AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. DECEMBER 2022 TIL 30. NOVEMBER 2023 OM BESKRIVELSEN AF VITEC MV-UDVIKLEDE SOFTWAREPRODUKTER 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

VITEC MV A/S

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

BDO

INDHOLD

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. DECEMBER 2022 TIL 30. NOVEMBER 2023 OM BESKRIVELSEN AF VITEC MV-UDVIKLEDE SOFTWAREPRODTUKTER 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 Vitec MV A/S
Vitec MV A/S' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Vitec MV A/S (databehandleren) for hele perioden fra 1. december 2022 til 30. november 2023 udarbejdede beskrivelse i sektion 3 af Vitec MV-udviklede softwareprodukter 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.

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen 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.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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 Vitec MV-udviklede softwareprodukter, 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 Vitec MV-udviklede softwareprodukter 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. december 2022 til 30. november 2023, 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. december 2022 til 30. november 2023, 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. december 2022 til 30. november 2023.

Beskrivelse af test af kontroller

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

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens Vitec MV-udviklede softwareprodukter, 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. juni 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

2. VITEC MV A/S' UDTALELSE

Vitec MV A/S varetager behandling af personoplysninger i forbindelse med Vitec MV-udviklede softwareprodukter 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 Vitec MV-udviklede softwareprodukter, 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.

Vitec MV A/S anvender underdatabehandler(e). Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Vitec MV A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af Vitec MV-udviklede softwareprodukter og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden fra 1. december 2022 til 30. november 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for Vitec MV-udviklede softwareprodukter, 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 Vitec MV-udviklede softwareprodukter 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.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

2. Indeholder relevante oplysninger om ændringer i Vitec MV-udviklede softwareprodukter og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden fra 1. december 2022 til 30. november 2023.

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

Vitec MV A/S bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. december 2022 til 30. november 2023. 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. december 2022 til 30. november 2023.

Vitec MV A/S 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.

Viby, den 24. juni 2024

Vitec MV A/S

Hans-Erik Schou
CEO

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

3. VITEC MV A/S' BESKRIVELSE AF VITEC MV-UDVIKLEDE SOFTWAREPRODUKTER

Nærværende beskrivelse skal læses i sammenhæng med sektion 4, hvoraf kontrolmål og kontrolaktiviteter fremgår.

VITEC MV A/S

Vitec MV A/S (herefter: Vitec MV) er ejet af svenske Vitec Software Group AB, der er noteret på den svenske børs og har hovedsæde i Umeå, Sverige. Vitec Software Group er en nordisk aktør med kontorer i Sverige, Danmark, Norge, Finland og Nederlandene.

Vitec MV's ca. 28 medarbejdere er specialiserede inden for systemudvikling, serverdrift, support og informationssikkerhed, og organiseret i en udviklingsafdeling, salgs- og supportafdeling og marketingafdeling.

Salgs- og udvikling styrer Vitec MV's persondatasikkerhed i forhold til den behandling, som Vitec MV varetager på vegne af sine kunder, herunder indgåelse af databehandleraftaler, besvarelse af henvendelser fra den dataansvarlige, underretning om brud på persondatasikkerheden, efterlevelse af interne politikker og procedurer og lignende.

VITEC MV-UDVIKLEDE SOFTWAREPRODUKTER OG BEHANDLING AF PERSONOPLYSNINGER

Vitec MV leverer softwareprodukter i form af digitale læremidler og læse- og skrivestøttende it-værktøjer til offentlige og private kunder i Danmark, Sverige, Norge og Holland.

Vitec MV leverer IntoWords som en Software-as-a-Service (SaaS) løsning i henhold til indgåede kontrakter med kommuner og private virksomheder. IntoWords fås både som mobil applikation, desktop applikation og som online løsninger.

Produkterne udvikles i Vitec MV's hovedsæde i Odense, Danmark, men afhængig af løsning afvikles fra hosting-centre i Europa. Der benyttes andre underdatabehandlere til IntoWords, og Vitec MV har indgået databehandleraftaler med disse underdatabehandlere.

Test og support varetages primært i Danmark og sekundært i det land, som produkterne er lokaliseret til.

Brugernes persondatasikkerhed har stor betydning for os, og vores behandling af personoplysninger lever op til bestemmelserne i EU's persondataforordning, GDPR.

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er: Formålet med at behandle personoplysninger i forbindelse med brugen af databehandlerens produkter er at yde den aftalte service samt at optimere produkternes performance, herunder skabe den bedste lærings-, læse- og skrivestøtte for bruger af produkterne/services, der herved opnår støtte til at "læse og forstå en tekst", "skrive en tekst" samt "tale en tekst".

Karakter af behandling

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om, at der for hver bruger oprettes en konto-/brugeradgang. Denne log in/registrering af bruger medvirker til, at produktet udarbejder en statistik for den pågældende bruger. Dette sker ved, at produkterne/services ved brug registrerer brugerens handlinger, herunder hvor mange ordforslag, brugeren foreslås, at der sker tekstoplæsning, samt at billeder konverteres til tekst. Hvilke ord og billeder, der er tale om, registreres dog ikke. Det er således funktionen, der registreres, men ikke indholdet af funktionerne, der registreres.

