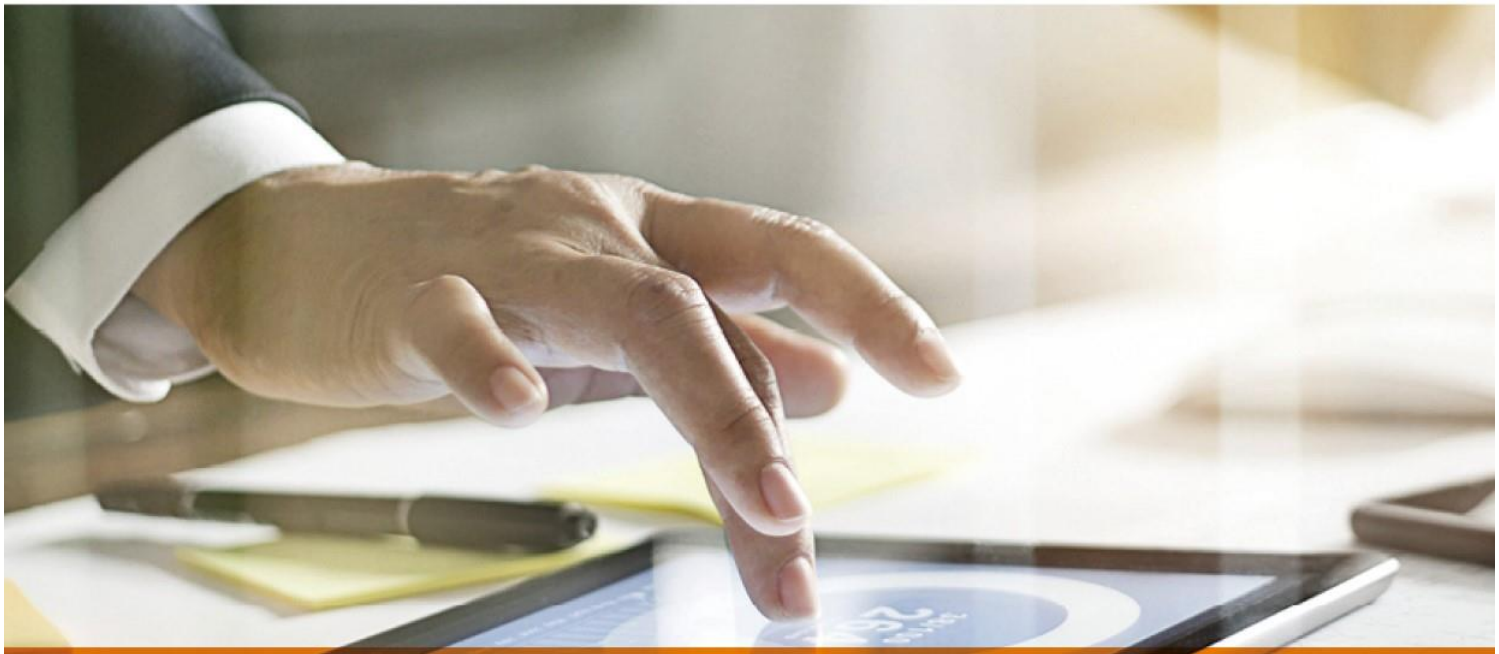
BEIERHOLM
VI SKABER BALANCE



Maj 2023

MCB A/S

ISAE 3000 TYPE 1 ERKLÆRING

CVR 29150966

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med dataansvarlige.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelsens udtalelse.

Kapitel 2:
Uafhængig revisors erklæring.

Kapitel 3:
Beskrivelse af behandling.

Kapitel 4:
Kontrolmål, kontrolaktivitet, test og resultat heraf.

KAPITEL 1:

Ledelseserklæring

MCB A/S behandler personoplysninger på vegne af sine kunder i henhold til databehandleraftalen.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt MCB A/S IT-løsninger, 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 "databeskyttelsesforordningen") er overholdt. MCB A/S bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 3, giver en retvisende beskrivelse af MCB A/S' IT-løsninger, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. den 25. maj 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne 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 kunden dvs. den dataansvarlige
- De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
- De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
- De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede
- De processer, der sikrer passende tekniske og organisatoriske 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 med henvisning til systemets 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
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de anvendte forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Indeholder relevante oplysninger om ændringer ved MCB A/S' IT-løsninger i behandlingen af personoplysninger foretaget pr. den 25. maj 2023.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontroller, som den enkelte kunde måtte anse som vigtigt efter deres særlige forhold.

