Det Danske Madhus A/S

Roholmsvej 11D
2620 Albertslund
CVR.NR. 27 38 53 54

ISAE 3000, type 2

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger for perioden 11. juni 2023 – 30. juni 2024

Indhold

S.nr. 367352

JR/SO

1. Ledelsens udtalelse

Det Danske Madhus A/S varetager behandling af personoplysninger på vegne af vores kunder, der er dataansvarlige i henhold til indgåede databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Det Danske Madhus A/S' madservices, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som 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 kaldet "databeskyttelsesforordningen") er overholdt.

Det Danske Madhus A/S bekræfter, at:

a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Det Danske Madhus A/S' madservice, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden 11. juni 2023 - 30. juni 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Det Danske Madhus A/S' systemer var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - 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
   - 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 underrettelse til de registrerede
   - 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
   - Kontroller, som vi 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
   - 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 ydelsen til behandling af personoplysninger foretaget i perioden 11. juni 2023 – 30. juni 2024.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne ydelse 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 ydelsen, 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 udformet og fungerede effektivt i hele perioden 11. juni 2023 til 30. juni 2024. 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 anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 11. juni 2023 til 30. juni 2024.

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.

Albertslund, den 30. august 2024
Det Danske Madhus A/S

Søren Stoltenberg Vilmand
CEO

Peter Tietgen
Direktør

2. Beskrivelse af behandling

Kort intro til virksomheden
Det Danske Madhus A/S bringer hjemmelavet mad til døren, med et udvalg af danske, vegetariske og internationale retter. Vi har et varieret menukort, der passer til forskellige præferencer og ernæringsbehov. Vores mission er at forbedre livskvaliteten med velsmagende og sund mad. Vi hjælper ældre og personer med særlige kostbehov med at få bedre livskvalitet. Vi blev grundlagt i 2003, er en markedsleder i måltidsløsninger til hjem og institutioner, og tilhører den tyske virksomhed Apetito.

Ydelsesbeskrivelse
Målet med denne beskrivelse er at informere Det Danske Madhus A/S' kunder og deres interessenter (inklusive revisorer) om overholdelsen af databehandleraftalerne med de kommuner, hvor Det Danske Madhus A/S yder madservice. Derudover er målet med denne beskrivelse at give oplysninger om sikkerheden af behandlingen, tekniske og organisatoriske foranstaltninger samt ansvarsfordeling mellem dataansvarlige (vores kunder) og Det Danske Madhus A/S.

Beskrivelse af aftaleforhold mellem parterne
Det Danske Madhus A/S leverer madservices til kommunernes borgere, hvor formålet er at håndtere egenbetaling og sikre korrekt levering af mad i henhold til kommunens anvisninger. Dette kræver en databehandleraftale for at sikre overholdelse af databeskyttelsesregler. Aftaleforholdet er baseret på en hovedaftale mellem kommunen og Det Danske Madhus A/S, som omfatter specifikke instrukser fra kommunen om, hvordan personoplysninger skal behandles. Der er også etableret underdatabehandleraftaler med IT-leverandører for at sikre databeskyttelse og overholdelse af ISAE 3000 krav.

Disse aftaler sikrer, at Det Danske Madhus A/S kan levere ydelserne korrekt og sikkert, og at alle behandlingsaktiviteter er i overensstemmelse med gældende lovgivning og kommunens specifikationer.

Karakteren af behandlingen
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om administration og levering af madservice til kommunens borgere. Dette inkluderer håndtering af egenbetaling, korrekt levering af ydelser baseret på borgernes specifikke behov og præferencer samt opbevaring og behandling af følsomme oplysninger for at sikre en skræddersyet service.