Personoplysninger

Databehandlerens produkter indsamler og registrerer data om brugeren ved oprettelse af log in-/brugerkonto samt ved brugen af produktet/services for at levere den aftalte ydelse.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

Ved Privatkunde registreres navn og e-mail på bruger for at oprette brugeradgang. Data opbevares så længe brugeradgang er aktiv. Herefter slettes data.

Ved Erhvervskunde registreres navn og e-mail på bruger i virksomheden. Data på slutbrugere kendes ikke. Data opbevares, så længe brugeradgang er aktiv. Herefter slettes data.

Ved Kommune-kunde er data pseudonymiseret. Brugerens login-hash fra idP gemmes permanent, dog kun så længe brugeren er tilknyttet databehandlerens login, eller den underliggende kontrakt er aktiv. Statistisk data er pseudonymiseret og alene tilknyttet login-hash fra idP. Disse data slettes automatisk ved aftaleophør.

Styring af overholdelse af krav m.v.

Vitec MV arbejder løbende med opgaver relateret til GDPR, og mindst en gang om året følger vi op på, at vi overholder procedurer i relation til EU-persondataforordningen.

Vitec MV's arbejder med overholdelse af GDPR omfatter nedenstående - bemærk, at listen ikke er udtømmende:

- It-sikkerhedspolitik
- Gennemgang af eventuelle sikkerhedsbrud
- Procedurer for adgang til personoplysninger
- Procedurer for risikovurdering
- Procedurer for sikkerhed i forbindelse med support
- Opfølgning på uddannelse og awareness
- Opfølgning på modtagelse og udsendelse af (nye) databehandleraftaler og godkendelse heraf
- Opfølgning på kunder (databehandleraftaler) med særlige krav i databehandleraftalerne
- Opfølgning på godkendelse af anvendelse af eventuelle underleverandører
- Opfølgning på, at dataansvarlig har godkendt eventuelle procedurer og tekniske foranstaltninger, som sikrer behandling og beskyttelse af personoplysninger
- Opfølgning på, at håndtering af henvendelser fra dataansvarlige i relation til håndtering af registreredes rettigheder (indsigt, sletning, berigtigelse) er foretaget korrekt og rettidigt
- I relation til eventuelle opståede incidents: Opfølgning på resultatet af den dataansvarliges høring hos tilsynsmyndigheden, i det omfang dette er relevant for Vitec MV's databehandling for denne dataansvarlige
- Opfølgning på, at personer, der er autoriseret til at behandle personoplysninger, er forpligtet til fortrolighed eller underlagt lovbestemt tavshedspligt.

Procedurer og kontroller

Vitec MV har etableret en række politikker og procedurer, som medarbejdere har modtaget og er trænet i efterlevelse af.

I de følgende afsnit er der lavet en risikovurdering af setuppet set i forhold til efterlevelse af den registreredes rettigheder, herunder vurdering af hvorvidt der er etableret de passende tekniske og organisatoriske kontroller på områderne.

Vitec MV har med afsæt i risikovurderingen etableret procedurer for håndtering af den registreredes rettigheder (indsigt, berigtigelse, begrænsning af behandling, sletning), for håndtering af sikkerhedsbrud, samt for at sikre at relevant viden er til stede hos medarbejdere, så de er bedst muligt rustet til at håndtere persondata, herunder afvise persondata og sende dem tilbage til kunden.

Vitec MV har sammen med advokater udarbejdet egen databehandleraftale. Aftalen tilbydes til kunder og samarbejdspartnere. Vi modtager også databehandleraftaler fra kunder og samarbejdspartnere. Alle databe-

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

handleraftaler modtages og gennemgås. Alle databehandleraftaler journaliseres med beskrivelse af særlige forhold fra den dataansvarlige som fx svarfrister og/eller krav til særlige kontroller. Eventuelle særlige krav kommunikeres til de relevante teams internt til indarbejdelse i deres servicering af kunderne.

Overordnet beskrivelse af udviklingsprocesserne

Udviklingsprocesserne for softwareudvikling er i store træk ens, uanset hvilket produkt der er tale om. Fælles for udviklingsprocesserne er, at der testes med anonymiserede "fiktive" data. Persondatasikkerhed er i fokus i udviklingen, herunder også at der tages højde for de registreredes rettigheder: Retten til berigtigelse, retten til begrænsning i behandling, retten til indsigt, retten til at blive glemt (slettet). Her sikres det, at de it-systemer, som Vitec MV udvikler, understøtter disse krav.

Support

Der ydes support på alle produkter, der er udviklet af Vitec MV. Personoplysninger i forbindelse med support behandles med fortrolighed og respekt for den enkelte bruger.

Henvendelser fra de dataansvarlige

Vitec MV har en procedure for håndtering og dokumentation af henvendelser fra dataansvarlige i relation til bistand til håndtering af de registreredes rettigheder (indsigtsret, sletning, berigtigelse m.v.).
Dokumentation af henvendelser fra dataansvarlige vedr. fx indsigtsret, sletning og berigtigelse håndteres i vores supportsystem.

ÆNDRINGER I PERIODEN

Vitec MV har ikke foretaget væsentlige ændringer i Vitec MV-udviklede softwareprodukter og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i perioden 1. december 2022 til 30. november 2023.