(B) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. den 25. maj 2023. Kriterierne for dette udsagn er, at:

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

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

(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.

Holstebro, den 1. juni 2023

CEO, Bo Hedegaard
MCB A/S, Lægårdvej 86 B, DK-7500 Holstebro, CVR-nummer: 29150966

KAPITEL 2:

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med MCB A/S' kunder

Til MCB A/S og relevante dataansvarlige

Omfang

Vi har fået som opgave at afgive erklæring om MCB A/S' beskrivelse af IT-løsninger jf. kapitel 3 i henhold til databehandleraftale med MCB A/S' kunder pr. den 25. maj 2023 (beskrivelsen) og om udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

MCB A/S' ansvar

MCB A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse jf. kapitel 3, 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 og implementere kontroller for at opnå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Beierholm er underlagt international standard om kvalitetsstyring, ISQM 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om MCB A/S' beskrivelse samt om udformningen og implementeringen 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 implementeringen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sit system samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet og implementeret.

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 jf. kapitel 3. Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusionen herom.

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

Begrænsninger i kontroller hos MCB A/S

MCB 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 systemet, 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. Det er vores opfattelse,

a) at beskrivelsen af MCB A/S' IT-løsninger, således som de var udformet og implementeret pr. den 25. maj 2023, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. den 25. maj 2023

Beskrivelse af test kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 3 er udelukkende tiltænkt MCB A/S' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Søborg, den 1. juni 2023

Beierholm
Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Allan Nielsen
Seniorkonsulent, IT-Revision

KAPITEL 3:

Indledning

Formålet med nærværende beskrivelse er at levere informationer til MCB A/S' kunder og deres revisorer vedrørende kravene i ISAE 3000. Det er den internationale revisorstandard for andre erklæringsopgaver med sikkerhed herunder informationssikkerhed og foranstaltninger i henhold til databehandleraftalen med dataansvarlige.

Denne kontrolbeskrivelse afdækker de tekniske og organisatoriske sikkerhedsforanstaltninger, der er implementeret i tilknytningen til udviklingen og driften af MCB's IT-løsninger.

Beskrivelse af MCB A/S

MCB er et digitalt konsulenthus, der er specialiseret i at hjælpe samarbejdspartnere til succes online.

Vi tror på, at vi via en bred forretningsforståelse, viden om data og et tillidsfuldt samarbejde kan sikre høj værdi, der afspejles på både top- og bundlinje. Derfor vil vores services altid være en god investering.

Vi sørger for at være tæt på din forretning, at være proaktive og at udfordre dig på dine strategier, tanker og ideer. På den måde hjælper vi med at realisere dit potentiale baseret på mange års hands-on erfaring fra branchen.

Vi leverer markedets bedste, cloudbaserede e-handels- og webløsninger til både B2B og B2C inden for en lang række platforme herunder vores egen gennemtestede e-commerce platform, Cloud. Vores specialistområder tæller også Umbraco, Magento, HubSpot, Shopify, Shopware, integrationer og meget andet. Derudover har vi vores egen marketingafdeling, der dagligt arbejder med alt fra tracking, Google Ads og sociale medier til e-mail marketing, SEO og video.

Vi er derfor meget mere end bare en leverandør. MCB vil være din tætte samarbejdspartner og din ekstra kollega.

Beskrivelse af behandlingens karakter

Formålet med behandlingen af personoplysninger er overordnet at behandle og eksekvere købsordrer fra kundens kunder. Som tillæg hertil kan der være indgået aftale om udførelse af online marketingaktiviteter på vegne af kunden.

Karakteren af behandlingen

MCB har adgang til følgende kategorier af personoplysninger (herefter benævnt 'Personoplysninger'):

- Særlige kategorier af personoplysninger: Fx fagforeningsmæssige tilhørsforhold
- Generelle kategorier af personoplysninger: Herunder navn, telefonnummer, postadresse, fødselsdato, kontonummer m.v.
- Købsadfærd: Herunder fx betalingsoplysninger, købsoplysninger, købsstatistik, transaktioner m.v.