Beskrivelse af typen af personoplysninger, der behandles:

- **Almindelige personoplysninger**
    - Identifikationsoplysninger: Navn, adresse, CPR-nummer.
    - Oplysninger om visiteret kostform og ydelsesfrekvens: Disse data bruges til at sikre, at borgerne modtager den rette type madservice med den rette hyppighed.
- **Særlige kategorier af personoplysninger**
    - Helbredsoplysninger: Disse inkluderer oplysninger, der er relevante for levering af madservice, såsom borgerens mobilitet og høreevne. Eksempler på disse oplysninger kan være:
        - "Borger er dårligt gående; vent på borger åbner døren."
        - "Borger er dårligt hørende; ring på 3 gange."
    - Andre følsomme oplysninger kan inkludere kostpræferencer, der er relateret til borgerens helbredstilstand, som f.eks. allergier eller specielle diæter.

- **Andre personlige oplysninger**
    - CPR-numre: Disse bruges til entydig identifikation af borgerne for at sikre korrekt opkrævning af egenbetaling og for at kunne følge kommunens retningslinjer for registrering og rapportering.
    - Økonomiske oplysninger: Håndtering af egenbetaling for madservice, som foretages som et træk i borgernes pension.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- **Borgere visiteret til madservice:**
    - Ældre borgere: De primære modtagere af madservice, som typisk er ældre personer, der har brug for hjælp med måltiderne.
    - Borgere med særlige behov: Dette kan inkludere personer med fysiske eller mentale udfordringer, som kræver speciel opmærksomhed og tilpasning af madleveringen baseret på deres individuelle behov.
    - Kommunens borgere generelt: Enhver borger, der er visiteret af kommunen til at modtage madservice, omfattes af databehandleraftalen.

Disse oplysninger sikrer, at Det Danske Madhus A/S kan levere en effektiv og præcis madservice, som er tilpasset hver enkelt borgers behov, og samtidig opfylder alle databeskyttelseskrav i henhold til gældende lovgivning.

Praktiske tiltag
En beskrivelse af de praktiske tiltag, herunder såvel tekniske som organisatoriske, som databehandleren har gennemført for at sikre overholdelse af sine forpligtelser efter databehandleraftalen.

Organisering af informationssikkerhed
Det Danske Madhus A/S har en klar fordeling af ansvarsområderne for informationssikkerheden, hvor Head of IT og GDPR-responsible står for at indføre, vedligeholde og overvåge sikkerhedsforanstaltningerne. De har også en central rolle i at implementere nye systemer og arbejde sammen med leverandører om at opfylde kravene til databeskyttelse. Når der startes et samarbejde med nye underdatabehandlere, vurderer Head of IT eller GDPR-responsible behovet for en databehandleraftale og indhenter den. Underleverandørernes kontrolmål gennemgås hvert år, og de tekniske og organisatoriske krav i databehandleraftalen tjekkes løbende gennem audits.

Politikker og retningslinjer
Det Danske Madhus A/S har udviklet en række politikker og retningslinjer, der understøtter informationssikkerhed og databeskyttelse:

- **Informationssikkerhedspolitik:** En omfattende politik, der beskriver nødvendige sikkerhedsforanstaltninger og adfærd for at beskytte virksomhedens informationer. Denne politik er tilgængelig for alle medarbejdere via intranetportalen Actimo.
- **Persondatapolitik:** En specifik politik, der fastlægger retningslinjer for behandling af personoplysninger i overensstemmelse med GDPR. Politikken er også tilgængelig for alle medarbejdere via intranetportalen Actimo.

Procedurer og kontroller
For at sikre efterlevelse af informationssikkerhedspolitikkerne og persondatapolitikken er der etableret følgende procedurer og kontroller:

- Medarbejdersikkerhed
- Styring af informationsaktiver
- Adgangsstyring
- Kryptering
- Fysisk sikkerhed
- Driftssikkerhed
- Kommunikationssikkerhed

- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af sikkerhedshændelser
- Nød-, beredskabs- og reetableringsstyring

Tekniske og organisatoriske kontroller
Der er implementeret en række tekniske og organisatoriske kontroller for at beskytte personoplysninger:

- Kontrolskema for ansættelse og fratrædelse samt dokumentation for udlevering og returnering af aktiver.
- Kryptering af trådløse netværk for at forhindre udefrakommende adgang.
- Løbende kontroller baseret på et årshjul for at sikre overholdelse af interne processer.
- CyperPilot aftale for løbende awarenesstræning for at forebygge risikoen for persondatasikkerhedsbrud.
- Hurtig underretning og analyse ved potentielle sikkerhedsbrud indenfor 24 timer, inklusive anmeldelse til datatilsynet og kommunikation med berørte personer.