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:

- Afgivelse af instruks til Vitec MV.
- Rettidig henvendelse ved ønske om bistand i relation til forespørgsler fra de registrerede i relation til deres rettigheder.
- Den dataansvarlige har ansvaret for at sikre, at administratorernes brug af MV-ID Admin og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen.
- Den dataansvarlige styrer brugerrettighederne i Vitec MV-udviklede softwareprodukter, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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 Vitec MV A/S' beskrivelse af Vitec MV-udviklede softwareprodukter 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 Vitec MV A/S, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden fra 1. december 2022 til 30. november 2023.

Udførte testhandlinger

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

Type	Beskrivelse
Forespørgsel	Forespørgsler hos Vitec MV A/S' 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, som Amazon Web Services leverer inden for serverhosting, oversættelse i online produkter/løsninger, har vi modtaget System and organization Controls 2 (SOC 2) for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Microsoft leverer inden for tale-til-tekst behandling i online produkter/løsninger, har vi modtaget System and organization Controls 2 (SOC 2) for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

For de ydelser, som Abbyy leverer inden for OCR-behandling i online produkter/løsninger, har vi modtaget System and organization Controls 2 (SOC 2) for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i Vitec MV A/S' beskrivelse af Vitec MV-udviklede softwareprodukter og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos Vitec MV A/S', 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.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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
Indgåelse af databehandleraftale med den dataansvarlige ▶ Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ▶ Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. ▶ Ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, anvender databehandleren en tjekliste, som fastlægger hvad databehandleren kan leve op til. ▶ Databehandleraftaler underskrives og opbevares elektronisk. ▶ Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for indgåelse af skriftlige databehandleraftaler og observeret, at databehandleren behandler personoplysninger på vegne af den dataansvarlige i overensstemmelse med bestemmelserne i databehandleraftalen. Vi har foretaget inspektion af databehandlerens skabelon til indgåelse af databehandleraftaler og observeret, at databehandleren anvender datatilsynets skabelon til databehandleraftaler. Vi har foretaget inspektion af databehandlerens skabelon til indgåelse af databehandleraftaler og observeret, at databehandler benytter sig af datatilsynets skabelon til databehandleraftaler, som en tjekliste der fastlægger, hvad databehandleren kan leve op til. Vi har ved stikprøve foretaget inspektion af indgåede databehandleraftaler og observeret, at disse er underskrevet og opbevares elektronisk. VI har ved stikprøve foretaget inspektion af indgåede databehandleraftaler og observeret, at disse indeholder informationer om brugen af underdatabehandlere.	Ingen afvigelser konstateret.
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens skabelon til en databehandleraftale og observeret, at denne indeholder instruks vedrørende behandling af personoplysninger.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
	Vi har ved stikprøve foretaget inspektion af indgåede databehandleraftaler og observeret, at databehandleren indhenter instruks for behandling af personoplysninger.	
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig. ▶ Databehandlerens procedurer gennemgås og opdateres løbende og minimum en gang årligt. ▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved stikprøve foretaget inspektion af indgåede databehandleraftaler og observeret, at databehandleren udfører behandling af personoplysninger efter den dataansvarliges instruks. Vi har foretaget inspektion af databehandlerens procedure for databehandleraftaler og observeret, at databehandleren behandler personoplysninger efter instruks fra den dataansvarlige. Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandlerens procedure for databehandleraftaler gennemgås og opdateres årligt. Vi har ved forespørgsel fået oplyst, at databehandleren udfører udviklingsopgaver med henblik på, at disse overholder instruksen fra dataansvarlige.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen. ▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for indgåelse af databehandleraftaler og observeret, at databehandleren omgående skal underrette den dataansvarlige, hvis instruksen strider mod databeskyttelseslovgivningen. Vi har ved forespørgsel fået oplyst, at der ikke har været eksem-	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
	pler på ulovlige instrukser i perioden, hvorfor det ikke har været muligt at efterprøve kontrollen yderligere.	

