cBrain A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden 1. januar 2023 til 31. december 2023 i henhold til databehandleraftale med de dataansvarlige, som anvender systemerne F2 og M4.

Indhold

1 Ledelsens udtalelse

cBrain A/S (herefter cBrain) behandler personoplysninger på vegne af de dataansvarlige i henhold til databehandleraftale.

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt F2- og M4-systemerne, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som underleverandører udfører og de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

cBrain anvender Sentia i forbindelse med levering af hosting-ydelser. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos cBrain og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos dataansvarlig, der forudsættes i designet af cBrains kontroller, er passende designet og operationelt effektive sammen med relaterede kontroller hos cBrain. Beskrivelsen omfatter ikke kontrolaktiviteter udført af dataansvarlig.

cBrain bekræfter, at:

a) Den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af funktioner udført af systemerne F2 og M4, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i perioden fra 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (I) Redegør for, hvordan informationssikkerhed og foranstaltninger i relation til systemerne F2 og M4 var designet og implementeret, herunder redegør for:

      i. De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger

      ii. De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger

      iii. De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige

      iv. 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

      v. 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

      vi. De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede

      vii. De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

      viii. Ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden

ix. Kontroller, som vi med henvisning til informationssikkerhed og foranstaltninger i relation til systemerne F2 og M4's afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

x. Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

(II) Indeholder relevante oplysninger om ændringer ved informationssikkerhed og foranstaltninger i relation til systemerne F2 og M4 til behandling af personoplysninger foretaget i perioden fra 1. januar 2023 til 31. december 2023

(III) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne informationssikkerhed og foranstaltninger i relation til systemerne F2 og M4 til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved informationssikkerhed og foranstaltninger i relation til systemerne F2 og M4, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og operationelt effektive i perioden fra 1. januar 2023 til 31. december 2023, hvis relevante kontroller hos underleverandører var hensigtsmæssigt designet og operationelt effektive, og de dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af cBrains kontroller i perioden fra 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(III) Kontrollerne var udført konsistent som designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. januar 2023 til 31. december 2023.

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

København, den 24. januar 2024
cBrain A/S

Robert Lentz
Direktør/COO
Kalkbrænderiløbskaj 2, 2100 København Ø

2 Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden 1. januar 2023 til 31. december 2023 i henhold til databehandleraftale med de dataansvarlige, som anvender systemerne F2 og M4.

Til: cBrain og dataansvarlige, der anvender systemerne F2 og M4

Omfang

Vi har fået som opgave at afgive erklæring om cBrains beskrivelse i sektion 3 af informationssikkerhed og foranstaltninger i relation til systemerne F2 og M4 i henhold til databehandleraftale med dataansvarlige, i perioden fra 1. januar 2023 til 31. december 2023 (beskrivelsen) og om designet og operationel effektivitet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af cBrains kontroller, er passende designet og er operationelt effektive sammen med relaterede kontroller hos cBrain. Vores handlinger har ikke omfattet kontrolaktiviteter udført af de dataansvarlige, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos de dataansvarlige.

cBrain anvender Sentia i forbindelse med levering af hosting-ydelser. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos cBrain og medtager således ikke kontrolmål og relaterede kontroller hos Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af cBrains kontroller, er passende designet og operationel effektive sammen med de relaterede kontroller hos cBrain. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Sentia, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

cBrains ansvar

cBrain er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 3, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene; identifikation af de risici der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier der er præsenteret i ledelsens udtalelse; samt for designet, implementeringen og operationel effektive kontroller for at nå 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.

EY Godkendt Revisionspartnerselskab 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.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om cBrains beskrivelse samt om designet og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og operationel effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i cBrains beskrivelse af F2 og M4 samt for kontrollernes design og operationel effektivitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive. 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, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som cBrain har specificeret og beskrevet i sektion 1.

