26 08:03:10 UTC
NEM ID