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering, baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens udarbejdede risikovurderinger og observeret, at databehandleren har udarbejdet risikovurderinger på alle ydelser. Vi har foretaget inspektion af databehandlerens udarbejdede risikovurderinger og observeret, at disse risikovurderinger indeholder risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandlerens risikovurderinger gennemgås årligt. Vi har ved forespørgsel fået oplyst, at databehandleren har foretaget revurdering af tidligere års udarbejdede risikovurderinger og vurderet, at risiciene stadig er relevante for databehandleren.	Ingen afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, beredskabsplanerne er tidssvarende og effektive i kritiske situationer. ▶ Beredskabstest dokumenteres og evalueres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens beredskabsplan og observeret, at denne skal sikre hurtig responstid fra databehandleren i tilfælde af hændelser. Vi har foretaget inspektion af databehandlerens dokumentation for afprøvning af den etablerede beredskabsplan og observeret, at denne er dokumenteret. Vi har ved forespørgsel fået oplyst, at databehandleren har evalueret afprøvningen af beredskabsplanen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang. ▶ Alle adgange registreres og logges.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for alarm og adgangskontrol og observeret, at databehandlerens indgange er aflåste, hvor man skal anvende adgangsbrik og kode. Vi har foretaget inspektion af databehandlerens procedure for eksterne besøg og observeret, at eksterne besøgende skal lukkes ind af en medarbejder og bære synligt gæstekort. Vi har foretaget inspektion af databehandlerens adgangslog og observeret, at alle adgange registreres og logges.	Ingen afvigelser konstateret.
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration, der sikrer at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. ▶ Der foretages halvårlig gennemgang af brugere og brugerrettigheder. ▶ Der foretages logning af alle brugeradgange og brugeraktiviteter. ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation. ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst databehandlerens proces for brugeradministration. Vi har ved forespørgsel fået oplyst, at ingen medarbejder i erklæringsperioden har fået tildelt adgang til personoplysninger, hvorfor vi ikke har kunnet teste processen for brugeroprettelser. Vi har ved stikprøve foretaget inspektion af brugernedlæggelser og observeret, at brugernes adgange er slettede. Vi har foretaget inspektion af databehandlerens miljøer og observeret, at rettighederne i miljøerne tildeles efter arbejdsbetingede behov. Vi har foretaget inspektion af udtræk over brugere med administratorrettigheder og observeret, at disse er tildelt efter arbejds-	Vi har konstateret, at én af de udvalgte stikprøver ikke var nedlagt rettidigt i databehandlerens system. Vi har konstateret, at databehandleren ikke har kunnet dokumentere sin halvårlige gennemgang af brugere og brugerrettigheder. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
eksterne konsulenter.	betingede behov. Vi har ved forespørgsel fået oplyst, at databehandleren har udført gennemgang af brugere og brugerrettigheder i erklæringsperioden. Vi har foretaget inspektion af logning af alle brugeradgange og brugeraktivitet for relevante systemer. Vi har foretaget inspektion af databehandlerens vejledning til adgangskoder og observeret, at denne indeholder retningslinjer for et stærkt password, hvor databehandleren påkræver, at medarbejderne anvender to-faktor autentifikation til systemerne. Vi har ved genudførelse af databehandlerens login på systemer med personoplysninger observeret, at der er etableret to-faktor autentifikation.	
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. ▶ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse. ▶ Fjernadgang skal foregå via to-faktor autentifikation.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved stikprøve foretaget inspektion af medarbejderes arbejdsstationer og observeret, at disse har installeret og opdateret antivirus-software. Vi har foretaget inspektion af databehandlerens fjernadgang og observeret, at fjernadgang tilgås via en krypteret VPN-forbindelse, og at VPN-forbindelsen tilgås via to-faktor autentifikation.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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
Eksterne kommunikationsforbindelser ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og VPN. ▶ Eksterne kommunikationsforbindelser er krypteret. ▶ Databehandleren har en oversigt over, hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens miljøer og observeret, at disse miljøer kun kan tilgås via VPN-forbindelse, og er understøttet af firewall. Vi har foretaget inspektion af databehandlerens eksterne kommunikationsforbindelser og observeret, at disse er krypteret. Vi har foretaget inspektion af databehandlerens firewall konfigurationer og observeret, at der fremkommer en oversigt over, hvilke eksterne kommunikationsforbindelser der kan tilgå databehandlerens netværk.	Ingen afvigelser konstateret.
Kryptering af personoplysninger ▶ Databehandleren har implementeret en krypteringspolitik for kryptering af personoplysninger. Politikken definerer styrken og protokollen for kryptering. ▶ Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens krypteringspolitik og observeret, at databehandleren anvender kryptering ”in transit” og ”at rest”. Vi har foretaget inspektion af dokumentation for, at databehandleren anvender kryptering ved transmission af personoplysninger via internettet.	Vi har konstateret, at databehandleren for deres API løsning anvender TLS 1.2, som ikke er i overensstemmelse med databehandlerens krypteringspolitik, som fremgår af instruksen til databehandleraftalerne, idet der heri står anført, at TLS 1.3 anvendes ”in transit”. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Firewall ▶ Databehandler har konfigureret firewall korrekt efter best-practice standard. ▶ Databehandler anvender kun services/porte, som de har behov for.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens firewall konfigurationer og observeret, at disse er opsat, så der kun gives adgang til de specifikke services/porte der er behov for.	Ingen afvigelser konstateret.
Netværkssikkerhed ▶ Databehandlerens netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet. ▶ Databehandleren anvender kendte netværksteknologier og mekanismer for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens netværk og observeret, at databehandleren har segmenteret netværk i gæstenetværk og administrativt netværk, hvor disse direkte ikke kan kommunikere med hinanden. Vi har foretaget inspektion af, at databehandlerens netværk er beskyttet af firewall, samt at medarbejdere skal være logget på wi-fi, eller have adgang via VPN-forbindelse, som er krypteret.	Ingen afvigelser konstateret.
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateres med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved stikprøve foretaget inspektion af medarbejderes arbejdsstationer og observeret, at disse har installeret og opdateret antivirus-software. Vi har ved stikprøve foretaget inspektion af medarbejderes arbejdsstationer og observeret, at databehandleren løbende opdateret antivirus-software, og at den seneste version er installeret.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Sårbarhedsscanning og penetrationstests ▶ Der udføres løbende sårbarhedsscanninger af databehandlerens netværk. Resultatet dokumenteres i en rapport. ▶ Databehandleren gennemgår rapporten og følger op på konstaterede svagheder. ▶ Databehandler håndterer/mitigerer eventuelle sårbarheder ud fra en risikovurdering. ▶	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens modtagne sårbarhedsscanninger og observeret, at databehandleren modtager disse i form af en rapport. Vi har på forespørgsel fået oplyst, at databehandleren ugentligt gennemgår de modtagne sårbarhedsscanninger på udviklingsmøder og inspiceret, at databehandleren håndterer disse sårbarheder ud fra en risikovurdering.	Ingen afvigelser konstateret.