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

Begrænsninger i kontroller hos en dataansvarlig

cBrains beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved F2 og M4, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet 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 sektion 1. Det er vores opfattelse,

(a) at beskrivelsen af informationssikkerhed og foranstaltninger i relation til systemerne F2 og M4, således som denne var designet og implementeret i perioden fra 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er retvisende,

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i perioden fra 1. januar 2023 til 31. december 2023, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontrollerne var operationelt effektive i perioden 1. januar 2023 til 31. december 2023, og hvis kontroller hos underleverandører og komplementerende kontroller hos dataansvarlige var hensigtsmæssigt designet og implementeret i perioden 1. januar 2023 til 31. december 2023, som forudsat i designet af cBrains kontroller, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har været operationelt effektive i perioden fra 1. januar 2023 til 31. december 2023, hvis kontroller hos underleverandør var operationelt effektive, og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af cBrains kontroller, har været operationelt effektive i perioden fra 1. januar 2023 til 31. december 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår af sektion 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt cBrains F2- og M4-systemer, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 24. januar 2024
EY Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Jesper Due Sørensen
Partner

Johanna Kansonen-Valtersdorf
statsaut. revisor
mne48476

3 Beskrivelse af behandling

cBrain A/S er leverandør af F2- og M4-løsningerne med tilhørende serviceydelser til cBrains kunder.

Løsningerne understøtter kunder i en lang række forskellige digitale forretningsprocesser, som involverer medarbejdere, medlemmer, borgere, myndigheder og virksomheder. Løsningerne er implementeret i organisationer i både privat sektor og i offentlig sektor. De digitale forretningsprocesser er fx. sags- og dokumenthåndtering, fagprocesser, medlemshåndtering, mødebooking, ledelsesbetjening, tilskudsadministration, afgørelser, godkendelser og meget mere. Kunder er placeret i Danmark og internationalt.

Ydelser relateret til digitalisering kan både være konsulentydelser og ydelser, der involverer levering af programmel.

I relation til databehandling er der en lang række ydelser, som ikke medfører, at cBrain er databehandler, fx. i forbindelse med konsulentopgaver som rådgivning, uddannelse, workshops, designopgaver, arkitekturopgaver. Der er også ydelser af programmel, hvor cBrain ikke er databehandler, fx. i forbindelse med opgaver hvor der skal udarbejdes et Proof of Concept eller ved installation af et testsystem.

3.1 Karakteren af behandlingen

Når cBrain er databehandler, er der tale om leverance af ydelser, som er karakteriseret ved, at cBrain er;

- leverandør af drift
- leverandør af support
- leverandør af ad hoc-opgaver.

3.1.1 cBrain er leverandør af drift

Denne ydelse udføres for kunder, som har en hosting-aftale eller Cloud-aftale, og som er placeret i cBrains driftsmiljø. I dette tilfælde er det cBrains ansvar at sikre, at driften udføres i henhold til aftalte Service Level Agreement og i henhold til de sikkerhedsbestemmelser, som er indgået.

3.1.2 cBrain er leverandør af support

Alle kunder har en aftale om programmel vedligeholdelse, og i den forbindelse gives der adgang til supportydelser. I forbindelse med udførelse af supportydelser, har cBrain adgang til kundens systemer og data. Adgangen til data og dermed behandlingen af data sker udelukkende med henblik på at afhjælpe kundens problem eller spørgsmål i relation til det programmel, som indgår under aftalen om programmelvedligeholdelse. Er der tale om fejl i programmel, afhjælpes problemet med rettelser til programmel.

3.1.3 cBrain er leverandør af ad hoc-opgaver

Aftaler om levering af opgaverne kan ske i de leveranceaftaler, hvor kunden skal i drift første gang, eller i det efterfølgende samarbejde, hvor kunden ønsker yderligere leverancer. Yderligere leverancer er reguleret af leverancekontrakten og betegnes som Ændringsønsker. Opgaver, som medfører, at cBrain behandler data, er eksempelvis ved:

- konvertering af data
- opgradering
- aflevering til Rigsarkivet
- flytning af database
- opdatering af database.