MCB's adgang til personoplysninger ved den Dataansvarlige sker ved følgende formål: Konsulentbistand til udvikling og drift af 3. parts systemer samt digital markedsføring.

Personoplysninger, som behandles:

- Almindelige personoplysninger herunder identifikationsoplysninger som navn og adresse eller oplysninger om økonomi, skat, gæld, væsentlige sociale problemer, andre private forhold, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato og -stilling, arbejdsområde og arbejdstelefon.
- Særlige kategorier af personoplysninger herunder race og etnisk oprindelse, politisk overbevisning, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data med henblik på entydig identifikation, helbredsoplysninger, seksuelle forhold eller seksuel orientering.
- Andre personlige oplysninger herunder oplysninger om strafbare forhold og cpr-numre.

Risikostyring i MCB A/S

Det er MCB's politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde en normal drift.

MCB har indarbejdet faste procedurer for risikovurdering af forretningen. Det sikres dermed, at de risici, som er forbundet med de services, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når der ændres i eksisterende systemer eller implementeres nye systemer. Risikovurderingen er en del af den IT-sikkerhedsansvarliges ansvar og skal efterfølgende forankres og godkendes hos virksomhedens ledelse.

Kontrolmål

I forbindelse med MCB's rolle som databehandler, har MCB implementeret procedurer og kontroller til at sikre overholdelse af GDPR og databehandleraftalen. MCB har defineret procedurer og kontroller inden for nedenstående kontrolmål.

Kontrolmål A

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

MCB har implementeret formelle procedurer for kontraktindgåelse, der sikrer, at databehandleraftaler udarbejdes og kontrolleres med henblik på at sikre aftalens lovlighed.

MCB anvender ISO27001+2, som rammeværk for styring af informationssikkerheden. Det betyder, at MCB har et integreret ledelsessystem, der stiller krav til, hvordan MCB:

- Gennem en risikobaseret tilgang beskytter de informationer og data, hvor der enten ageres databehandler eller dataansvarlig
- Udfører interne og eksterne kontroller af informationssikkerheden
- Årligt evaluerer procedurer, mål, politikker, kontroller og sikkerhedsforanstaltninger i forhold til informationssikkerhed

Kontrolmål B

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

MCB har på implementeret nedenstående tekniske foranstaltninger:

1. Malwarebeskyttelse, Firewall og netværk
   Arbejdsmaskiner og servere er udstyret med antivirussoftware, hvor dette er hensigtsmæssigt med henblik på at blokere vira, malware m.v. Alternativt sikkerhedsopdateres disse løbende.
   Netværket er placeret bag Firewalls for at beskytte netværket mod uautoriseret adgang.

2. Kryptering
   Der er etableret kryptering (hashing), hvor dette er en del af aftalen. Herunder passwords til systemerne.

3. Adgangsstyring og brugerstyring
   Medarbejdere hos Databehandleren har alene adgang til de systemer, der er relevante for den enkelte medarbejder. Der anvendes om 2-faktor autentifikation hvor dette er muligt, som minimum på brugere med privilegerede rettigheder.

   Alle ansatte har unikke brugernavne og passwords. Brugernavne og passwords oprettes og ændres efter alment anerkendte principper. Der foretages registrering af alle afviste adgangsforsøg. Efter gentagne afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, blokeres der for yderligere forsøg.

4. Logning
   Der sker logning af alle tilgange til tjenesterne. Logning registrerer tidspunktet, en medarbejder tilgår tjenesterne samt varigheden af tilgangen. Loggen gemmes i min. 6 måneder.

5. Fysisk adgangssikring
   Der er beskyttet med sædvanlige indbruds- og tyverialarmer. Det er udelukkende relevante personer, der har adgang til Databehandlerens faciliteter, og der er fysisk adgangskontrol til alle lokationer.