Vedligeholdelse af systemsoftware ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende. ▶ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandleren har outsourcet deres drift af deres operativsystem, og inspiceret dokumentation for, at databehandleren modtager nyhedsbreve om opdateringer på deres operativsystem. Vi har foretaget inspektion af databehandlerens proces for opdatering af systemsoftware og observeret, at databehandleren ugentligt gennemgår systemsoftware for opdateringer. Vi har ved stikprøve foretaget inspektion af systemsoftwareopdateringer og observeret, at databehandleren udfører disse opdateringer i overensstemmelse med at sikre systemers tilgængelighed og sikkerhed.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle brugerændringer i systemer og databaser logges. ▶ Loggen slettes efter den fastsatte retentionsperiode ▶ Databehandler monitorerer og logger netværkstrafik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af logning af alle brugeradgange og brugeraktivitet for relevante systemer og databaser. Vi har foretaget inspektion af databehandlerens oversigt af log på brugerændringer og observeret, at databehandleren fører oversigt over de registrerede brugerændringer. Vi har ved stikprøve foretaget inspektion af log på nedlagte brugere og observeret, at brugerændringerne registreres i loggen. Vi har foretaget inspektion af databehandlerens indstillinger for logning og observeret, at logge slettes efter en retentionsperiode på 3 måneder. Vi har foretaget inspektion af databehandlerens log på netværkstrafikken og observeret, at databehandlerens monitorerer og logger netværkstrafikken.	Ingen afvigelser konstateret.
Overvågning ▶ Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. ▶ Databehandleren notificeres om identificerede alarmer, og følger op herpå.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens overvågningssystemer og observeret, at databehandleren overvåger produktionsmiljøets oppetid, ydeevne og kapacitet. Vi har foretaget inspektion af databehandlerens opsatte alarmer for overvågningen af produktionsmiljøet og observeret, at databehandleren modtagne alarmer ved fald i oppetid, ydeevne og kapacitet.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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 ved stikprøve foretaget inspektion af databehandlerens modtaget alarmer i forbindelse med overvågningen af produktionsmiljøet og observeret, at databehandleren følger op på disse alarmer.	
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurderer og evaluerer effektiviteten af, at de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren løbende følger op på de nye arbejdsprocesser, hvori der behandles personoplysninger og foretages en risikovurdering. Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren årligt vurderer om sikkerhedsniveauet er tilstrækkeligt.	Ingen afvigelser konstateret.
Udvikling og vedligeholdelse af systemer ▶ Databehandleren arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelsesopgaver. ▶ Risikovurdering af systemændringer er udført for, at sikre databeskyttelse gennem design og standardindstillinger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens persondatapolitik og observeret, at denne indeholder retningslinjer for behandling af personoplysninger. Vi har foretaget inspektion af udviklingsopgaver i perioden og observeret, at disse er udført i henhold til privacy-by-design principper, hvor databehandleren har foretaget en risikovurdering på udviklingsopgaver.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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
Informationssikkerhed i udvikling og ændringer ▶ Rollback-plan er implementeret i tilfælde af fejl i produktionsmiljøet. ▶ Databehandleren minimerer angrebsflader ved at forholde sig til funktionaliteter og åbne services anvendelighed i udviklings- og ændringsopgaver. ▶ Brugeroprettelse sker som udgangspunkt med laveste brugerrettighedsniveau. ▶ Kun databehandlerens udviklere har adgang til kildekode.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens rollback-plan og observeret, at databehandleren registrerer ændringer i produktionsmiljøet, som muliggør rollback i tilfælde af fejl. Vi har foretaget inspektion af databehandlerens udviklingsproces og observeret, at udviklings- og ændringsopgaver skal verificeres, før de køres ud i produktionsmiljøet. Vi har ved stikprøve foretaget inspektion af udviklings- og ændringsopgaver og observeret, at disse er verificeret, før de er kørt ud i produktionsmiljøet. Vi har foretaget inspektion af udtræk over brugere med administratorrettigheder og observeret, at disse er tildelt efter arbejdsbetingede behov. Vi har foretaget inspektion af dokumentation for, at det kun er udviklere, der har adgang til databehandlerens kildekode.	Ingen afvigelser konstateret.
Adskillelse af udviklings-, test og produktionsmiljø ▶ Der er indført funktionsadskillelse mellem udvikling og drift. ▶ Ændringer af funktionalitet testes, inden det sættes i drift. ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. ▶ Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens udviklingsproces og observeret, at udviklings- og ændringsopgaver skal verificeres, før de køres ud i produktionsmiljøet. Vi har ved stikprøve foretaget inspektion af pull requests i erklæringsperioden og observeret, at disse er godkendt af en eller flere personer.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
▶ Udviklings- og testmiljøer er adskilte.	Vi har foretaget inspektion af databehandlerens miljøer og observeret, at disse er adskilt fra hinanden, hvor hvert miljø har sin egen VPN. Vi har foretaget inspektion af databehandlerens rollback-plan og observeret, at databehandleren registrerer ændringer i produktionsmiljøet, som muliggør rollback i tilfælde af fejl.	
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes fiktive testdata i udviklingsmiljøet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af data i databehandlerens udviklingsmiljø og observeret, at der anvendes fiktive data i udviklingsmiljøet.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Informationssikkerhedspolitik ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens informationssikkerhedspolitik og observeret, at denne er tilgængelig for alle medarbejdere.	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandlerens informationssikkerhedspolitik gennemgås og opdateres årligt. Vi har på forespørgsel fået oplyst, at databehandleren har gennemgået informationssikkerhedspolitikken og vurderet, at den udarbejdede informationssikkerhedspolitik ikke nødvendiggøre en opdatering i erklæringsperioden.	Ingen afvigelser konstateret.
Organisering af informationssikkerhedspolitik ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at databehandlerens CTO årligt udarbejder en GDPR-workshop og observeret, at databehandlerens CTO har arrangeret og afholdt GDPR-workshoppen. Vi har foretaget inspektion af databehandlerens udarbejdede materiale for GDPR-workshoppen og observeret, at denne indeholder emner som informationssikkerhed.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse. ▶ Databehandleren udfører baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren foretager screening af potentielle medarbejdere, hvor databehandleren indhenter CV. Vi har på forespørgsel fået oplyst, at databehandleren afholder to interview i forbindelse med baggrundstjek af potentielle medarbejdere, hvor databehandleren tester kandidaten i deres udviklingsfærdigheder under interview. Vi har foretaget inspektion af databehandlerens skabelon for jobsamtaler og observeret, at denne bruges som en tjekliste. Vi har ved stikprøve foretaget inspektion af ansatte medarbejdere i erklæringsperioden og observeret, at disse medarbejdere under interviewet har udført en udviklingstest, og at databehandleren har indhentet CV.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sletteliste, som angiver de systemer, som den nærmeste leder skal gennemgå i forbindelse med fratrådte medarbejdere. Vi har ved stikprøve inspiceret dokumentation for, at stoppede medarbejdere ikke længere har adgang til systemerne. Vi har ved stikprøve foretaget inspektion af databehandlerens ansættelseskontrakt og observeret, at medarbejdere har underskrevet, at tavshedspligten stadig er gældende i forbindelse med	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