De generelle vilkår omkring behandling af data og instrukser er anført i databehandleraftalerne. Der udføres om udgangspunkt udelukkende behandling af data for kunder, som har indgået en databehandleraftale med cBrain. Derudover har cBrain indført en yderligere angivelse af instruks for de ad hoc-opgaver, som udføres. Dermed bliver de relevante medarbejdere hos kunden og hos cBrain opmærksomme på den specifikke instruks, der relaterer sig til den konkrete opgave.

3.2 Personoplysninger

Karakteren af den anvendelse, som kunden udfører med programmellet, medfører, at typen af data kan have karakter af personfølsomme oplysninger.

Typen af personfølsomme oplysninger er eksempelvis:

- almindelige personoplysninger, herunder identifikationsoplysninger som navn og adresse eller oplysninger om økonomi, skat, gæld, væsentlige sociale problemer, andre rent private forhold, sygedage, tjenstlige forhold, familieforhold, bolig, bil, uddannelse, eksamen, ansøgning, CV, ansættelsesdato og -stilling, arbejdsområde og arbejdstelefon
- særlige kategorier af personoplysninger, herunder race og etnisk oprindelse, fagforeningsmæssige tilhørsforhold og helbredsoplysninger
- andre personlige oplysninger, herunder oplysninger om strafbare forhold og CPR-numre.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- ansatte
- borgere
- udlændinge (som skal arbejde eller studere i DK, eller som søger statsborgerskab)
- personer med tilknytning til virksomheder.

3.3 Praktiske tiltag

Der er etableret et veldokumenteret kontrolapparat for understøttelse af sikkerhed for databehandling i de tre overordnede ydelser for henholdsvis drift, support og ad hoc-opgaver.

cBrain har tilrettelagt it-sikkerheden med udgangspunkt i ISO 27001. Processer i tilknytning til F2-produktet og medarbejdere ansat i Danmark er ISO 27001-certificeret.

Medarbejdere er underlagt fortrolighedserklæringer, og der er etableret processer for onboarding, offboarding og reboarding, som sikrer, at adgangsforhold m.m. stemmer overens med ansættelsesforhold. En lang række af cBrains medarbejdere er sikkerhedsgodkendte for at kunne arbejde med kunder i den offentlige sektor. Der udføres løbende awareness-tiltag med henblik på at sikre, at medarbejdere kontinuerligt bliver opdateret på sikkerhedstiltag og -processer.

Udvikling af programmel udføres af medarbejdere ansat af cBrain i Danmark og de støttesystemer, som anvendes til programmelvedligeholdelse, og supporthenvendelser bliver ligeledes driftet og vedligeholdt af cBrain-medarbejdere i Danmark.

Der arbejdes med standarder for sikkerhed omkring adgangsstyring til data, og niveauer for beskyttelse er udført i samarbejde med kunden. Der er kontrolforanstaltning og -rapportering i de tilfælde, hvor kunden afviger fra den anbefalede tilgang.

Der er Standard Operating Procedures (SOP) for en lang række aktiviteter, herunder for håndtering af personhenførbare data i forbindelse med supportrapporteringer. Der er indført protokoller for, hvad der er tilladt, og hvordan og hvornår der slettes data fra supportsystemer.

3.4 Anvendelse af underleverandør

cBrain anvender Sentia som samarbejdspartner i forbindelse med levering af hosting-ydelser.

Sentia er en full-service hosting-virksomhed. Selskabet leverer professionelle it-løsninger til offentlige og private virksomheder. Ydelserne omfatter virtuelle løsninger, colocation (fysiske rackskabe), driftsløsninger og outsourcing, backup (inklusive remote backup), storage, professionelle internetforbindelser, IP-trafik og sikrede omgivelser. Sentia driver datacentre i Danmark, der er redundant forbundet via egen infrastruktur, som er forbundet med Danmarks største teleknudepunkter.