Disse tiltag sikrer, at Det Danske Madhus A/S overholder sine forpligtelser i henhold til databehandleraftalen og beskytter personoplysningerne på en sikker og effektiv måde. Ved at have en stærk organisering af informationssikkerheden, klare politikker og retningslinjer samt omfattende tekniske og organisatoriske kontroller, kan Det Danske Madhus A/S levere sine ydelser med høj grad af sikkerhed og overholdelse af gældende databeskyttelseslovgivning.

Risikovurdering
En beskrivelse af hvordan databehandleren har foretaget en kortlægning over risikoen for de registreredes rettigheder herunder en afvejning af disse risici i forhold til de forholdsregler der bliver truffet for at beskytte disse rettigheder. Denne risikovurdering er baseret på en detaljeret flowbeskrivelse af data, hvordan data modtages, opbevares, deles og slettes i Det Danske Madhus A/S. For at sikre løbende overholdelse af processer gennemføres der interne kontroller baseret på et årshjul, som fungerer som sikring af, at ikke eliminerede risici kontinuerligt fastholdes under kontrol.

Kortlægning af risici
Det Danske Madhus A/S har foretaget en flow-beskrivelse af data, hvordan denne modtages, opbevares, deles og slettes i Det Danske Madhus A/S. Denne kortlægning involverer følgende trin:

1. **Identifikation af risici:** Kortlægning af alle potentielle risici forbundet med behandlingen af personoplysninger, herunder uautoriseret adgang, datalækage, dataforvanskning og systemfejl.

2. **Kategorisering af risici:**

    - **Sandsynlighed:** Vurdering af sandsynligheden for, at hver identificeret risiko vil opstå. Dette omfatter en scoring baseret på historiske data, sikkerhedsinfrastruktur og andre relevante faktorer.

    - **Alvorlighed:** Vurdering af alvorligheden af konsekvenserne, hvis en risiko materialiserer sig. Dette inkluderer potentielle påvirkninger på de registreredes privatliv, økonomi, og generelle sikkerhed.

Vurdering af passende foranstaltninger
Efter kortlægningen af risici, vurderer Det Danske Madhus A/S, hvilke tekniske og organisatoriske foranstaltninger der er passende for at sikre overholdelse af forordningen og beskytte de registreredes rettigheder:

1. **Tekniske foranstaltninger:**

    - Implementering af kryptering for at beskytte data under transmission og opbevaring.

    - Adgangsstyring for at begrænse adgangen til personoplysninger til kun autoriserede personer.

    - Regelmæssige sikkerhedsopdateringer og vedligeholdelse af systemer for at beskytte mod sikkerhedstrusler.

2. **Organisatoriske foranstaltninger:**
    - Uddannelse og træning af medarbejdere i informationssikkerhed og databeskyttelse.
    - Etablering af klare politikker og procedurer for håndtering af personoplysninger.
    - Regelmæssige audits og overvågning af compliance med databeskyttelsesregler.

Kontrolforanstaltninger
En beskrivelse af, hvilke kontrolforanstaltninger databehandleren har iværksat og gennemført til måling og kontrol af virkningen af det etablerede ledelsessystem for informationssikkerhed og for behandling af personoplysninger samt resultatmålinger herfra.