	ansættelsens ophør.	
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren udfører oplysningskampagner for medarbejdere om databeskyttelse og informationssikkerhed. ▶ Databehandleren foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens resultater for udførte phishing-kampagner og observeret, at ingen medarbejdere er faldet for phishing-mailen. Vi har foretaget inspektion af databehandlerens årlige GDPR-workshop og observeret, at databehandleren løbende afholder træning i henhold til databeskyttelse og informationssikkerhed.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet en ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Alle medarbejdere har underskrevet en tavsheds- og fortrolighedsaftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved stikprøve foretaget inspektion af ansatte medarbejdere i erklæringsperioden og observeret, at disse medarbejdere i forbindelse med deres ansættelseskontrakt har underskrevet en tavshedspligt samt at der er underskrevet en udvidet fortrolighedserklæring, når medarbejderen i henhold til et arbejdsbetinget behov, gives adgang til persondata.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til behandlingssikkerhed og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32 og 35.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens databehandleraf-	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
	taleskabelon og observeret, at den indeholder et afsnit vedrørende databehandlernes bistand til den dataansvarlige i forbindelse med overholdelse af dennes forpligtelser i medfør af Databeskyttelsesforordningens artikel 32-36. Vi har foretaget inspektion af databehandlerens udarbejdede konsekvensanalyse og observeret, at denne skal sikre, at databehandleren overholder den til enhver tid gældende persondataretlige regulering.	
Bistand til den dataansvarlige i forhold til revision og inspektion ▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandler bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens databehandleraftaleskabelon og observeret, at databehandleren en gang årligt skal stille en rapport til rådighed til den dataansvarlige med oplysninger, der påviser, om databehandleren overholder databehandleraftalen. Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation. Vi har foretaget inspektion af databehandlerens databehandleraftaleskabelon og observeret, at denne indeholder et afsnit vedrørende databehandlerens bistand til den dataansvarlige i forbindelse med overholdelse af dennes forpligtelser i medfør af Databeskyttelsesforordningens artikel 32-36. Vi har ved forespørgsel fået oplyst, at der ikke har været forespørgsel fra dataansvarlig vedrørende bistand, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standardskabelon for en databehandleraftale og observeret, at databehandleren er forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige ved aftalens ophør. Vi har inspiceret, at slettepolitik er udarbejdet. Vi har ved forespørgsel fået oplyst, at der ikke har været forespørgsel fra dataansvarlig vedrørende sletning af personoplysninger, hvorfor vi ikke har kunnet efterprøve proceduren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Opbevaring af personoplysninger ▶ Personoplysninger opbevares utilgængeligt for andre. ▶ Adgang til personoplysninger tildeles på baggrund af et arbejdsbetinget behov/need-to-know principper. ▶ Fortroligheden af digitale personoplysninger opbevares i krypteret form. ▶ Personoplysninger opbevares kun så længe, der er hjemmel/en legitim grund.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har på forespørgsel fået oplyst, at personoplysninger kun opbevares på databehandlerens produktionsmiljø. Vi har foretaget inspektion over de brugere, der har adgang til databehandlerens produktionsmiljø og observeret, at disse brugere har et arbejdsbetinget behov. Vi har foretaget inspektion af databehandlerens oversigt over kryptering for anvendte services og observeret, at personoplysninger opbevares i krypteret form og kun kan tilgås ved brug af VPN-forbindelse. Vi har foretaget inspektion af databehandlerens slettepolitik og observeret, at databehandleren kun opbevarer personoplysninger, så længe, der er en legitim grund.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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
Underdatabehandleraftaler og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk. ▶ Databehandleraftalen med underdatabehandlers indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved stikprøve foretaget inspektion af en databehandleraftale og en underdatabehandleraftale og observeret, at underdatabehandler pålægges de samme databeskyttelsesforpligtelser, som databehandleren er pålagt, og at instruks er videregivet til underdatabehandler. Vi har foretaget inspektion af indgåede databehandleraftaler med underdatabehandlere og observeret, at disse er underskrevet, opbevares elektroniske og indeholder information om brugen af underdatabehandlere.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved stikprøve foretaget inspektion af indgåede databehandleraftaler og observeret, at godkendte underdatabehandlere fremgår heraf.	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere ▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere. ▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler. ▶ Dataansvarlig har mulighed for at gøre indsigelse vedrørende udskiftning af underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standardskabelon for en databehandleraftale og observeret, at databehandleren er forpligtet til at underrette den dataansvarlige vedrørende ændringer af underdatabehandlere, hvor den dataansvarlige har mulighed for at gøre indsigelse.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
▶ Ved udskiftning af underdatabehandler skal databehandleren have en ny forudgående specifik skriftlig godkendelse fra dataansvarlig.	Vi har ved forespørgsel fået oplyst, at processen ved ændringer er, at databehandleren sender en informationsmail ud angående udskiftning af godkendte underdatabehandlere med mulighed for indsigelser. Vi har ved stikprøve foretaget inspektion af databehandlerens kommunikation med dataansvarlige angående ændringer i godkendte underdatabehandlere og observeret, at databehandleren har informeret dataansvarlige angående ændring af underdatabehandlere i databehandleraftalen.	
Oversigt over godkendte underdatabehandlere ▶ Databehandleren har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet oplysninger om behandlingssted og type behandling, som underdatabehandleren påtager sig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standardskabelon for en databehandleraftale og observeret, at der fremkommer en oversigt over de godkendte underdatabehandlere, hvor der oplyses behandlingssted og type af behandling.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering. ▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året, baseret på en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren årligt foretager tilsyn med underdatabehandlere. Vi har observeret, at databehandleren har foretaget tilsyn i form af indhentede revisorerklæringer fra underdatabehandlere. Vi har inspiceret SOC 2 erklæring fra Amazon Web Services for perioden 1. oktober 2022 til 30. september 2023, SOC 2 erklæring fra Microsoft for perioden 1. april 2022 til 31. marts 2023 og	Vi har konstateret, at risikovurderingen af underdatabehandlere ikke er fuldt opdateret, da der blandt andet mangler oprydning i forhold til underdatabehandlere, som ikke længere anvendes. Vi har konstateret, at der ikke er foretaget tilsyn af underdatabehandleren Vitec Software Group i erklæringsperioden, men at en ISO/IEC 27001:2022 certificering er udstedt marts 2024 valid til februar 2027. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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
	SOC 2 erklæring fra Abbyy for perioden 1. marts 2022 til 28. februar 2023. Vi har foretaget inspektion af databehandlerens risikovurdering af underdatabehandlerne og observeret, at tilsyn er foretaget med baggrund heri.	