I relation til samarbejde med cBrain, leverer Sentia kun de fysiske rammer for hostingen, mens cBrain ejer og administrerer hardware og software inklusive basis software, databaser m.m. Kun udvalgte cBrain-medarbejdere har adgang til cBrains servere placeret i Sentias lokationer i Danmark. Kunders data inklusive backup er placeret i Danmark.

Sentias administrative personale har ikke adgang til at forbinde til cBrains servere. Af supporthensyn for at sikre maksimal oppetid og evt. fejlfinding har Sentia dog administrative rettigheder til firewall i Taastrup. Det er vurderet, at Sentia ikke er underdatabehandler, som følge af at Sentia ikke har adgang til servere og dermed heller ikke til data.

It-sikkerheden hos Sentia efterprøves ved, at de hvert år får udarbejdet ISAE 3000- og 3402-erklæringer. Deres ISAE-erklæringer gennemgås og godkendes efterfølgende i cBrain. Det bemærkes, at denne ISAE-rapport ikke inkluderer de ydelser, som Sentia leverer.

Gennem ejerskabet af servere m.m., som både er placeret hos Sentia og i cBrains kontorlokaler, sikrer cBrain, at personer eller organisationer fra sikre/usikre tredjelande ikke har adgang til at behandle data eksempelvis i forbindelse med supportydelser (dette gælder også "se-adgang") eller udvikling.

På cBrains kontorlokaler i Danmark kræves der adgangschip samt kode for at tilgå serverlokalet. Adgang til kontorlokalerne kræver adgangschip i dagtimerne og adgangschip og kode uden for normal åbningstid.

3.5 Risikovurdering

cBrain gennemfører mindst én gang årligt en risikovurdering. Vurderingen er baseret på KOMBITs standard for risikovurdering. Selve vurderingen tager udgangspunkt i en række potentielle hændelser, hvori risikoen for tab af fortrolighed, tab af integritet, og tab af tilgængelighed indgår. For hver af disse er der foretaget en vurdering af risikoen for, at hændelsen indtræffer, og hvilken konsekvens denne måtte have (Konsekvens for den registrerede, Omdømme, Økonomisk osv.).

cBrains ledelse afholder kvartalsvis Management Review-møder, som behandler compliance i forhold til ISO27001. Management Review møder er et krav under ISO27001.

3.6 Processer vedrørende personoplysninger

Processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger.

Al behandling af personoplysninger i kundedata, skal følge en instruks.

Instruksen kan være udtrykt i relation til følgende:

- Leverance-aftaler
- Hosting-aftaler
- Programmel vedligeholdelse
- Support
- Ad hoc-opgaver eller individuelle opgaver, eksempelvis opgradering, integration, aflevering.

Instruksen er reguleret af databehandleraftalen, som indgås med kunden. Instruksen omfatter igangsætning, registrering, behandling inkl. begrænsninger, korrigering og sletning af personoplysninger.

Alle standardydelser med relation til GDPR (behandling af personoplysninger) bliver godkendt af et medlem af Chefgruppen, så det sikres, at disse er i overensstemmelse med gældende lovgivning.

cBrain gennemfører en vurdering ved ændring i lovgivning eller hvis der kommer nye retningslinjer fra Datatilsynet eller fra Kombit i forhold til databehandleraftaler.

Alle hændelser, der er blevet vurderet i strid med lovgivning skal meldes til den dataansvarlige.

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.

Procedurer for datahåndtering ved opsigelse gælder for kunder, hvis aktiviteter er placeret i cBrains hostingcenter.

cBrain udleverer data til kunden i cBrain hostede F2 og M4 systemer i forbindelse med kundeexit, i henhold til aftale med kunderne herom. Systemerne inkl. data slettes efterfølgende, som del af kunde-offboarding-processen.

Data i cBrains supportsystem slettes løbende. Rutiner og retningslinjer er på plads for både kundernes og cBrain-medarbejdernes brug af supportsystemet for at forhindre brugen af personlige oplysninger i supportsager.

Processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede.

cBrain har en procedure for håndtering af sikkerhedsbrud, som inkl. underretning af påvirkede kunder om:

a) Karakteren af bruddet på sikkerheden

b) Sandsynlige konsekvenser af brud på sikkerheden

c) Foranstaltninger, der er truffet eller foreslået for at håndtere brud på sikkerheden.

cBrain har i databehandleraftaler anført, hvorledes der ydes støtte til den dataansvarlige i relation til registreredes rettigheder. cBrain har procedure, der sikrer, at dette håndteres i henhold til den indgåede databehandleraftale.

Proceduren muliggør en rettidig bistand til den dataansvarlige i relation til følgende punkter:

- Udlevering af oplysninger
- Rettelse af oplysninger
- Sletning af oplysninger
- Begrænsning af behandling af personoplysninger
- Oplysning om behandling af personoplysninger til den registrerede.

Processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Proceduren for etablering af sikkerhedsforanstaltninger er defineret ved de forskellige instrukser.

Instruksen kan være udtrykt i relation til følgende:

- Leverance-aftaler
- Hosting-aftaler
- Programmel vedligeholdelse
- Support (Ad hoc-opgaver)
- Individuelle Løsningsbeskrivelser (Opgradering, Integration, Aflevering).

cBrain har indført standard operating-procedurer for opgaver, og der er angivet procedurer i relation til ISO 27001.

Risikovurdering foretages årligt for virksomheden, herunder for F2, M4 samt leverandører. Reevaluering og opsamling på risikovurderingerne sker kontinuerligt på Management Review-møder.

cBrain har implementeret IT-sikkerheds- og GDPR-politikker. Nye cBrain-medarbejdere modtager undervisning i IT-sikkerhed ved ansættelsesstart, og der gennemføres årligt genopfriskningstræning for alle medarbejdere. Ansatte i cBrain er underlagt fortrolighedsbestemmelser, både under og efter ansættelse i cBrain.

cBrain indgår databehandleraftaler med kunder og leverandører i relevant omfang. En gang årligt kontrolleres at indgåede databehandleraftaler er i overensstemmelse med IT-sikkerheds- og GDPR-politikker.

3.7 Kontrolforanstaltninger

Der er indført en lang række kontrolforanstaltninger, som til dels er anbefalet i forhold til målrettet beskyttelse af persondata og i forhold til ISO 27001-aktiviteter. Kontrolforanstaltninger bliver løbende justeret og revideret i forhold til risikovurderinger og ændringer i markedsforhold generelt.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

3.8 Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige har følgende forpligtelser:

- Den dataansvarlige skal sikre, at den givne instruks til enhver tid er dækkende for den behandling af personoplysninger, som cBrain varetager på vegne af den dataansvarlige, og at behandlingen er i overensstemmelse med gældende særlovgivning og databeskyttelsesretlige love og reguleringer.
- cBrain kan med forudgående aftale med kunden opsætte logning i systemerne. Det er dermed kundens eget ansvar at tage stilling til de opsatte logningskrav i brugergrænsefladen i M4 og F2. Kunderne er også selv ansvarlige for, at logs gennemgås regelmæssigt. Det er kun medlemsadministratorrollen hos kunderne, som har adgang til loggen.
- Kunder på F2 og M4 skal selv tildele medarbejdere en rolle, der giver forskellige niveauer af adgange til løsningerne. Det er kundens eget ansvar at sikre, at disse rettigheder kun gives til relevante ansatte, samt cBrain medarbejdere og det niveau af adgang, de enkelte medarbejder bør have.
- Hver kunde har adgang til et testmiljø og et produktionsmiljø, som er selvstændige installationer til den enkelte kunde. Det er kundernes eget ansvar at sikre, at testdata på testmiljøet ikke indeholder data på virkelige personer.
- Den dataansvarlige skal selv indføre kontroller for styring af brugeres adgange og rettigheder i M4 og F2.
- Den dataansvarlige skal sikre, at personoplysninger i M4 og F2 slettes i overensstemmelse med lovgivningen.
- Den dataansvarlige skal sikre, at de lever op til det ansvar, som er angivet i databehandleraftalen, herunder advisering ved tilfælde af brud på datasikkerheden.