Kontrolmål C

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

MCB har implementeret kontroller fra ISO27001 Informationssikkerhed, Anneks A. Herunder kontrollerne:

A.5 Informationssikkerhedspolitikker
5.1.1 Politikker for informationssikkerhed
5.1.2 Gennemgang af politikker for informationssikkerhed

A.7 Personalesikkerhed
7.1 Før ansættelsen
7.1.1 Screening
7.1.2 Ansættelsesvilkår og -betingelser
7.2 Under ansættelsen
7.2.1 Ledelsesansvar
7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed
7.2.3 Sanktioner
7.3 Ansættelsesforholdets ophør eller ændring
7.3.1 Ansættelsesforholdets ophør eller ændring

I forbindelse med ansættelse ved MCB gennemgår kandidaterne 3 samtaler med Team leads og ledere. Mellem samtale 1 og 2 tages referencer på den kommende medarbejder, hvor CV konfirmeres, og eventuelle spørgsmål til arbejdsområde afklares. I forbindelse med indgåelse af kontrakt underskriver medarbejderen at være oplyst om, at de arbejdes under tavshedspligt.

Ved fratrædelse fra MCB, har den nærmeste leder ansvar for at gennemføre proceduren for fratrædelse I denne tjekliste – fremgår det også at nærmeste leder, skal gøre medarbejderen opmærksom på at tavshedspligten forsat gælder efter endt ansættelse. Efter endt ansættelsen, nedlæggelse brugeren og dens eksterne adgange i henhold til MCB slette og opbevaringspolitik og procedure for privilegerede brugere.

Kontrolmål D

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

MCB har en Slettepolitik, som har til hensigt:

1. At vejlede for at sikre, at personoplysninger opbevares og beskyttes hos MCB A/S i hele personoplysningernes opbevaringsperiode.
2. At gøre personoplysningerne mere tilgængelige og brugbare for medarbejdere hos MCB A/S.
3. At sikre, at der sker afvigelse fra standardopbevaringsperioden for personoplysninger, når der skal ske fastfrysning af personoplysninger.
4. At etablere passende praksis for sletning og bortskaffelse af personoplysninger.

MCB har udpeget en ansvarlig for Slettepolitikken, hvis ansvar er at sikre korrekt opbevaring og sletning af data samt førelse af kontrol med de implementerede procedurer.

A.5 Informationssikkerhedspolitikker
5.1.1 Politikker for informationssikkerhed
5.1.2 Gennemgang af politikker for informationssikkerhed

A.8 Styring af aktiver
8.1.1. Ansvar for aktiver – Identifikation
8.1.2. Ansvar for aktiver – Ejer
8.1.3. Ansvar for aktiver – Regler for brug
8.1.4. Ansvar for aktiver – Tilbagelevering ved nedlukning
8.2.1. Klassifikation af information - Klassificering
8.2.2. Klassifikation af information – Procedure
8.2.3. Klassifikation af information – System
8.3.1. Mediehåndtering - Procedure
8.3.2. Mediehåndtering – Bortskaffelse
8.3.3. Mediehåndtering – Beskyttelse / Bortskaffelse

Kontrolmål E

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

MCB har via sin IT-sikkerhedspolitik, Databehandleraftaler med sine kunder og underdatabehandleraftaler med sine leverandører sikret, at det kun er tilladt at arbejde efter instruks, at denne dokumenteres via intern timesagsstyring og alene nødvendig personlig information opsamles i henhold til de behandlingskrav, som kunderne har redegjort for i deres underdatabehandleraftale.

A.5 Informationssikkerhedspolitikker
5.1.1 Politikker for informationssikkerhed
5.1.2 Gennemgang af politikker for informationssikkerhed

A.8 Styring af aktiver
8.1.1. Ansvar for aktiver – Identifikation

8.1.2. Ansvar for aktiver – Ejer
8.1.3. Ansvar for aktiver – Regler for brug
8.1.4. Ansvar for aktiver – Tilbagelevering ved nedlukning
8.2.1. Klassifikation af information - Klassificering
8.2.2. Klassifikation af information – Procedure
8.2.3. Klassifikation af information – System
8.3.1. Mediehåndtering - Procedure
8.3.2. Mediehåndtering – Bortskaffelse
8.3.3. Mediehåndtering – Beskyttelse / Bortskaffelse

A.15 Informationssikkerhed i leverandørforhold
15.1.1. Informationssikkerhed i leverandørforhold – Brug af underdatabehandler
15.1.2. Informationssikkerhed i leverandørforhold – Krav til underdatabehandler
15.1.3. Informationssikkerhed i leverandørforhold – Aftalegrundlag
15.2.1. Styring af leverandørydelser – Auditerer
15.2.2. Styring af leverandørydelser - Ændringer af leverandørydelser.