Hovedområder for procedurer og kontroller
Det Danske Madhus A/S har udarbejdet og implementeret en række procedurer og kontroller, som er i overensstemmelse med databeskyttelsesforordningen (GDPR) og den indgående databehandleraftale:

- **Instruks vedrørende behandling af personoplysninger:** Sikrer, at behandlingen af personoplysninger sker i overensstemmelse med den indgående databehandleraftale.
- **Tekniske foranstaltninger:** Implementering af passende tekniske foranstaltninger for at sikre behandlingssikkerheden, herunder kryptering, adgangsstyring og regelmæssige sikkerhedsopdateringer.
- **Organisatoriske foranstaltninger**: Etablering af organisatoriske foranstaltninger såsom medarbejderuddannelse, informationssikkerhedspolitik, og løbende overvågning af compliance med sikkerhedsprocedurer.
- **Sletning eller tilbagelevering af personoplysninger:** Personoplysninger kan slettes eller tilbageleveres til den dataansvarlige efter aftale.
- **Opbevaring af personoplysninger**: Personoplysninger opbevares alene i overensstemmelse med aftalen med den dataansvarlige.
- **Godkendte underdatabehandlere:** Anvendelse af godkendte underdatabehandlere samt regelmæssig opfølgning på deres tekniske og organisatoriske foranstaltninger for at sikre en betryggende behandlingssikkerhed.
- **Overførsel af personoplysninger:** Personoplysninger overføres alene til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige og på baggrund af et gyldigt overførselsgrundlag.
- **Bistand til dataansvarlig:** Databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.
- **Håndtering af sikkerhedsbrud:** Eventuelle sikkerhedsbrud håndteres i overensstemmelse med den indgåede databehandleraftale, herunder rettidig underretning af den dataansvarlige og relevante myndigheder.

Disse kontrolforanstaltninger sikrer, at Det Danske Madhus A/S opretholder en høj standard for informationssikkerhed og databeskyttelse, som kontinuerligt overvåges og evalueres for effektivitet. For yderligere detaljer om konkrete kontrolaktiviteter henvises til afsnit 4.

Komplementerende kontroller hos de dataansvarlige
Som led i levering af ydelserne er der kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i beskrivelsen. Dette omfatter blandt andet, at den dataansvarlige:

- **Sikrer, at personoplysningerne er ajourførte:** Det er afgørende, at alle personoplysninger, der behandles, er nøjagtige og opdaterede for at sikre korrekt levering af ydelser og overholdelse af databeskyttelseskravene.

- **Sikrer, at instruksen er lovlig:** Instruksen, der gives til databehandleren, skal være i overensstemmelse med den til enhver tid gældende persondataretlige regulering for at sikre, at behandlingen af personoplysninger sker lovligt.

- **Sikrer, at instruksen er hensigtsmæssig:** Instruksen skal være hensigtsmæssig i forhold til databehandleraftalen og hovedydelsen for at sikre, at behandlingen af personoplysninger understøtter formålet med aftalen og leveringen af ydelserne.

- **Sikrer, at den dataansvarliges brugere er ajourførte:** Brugerne hos den dataansvarlige, der har adgang til personoplysningerne, skal være opdaterede med de nødvendige oplysninger og træning for at sikre korrekt håndtering og beskyttelse af data.

- **Sikrer, at den fornødne hjemmel til behandling er til stede:** Det er den dataansvarliges ansvar at sikre, at der er lovhjemmel til behandlingen af personoplysninger, herunder samtykke fra de registrerede eller anden relevant hjemmel.

- **Efterlever oplysningspligten:** Den dataansvarlige skal sikre, at de registrerede informeres om deres rettigheder og om, hvordan deres personoplysninger behandles, samt sikre at de kan udøve disse rettigheder.

- **Kontrollerer identiteten af de registrerede**: Når de registrerede ønsker at udøve deres rettigheder, skal den dataansvarlige kontrollere deres identitet for at sikre, at oplysningerne ikke gives til uvedkommende.

Ved at implementere disse kontroller sikrer den dataansvarlige, at personoplysningerne behandles korrekt og i overensstemmelse med gældende lovgivning, hvilket er afgørende for at opretholde databehandlerens og den dataansvarliges fælles forpligtelser over for de registrerede og myndighederne.

3. Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger

Til ledelsen hos Det Danske Madhus A/S og deres kunder

Omfang
Vi har fået som opgave at afgive erklæring om Det Danske Madhus A/S' beskrivelse i afsnit 2 af ydelse til behandling af personoplysninger i henhold til databehandleraftaler med dataansvarlige, i hele perioden 11. juni 2023 – 30. juni 2024 (beskrivelsen) og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter kontrolmål og tilknyttede kontroller hos Det Danske Madhus A/S' underleverandører og underdatabehandlere. Brugen af underleverandører er nærmere oplistet i databehandleraftaler med kunderne.

Det Danske Madhus A/S' ansvar
Det Danske Madhus A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at 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, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Inforevision 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 Det Danske Madhus A/S' beskrivelse samt om udformningen 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* og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin ydelse samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af 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 funktionaliteten 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 mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i afsnit 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
Det Danske Madhus A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved ydelsen, 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 funktionaliteten 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 ledelsens udtalelse i afsnit 1. Det er vores opfattelse,

(a) at beskrivelsen af ydelsen, således som denne var udformet og implementeret i hele perioden fra 11. juni 2023 til 30. juni 2024, i alle væsentlige henseender er retvisende, og
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 11. juni 2023 til 30. juni 2024,
(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 fungeret effektivt i hele perioden fra 11. juni 2023 til 30. juni 2024.

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

Tiltænkte brugere og formål
Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Det Danske Madhus A/S' ydelse, 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.

Søborg, 30. august 2024

inforevision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
statsautoriseret revisor

Simon Okkels
Partner, Lead IT-auditor (CISA)

4. Kontrolmål, kontrolaktiviteter, test og resultat heraf

4.1 Formål og omfang

Vores arbejde er udført i overensstemmelse med ISAE 3000, *Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger.*

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Det Danske Madhus A/S har implementeret. Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, som vi har vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i hele perioden fra 11. juni 2023 til 30. juni 2024.

Denne erklæring er afgivet efter den partielle metode, og omfatter ikke kontrolmål og tilknyttede kontroller hos Det Danske Madhus A/S' underleverandører og underdatabehandlere.

Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Det Danske Madhus A/S' kunder er ikke omfattet af vores testhandlinger.

4.2 Udførte testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrolaktiviteternes funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel til passende personale hos virksomheden er udført for alle væsentlige kontrolaktiviteter. Forespørgsler er udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres. Endvidere for at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation, som indeholder information om udførelse af kontrollen. Det omfatter gennemlæsning 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.
Observation	Observation af kontrollens udførelse.
Genudførelse af kontrol	Den relevante kontrol er genudført med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores test af de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Kontrolmål A (Instruks)