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

Kontrolområde G

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Overførsel af personoplysninger til tredjelande ▶ Der foreligger skriftlige procedurer for overførsel af personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. ▶ Databehandlerens procedure gennemgås og vurderes løbende, og som minimum en gang årligt, om proceduren skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standarddatabehandleraftale og observeret, at overførselsgrundlaget skal være baseret på databeskyttelsesforordningens kapitel V og Europa-Kommissionens gennemførelsesafgørelse 2021/914 af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679. Vi har foretaget inspektion af databehandlerens årshjul og dokumentation på, at databehandleren har gennemgået deres databehandleraftaler for at sikre, at de er opdaterede.	Ingen afvigelser konstateret.
Instruks fra den dataansvarlige ▶ Databehandleren overfører kun personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige. ▶ Databehandleren dokumenterer indhentet instruks vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer fra dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standarddatabehandleraftale og observeret, at det heraf fremgår, at enhver overførsel af personoplysninger til tredjelande eller internationale organisationer kun må foretages af databehandleren på baggrund af dokumenteret instruks fra den dataansvarlige. Vi har ved stikprøve foretaget inspektion af indgåede databehandleraftaler og observeret, at databehandleren indhenter instruks fra den dataansvarlige angående overførsel af personoplysninger til tredjelande.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