4 Tests udført af EY

4.1 Formål og omfang

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

Vores test af kontrollers design og operationelle effektivitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af afsnit 3. Eventuelle andre kontrolmål, tilknyttede kontroller og komplementære kontroller hos dataansvarlige, der anvender løsningen, beskrevet i afsnit 3, er ikke omfattet af vores test.

Test af design og operationel effektivitet har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden fra 1. januar 2023 til 31. december 2023.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og operationel effektivitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er designet og effektive i perioden fra 1. januar 2023 til 31. december 2023.
Forespørgsler	Forespørgsel af passende personale hos cBrain. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

4.3 Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
A.2	cBrain udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret stikprøvevist på behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
A.3	cBrain underretter omgående den dataansvarlige, hvis en instruks efter cBrains mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Forespurgt, om cBrain har registreret tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen. Inspiceret liste af incidents.	cBrain har oplyst, at man ikke har registreret tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
B.2	cBrain 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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at cBrain foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at cBrain har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret procedurer for forebyggelse og detektering af et udbrud af ondsindet kode og reetablering efter et ondsindet virusangreb. Inspiceret et udvalg af enheder med henblik på at konstatere, om virusbeskyttelse er installeret, kørende og opdateret.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret netværkstegninger for cBrain og Sentia, som viser, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at Sentia firewall er konfigureret i henhold til cBrains interne politik herfor.	Ingen afvigelser konstateret.
B.5	Netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Inspiceret netværkstegninger, som viser, at netværk hos cBrain og Sentia er segregerede.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret stikprøvevist på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret procedurer for indsamling og vurdering af tekniske sårbarheder. Inspiceret servere, databaser, arbejdspladser for at konstatere, hvorvidt systemerne er rettidigt patchet i perioden dækket af erklæringen.	Ingen afvigelser konstateret.
B.9	Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres og opbevares. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Inspiceret, at der foreligger krav til omfang og indhold af hændelseslogninger. Inspiceret, at der er opsat auditlogning. Inspiceret, at der udføres regelmæssig gennemgang af logs.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret proceduren vedrørende udvælgelse og beskyttelse af testdata. Inspiceret dokumentation fra testmiljøer med henblik på at konstatere, at testdata er anonymiseret og derfor ikke indeholder fortrolige eller personlige oplysninger.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Inspiceret procedurer for indsamling og vurdering af tekniske sårbarheder. Inspiceret servere, databaser, arbejdspladser for at konstatere, hvorvidt systemerne er rettidigt patchet i perioden dækket af erklæringen.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret servere, databaser, arbejdspladser for at konstatere, hvorvidt systemerne er rettidigt patchet i perioden dækket af erklæringen Forespurt om der har været ændringer til M4-system i erklæringsperioden. Inspiceret liste af ændringer i sagsstyringssystem.	cBrain har oplyst, at der ikke er udført ændringer med relation til M4 systemet i erklæringsperioden. Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til systemer. Administrative brugeres adgang revurderes årligt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret proceduren for registrering og afmelding af brugere. Inspiceret proceduren for oprettelse og nedlæggelse af et udvalg af brugere, der henholdsvis til- og fratrådte i erklæringsperioden med henblik på at konstatere, om procedurerne for brugeroprettelse og -nedlæggelse er fulgt. Inspiceret at der foreligger dokumentation for årlig vurdering og godkendelse af administrative brugeradgange.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
C.1	cBrains ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder cBrains medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt i revisionsperioden. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til cBrains medarbejdere.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
C.2	cBrains ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret stikprøvevist på databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af cBrains medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Eksamensbeviser.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af cBrains medarbejdere i forbindelse med ansættelse i relevant omfang. Inspiceret stikprøvevist på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at der er udført en vurdering af de ansatte inden ansættelsen.	Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret stikprøvevist på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret stikprøvevist på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har modtaget træning i informationssikkerhedspolitik og procedurer vedrørende databehandling.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at cBrain har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	***cBrains kontrolaktivitet***	***EY's udførte test***	***Resultat af EY's test***
C.5	Ved fratrædelse er der hos cBrain implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører.	Inspiceret proceduren for ansættelsesophør og fjernelse og rettelse af adgangsrettigheder. Stikprøvevist inspiceret fratrådte medarbejdere med henblik på at konstatere, om medarbejderne havde fået fjernet deres adgangsrettigheder i relevante systemer.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, cBrain udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret stikprøvevist på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen afvigelser konstateret.
C.7	cBrain udfører awareness-træning af cBrains medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger en gang årligt. Hertil introduceres medarbejdere til it-sikkerhed i forbindelse med deres ansættelse.	Inspiceret, at cBrain udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger årligt. Inspiceret dokumentation for, at cBrains medarbejdere har modtaget den udbudte awareness-træning. Inspiceret stikprøvevist på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har modtaget træning i informationssikkerhedspolitik og procedurer vedrørende databehandling.	Ingen afvigelser konstateret.

Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
D.2	Der er aftalt følgende krav til cBrains opbevaringsperioder og sletterutiner: • For dataansvarlige, som har en hostingaftale, opbevares og behandles data alene inden for Danmark. • Ved ophør af tjenesterne vedrørende behandling forpligtes cBrain til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til cBrains opbevaringsperioder og sletterutiner. Inspiceret stikprøvevist, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med databehandleraftalen. Forespurgt på ophørte databehandlinger i erklæringsperioden, om der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført i henhold til databehandleraftalen.	cBrain har oplyst, at der ikke har været ophør af behandling af personoplysninger i erklæringsperioden. Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Forespurgt på ophørte databehandlinger i erklæringsperioden, om der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført i henhold til databehandleraftalen.	cBrain har oplyst, at der ikke har været ophør af behandling af personoplysninger i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at cBrain alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
E.2	cBrains databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at cBrain har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret stikprøvevist på databehandlinger, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål H Der efterleves procedurer og kontroller, som sikrer, at cBrain kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at cBrain skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for cBrains bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
H.2	cBrain 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.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Forespurgt, om cBrain har modtaget nogen anmodninger om bistand i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede i erklæringsperioden.	cBrain har oplyst, at de ikke har modtaget anmodninger om bistand i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at cBrain skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	cBrain har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik.	Inspiceret, at cBrain gennemfører awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer m.v.	Ingen afvigelser konstateret.
I.3	cBrain har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos cBrain eller en underleverandør.	Inspiceret, at cBrain har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Inspiceret, at cBrain har medtaget eventuelle brud på persondatasikkerheden hos underleverandører i cBrains log over sikkerhedshændelser. Forespurgt om der har været registreret brud på persondatasikkerheden hos cBrain. Inspiceret oversigt over sikkerhedshændelser.	cBrain har oplyst, at der ikke er registreret brud på persondatasikkerheden i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	*cBrains kontrolaktivitet*	*EY's udførte test*	*Resultat af EY's test*
I.4	cBrain har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Forespurgt om der er registreret nogen brud på persondatasikkerheden i erklæringsperioden. Inspiceret oversigt over sikkerhedshændelser.	cBrain har oplyst, at der ikke er registreret brud på persondatasikkerheden, som er meddelt til datatilsynet i erklæringsperioden. Ingen afvigelser konstateret.

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."

Robert Lentz
Direktion
På vegne af: cBrain A/S
Serienummer: 6dc38cf6-95f0-4fe9-a814-ca47a9899994
IP: 188.120.xxx.xxx
2024-01-24 14:35:54 UTC

Johanna Sini Annikki Kansonen-Valtersdorf
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: 8af9acce-b73e-4a45-b435-2f7d1272dfaa
IP: 165.225.xxx.xxx
2024-01-24 14:40:48 UTC

Jesper Due Sørensen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3
IP: 80.208.xxx.xxx
2024-01-24 15:02:32 UTC