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A1	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 n 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.	Vi har ikke konstateret afvigelser.
A2	Databehandler 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 via stikprøver på behandling af personoplysninger, at disse foregår i overensstemmelse med instruks.	Vi har ikke konstateret afvigelser.
A3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	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 den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vi har observeret, at der ikke er en formaliseret procedure for intern håndtering af ulovlige instrukser. Vi har fået oplyst, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. Ingen yderligere afvigelser fundet.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B1	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. Inspiceret via stikprøver på indgåede databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Vi har konstateret, at Det Danske Madhus' procedurer og kontroller for sikring af stærke adgangskoder ikke har fungeret effektivt frem til 4/10 2023. Den 4/10 2023 har selskabet forbedret kontrollerne på området, og kontrollerne har fungeret effektivt i den resterende del af erklæringsperioden. Vi har konstateret at virksomhedens procedure for at ajourføre interne procedurer, så de stemmer overens med kravene i databehandleraftaler, ikke i alle tilfælde er udført Ingen yderligere afvigelser fundet.
B2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler 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 databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser fundet.
B3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Vi har ikke konstateret afvigelser.
B5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Vi har ikke konstateret afvigelser.
B6	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 via stikprøver på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Vi har ikke konstateret afvigelser.
B7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at der via stikprøver på alarmer er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Vi er blevet oplyst om at der ikke har været rapporteret om ukrypterede transmission af personfølsomme data i erklæringsperioden. Vi har ikke konstateret afvigelser.
B9	Der er etableret logning i systemer, databaser og netværk. F.eks.: - aktiviteter udført af administratorer, - sikkerhedshændelser som ændringer i log indstillinger, - deaktivering af logning, - ændringer i brugerrettigheder, - fejlede loginforsøg. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Vi er blevet oplyst at logs for netværk ikke opsamles og at logs for perioden ikke kan dokumenteres da de er overskrevet. Vi har på den baggrund ikke kunne teste effektiviteten af kontrollen. Vi har ikke konstateret afvigelser.
B11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at evt. afvigelser og	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
		svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	
B12	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 ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Vi har konstateret at user endpoints ikke er blevet opdateret med sikkerhedspatches fyldestgørende i perioden. Ingen yderligere afvigelser fundet.
B13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret via stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret via stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Vi har konstateret at der ikke har været udført brugeradgang-reviews i erklæringsperioden som beskrevet i virksomhedens procedurer. Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Vi har konstateret at et system der indeholder persondata ikke er beskyttet af to-faktor autentificering. Ingen yderligere afvigelser fundet.
B15	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 haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Vi har ikke konstateret afvigelser.

Kontrolmål C (Organisatoriske foranstaltninger)

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

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens 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 inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Vi har ikke konstateret afvigelser.
C2	Databehandlerens 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 via stikprøve på indgåede databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Vi har ikke konstateret afvigelser.
C3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: - Referencer fra tidligere ansættelser, - straffeattest, - eksamensbeviser m.v.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret via stikprøve på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret via stikprøve på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet referencer fra tidligere ansættelser, straffeattest, eksamensbeviser m.v., i relevant omfang.	Vi har ikke konstateret afvigelser.

Kontrolmål C (Organisatoriske foranstaltninger)

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

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C4	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 ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: informationssikkerhedspolitikken, procedurer vedrørende databehandlings, samt anden relevant information.	Vi har ikke konstateret afvigelser.
C5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Vi har ikke konstateret afvigelser.
C6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Vi har ikke konstateret afvigelser.
C7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Vi har ikke konstateret afvigelser.

Kontrolmål D (Sletning og tilbagelevering) Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D1	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.	Vi har ikke konstateret afvigelser.
D2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har fået oplyst, at der ikke har været nogle ophørte databehandleraftaler indenfor det seneste år, hvorfor vi ikke kan teste effektiviteten af kontrollen. Vi er blevet oplyst at der ikke er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Ingen yderligere afvigelser fundet.
D3	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.	Vi har fået oplyst, at der ikke har været nogle ophørte databehandleraftaler indenfor det seneste år, hvorfor vi ikke kan teste effektiviteten af kontrollen. Ingen yderligere afvigelser fundet.

Kontrolmål E (Opbevaring)

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E1	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. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Vi har ikke konstateret afvigelser.
E2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, 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.	Vi har ikke konstateret afvigelser.

Kontrolmål F (Underdatabehandlere)

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.

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Vi har ikke konstateret afvigelser.
F2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Vi har ikke konstateret afvigelser.
F3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.	Vi har fået oplyst, at der ikke har været nogle ophørte underdatabehandleraftaler indenfor det seneste år, hvorfor vi ikke kan teste effektiviteten af kontrollen. Ingen yderligere afvigelser fundet.
F4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har ikke konstateret afvigelser.

Kontrolmål F (Underdatabehandlere)

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.

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: - Navn, - CVR-nr., - Adresse, - beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Vi har ikke konstateret afvigelser.
F6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Vi er blevet oplyst om at tilsyn foretaget af underdatabehandlere i perioden, ikke har resulteret i nogen væsentlige findings, der har afstedkommet et behov for at underrette dataansvarlige. Vi har ikke konstateret afvigelser.