Kontrolområde G

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Gyldigt overførselsgrundlag ▶ Databehandleren vurderer og dokumenterer, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens oversigt over underdatabehandlere og observeret, at databehandleren anvender tre underdatabehandlere, der er reguleret af amerikansk lovgivning, og at der derved kan ske en utilsigtet overførsel til tredjelande. Det drejer sig om underdatabehandlerne Amazon Web Services, Microsoft og Abbyy. Vi har foretaget inspektion af databehandlerens udarbejdede TIA-analyser (Transfer Impact Assessment) for de tre amerikanske underdatabehandlere i forbindelse med EDPB's (European Data Protection Board) anbefalinger og observeret, at databehandlerens beskyttelsesniveau på overførsel af personoplysninger til tredjelande. Vi har observeret, at Amazon Web Services og Microsoft har en aktiv certificering og dermed har databehandleren et gyldigt overførselsgrundlag for at overføre dataansvarliges personoplysninger til underdatabehandlerne Amazon Web Services og Microsoft. Underdatabehandleren Abbyy har ikke en aktiv certificering, og dermed har databehandleren ikke et gyldigt overførselsgrundlag for at overføre dataansvarliges personoplysninger til underdatabehandleren Abbyy.	Vi har konstateret, at Amazon Web Services og Microsoft har tiltrådt det nye overførselsgrundlag EU-U.S. Data Privacy Framework, som trådte i kraft den 10. juli 2023. Databehandleren har redegjort for, at der i perioden før den 10. juli 2023, ikke skete overførsel af personoplysninger til usikre tredjelande, og at de har konfigureret samt implementeret sikringsforanstaltninger til beskyttelse af personoplysninger ved brug af Amazon Web Services og Microsoft som underdatabehandlere. Vi har konstateret, at databehandleren benytter Abbyy som underdatabehandler, uden at denne har tiltrådt det nye overførselsgrundlag. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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
Bistand til den dataansvarlige i forhold til de registreredes rettigheder - Databehandler har udarbejdet en procedure for bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder. - Det er muligt at give indsigt i alle oplysninger, der er registreret hos Vitec MV.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens udarbejdede procedure for behandling af indsigtsanmodninger fra den dataansvarlige og observeret, at denne anfører, at databehandleren skal yde bistand i form af oplysning om, hvorvidt der behandles personoplysninger om dataansvarlige, og om der kan udleveres de personoplysninger, som databehandleren behandler om dataansvarlige. Vi har ved forespørgsel fået oplyst, at der ikke har været forespørgsel fra dataansvarlig vedrørende bistand i forhold til de registreredes rettigheder, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for vejledning ved brud på persondatasikkerhed og observeret, at databehandleren skal underrette den dataansvarlige uden unødig forsinkelse, hvor underretningsfristen er 12 timer. Vi har foretaget inspektion af databehandlerens procedure for vejledning ved brud på persondatasikkerhed og observeret, at alt dokumentation og forløb om bruddet skal registreres. Vi har ved forespørgsel fået oplyst, at der i erklæringsperioden ikke har været brud på persondatasikkerheden, hvorfor det ikke har været muligt at efterprøve kontrollen.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for vejledning ved brud på persondatasikkerhed og observeret, at databehandleren har en procedure for vurdering og identifikation af brud på persondatasikkerheden. Vi har ved forespørgsel fået oplyst, at der i erklæringsperioden ikke har været brud på persondatasikkerheden, hvorfor det ikke har været muligt at efterprøve kontrollen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

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**
Registrering af brud på persondatasikkerheden ▶ Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen. ▶ Databehandleren har udarbejdet og implementeret en procedure for erfaringsopsamling ved brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for vejledning ved brud på persondatasikkerhed og observeret, at databehandleren har implementeret en procedure for erfaringsopsamling. Vi har ved forespørgsel fået oplyst, at der i erklæringsperioden ikke har været brud på persondatasikkerheden, hvorfor det ikke har været muligt at efterprøve kontrollen.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 33-34.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for vejledning ved brud på persondatasikkerhed og observeret, at dataansvarlige skal kontaktes 12 timer fra, at man er blevet bekendt med bruddet, og at der udøves bistand i forhold til dataansvarliges anmeldelse til Datatilsynet. Vi har ved forespørgsel fået oplyst, at der i erklæringsperioden ikke har været brud på persondatasikkerheden, hvorfor det ikke har været muligt at efterprøve kontrollen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

BDO Statsautoriseret revisionsaktieselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlems-firmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.700 medarbejdere, mens det verdensomspændende BDO-netværk har over 115.000 medarbejdere i 166 lande.

Copyright - BDO Statsautoriseret revisionsaktieselskab, cvr.nr. 20 22 26 70.

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

PENNEO

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

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

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-06-24 13:07:30 UTC

Hans-Erik Schou
CEO
Serienummer: a962d6db-feb5-4a50-9f0a-9b69cfa338e5
IP: 80.208.xxx.xxx
2024-06-24 13:27:33 UTC

Mikkel Jon Larssen
BDO Statsautoriseret revisionsaktieselskab CVR: 20222670
Partner, chef for Risk Assurance, CISA, CRISC
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2024-06-24 13:29:05 UTC

Penneo dokumentnøgle: N2CZN-YOC2S-EKS16-VYXZB-FPZMZ-EUK8K

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>.** Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**