Kontrolmål G (Tredjelandsoverførsler)

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.

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Vi er blevet oplyst om at der ikke er foretaget nogen overførsler af data til tredjelande i perioden. Vi har ikke konstateret afvigelser.
G2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved en stikprøve på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Vi er blevet oplyst om at der ikke er foretaget nogen overførsler af data til tredjelande i perioden. Vi har ikke konstateret afvigelser.
G3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag.	Vi er blevet oplyst om at der ikke for nogle kundeløsninger er aftaler om, at virksomheden må overføre data til tredjelande Vi har ikke konstateret afvigelser.

Kontrolmål H (Registreredes rettigheder)

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

Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren 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 databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.	Vi har ikke konstateret afvigelser.
H2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	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. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Vi har fået oplyst, at der ikke har været udført bistand til dataansvarlig i perioden, og har derfor ikke kunne teste effektiviteten af kontrollen. Vi har ikke konstateret afvigelser.

Kontrolmål I (Sikkerhedsbrud) Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Vi har ikke konstateret afvigelser.
I2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Inspiceret, at databehandler udbyder 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 mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Vi har ikke konstateret afvigelser.
I3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 72 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Vi er blevet oplyst at Det Danske Madhus vurderede at databrud i perioden ikke har krævet involvering af den dataansvarlige Vi har ikke konstateret afvigelser.

Kontrolmål I (Sikkerhedsbrud) Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Det Danske Madhus A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet og tager højde for følgende vigtige elementer: Karakteren af bruddet, sandsynlige konsekvenser af bruddet samt foranstaltninger som er truffet eller foreslås truffet for at håndtere bruddet.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for beskrivelser af: - Karakteren af bruddet, - sandsynlige konsekvenser af bruddet - foranstaltninger som er truffet eller foreslås truffet for at håndtere bruddet. Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Ingen afvigelser fundet.

5. Ledelsens kommentar til ”resultat af revisors test”

Ledelsen har følgende kommentarer til “resultat af revisors test” i kapitel 4.

B1

Resultat af revisors test	Vi har konstateret, at Det Danske Madhus' procedurer og kontroller for sikring af stærke adgangskoder ikke har været tilstrækkelig
Ledelsens kommentarer	Vi har pr. 04.10.23 indført følgende: Stærke adgangskoder er obligatoriske for alle systemer med personhenførbare data og skal ændres hver tredje måned. Adgangskoder skal indeholde mindst 12 tegn, inklusiv store og små bogstaver, tal og specielle tegn. Desuden skal det tilstræbes ikke at anvende almindeligt kendte ord fra ordbogen. Adgangskoder er personlige og skal opbevares forsvarligt. Når IT-udstyr efterlades (også på arbejdspladsen), skal udstyret låses, således at der skal anvendes kode for at få adgang. Det er ikke tilstrækkeligt at forlade sig på automatisk låsning – for at låse ens computer tryk ”WINDOWS TAST” + ”L TAST”

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."

Peter Michael Skotte Tietgen
Direktør
Serienummer: 8c756aa9-36be-4231-aaac-a2cb3caeade4
IP: 194.239.xxx.xxx
2024-08-30 14:30:23 UTC

Søren Stoltenberg Vilmand
CEO
Serienummer: a5b626e3-2135-495c-8ea8-031505883d5b
IP: 94.147.xxx.xxx
2024-09-02 06:41:07 UTC

Simon Okkels
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Partner, Lead IT-auditor (CISA)
Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a
IP: 93.165.xxx.xxx
2024-09-02 11:12:46 UTC

John Richardt Søbjærg
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Statsautoriseret revisor
Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a
IP: 93.165.xxx.xxx
2024-09-02 11:32:21 UTC

Penneo dokumentnøgle: M8SHS-CQNVE-GKSAX-WCYMI-QTPY4-IATVE