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

MCB har via samhandels- og underdatabehandleraftaler sikret, at leverandører til MCB som minimum opfylder de af MCB definerede krav til håndtering og dokumentation af Informationssikkerhed. Kritiske leverandører, som behandler eller opbevarer personhenførbar data auditeres én gang årligt. Enten via fremsendelse af en ekstern auditrapport i form af ISEA3000, SOC2 eller en anden anerkendt standard for ekstern audit. Alternativt gennemføres audit via fremsendelse af udvidet kontrolspørgeskema med en efterfølgende opfølgning.

A.15 Informationssikkerhed i leverandørforhold
15.1.1. Informationssikkerhed i leverandørforhold – Brug af underdatabehandler
15.1.2. Informationssikkerhed i leverandørforhold – Krav til underdatabehandler
15.1.3. Informationssikkerhed i leverandørforhold – Aftalegrundlag
15.2.1. Styring af leverandørydelser – Auditerer
15.2.2. Styring af leverandørydelser - Ændringer af leverandørydelser.

Kontrolmål G

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.

MCB har via følgende tiltag indført tekniske begrænsninger, der forhindrer vores medarbejdere i tredjelande i at kunne tilgå PI (Personlig Information):

- MCB.Cloud's SQL database har indført data scramling for alle ikke EU medarbejdere på alle PI felter.
- Medarbejdere uden for EU har ikke adgang til MCB.Cloud Management og kan hverken se eller ændre på sites, hvor det er indført, at kunden har sat krav om, at overførelser til tredjelande ikke må forefindes.
- Alt kommunikation og dataudveksling mellem MCB's enheder køre via krypterede linjer og forgår via opsat VPN tunnel.

Udover de tekniske foranstaltninger har MCB indgået SCC (Standardkontraktklausuler) med MCB VN (datterselskab), som muliggør, at de af EU påførte retsmæssige påbud kan håndhæves i tredjeland. Dette benyttes ved de af MCB's kunder, som køber service og ydelser til supportering af deres løsning, når disse sager efter instruks fra kunden kræver adgang til PI data for at kunne fejlsøge og udbedres.

Alle medarbejdere i MCB og dennes datterselskaber er underlagt MCB's IT-sikkerhedspolitik og de samme krav til træning og kontrol, som medarbejdere i MCB A/S.

A.5 Informationssikkerhedspolitikker
5.1.1 Politikker for informationssikkerhed
5.1.2 Gennemgang af politikker for informationssikkerhed

A.14 Anskaffelse, udvikling og vedligeholdelse
14.2.7. Sikkerhed i udviklings- og hjælpeprocesser – Outsource

A.15 Leverandørforhold
15.1.1. Informationssikkerhed i leverandørforhold – Risikostyring
15.1.2. Informationssikkerhed i leverandørforhold – Aftalegrundlag
15.1.3. Informationssikkerhed i leverandørforhold – Krav og risiko

A.18 Overensstemmelse
18.1.1. Overensstemmelse med lov- og kontraktkrav - Relevante lov-, myndigheds- og kontraktkrav
18.1.2. Overensstemmelse med lov- og kontraktkrav - Procedure
18.1.3. Overensstemmelse med lov- og kontraktkrav - Kontinuitet/Back-up
18.1.4. Overensstemmelse med lov- og kontraktkrav - Privatlivets fred
18.2.1. Gennemgang af informationssikkerhed - Organisationens styring af information sikkerhed
18.2.2. Gennemgang af informationssikkerhed - Lederne auditering
18.2.3. Gennemgang af informationssikkerhed – Auditering af systemer

Kontrolmål H

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

MCB skal så vidt muligt bistå den Dataansvarlige med opfyldelse af den Dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder, herunder om indsigt, berigtigelse, begrænsning eller sletning, hvis de relevante personoplysninger behandles af Databehandleren. Modtager Databehandleren sådan henvendelse fra den registrerede, orienterer Databehandleren den Dataansvarlige herom.

A.16 Styring af informationssikkerhedsbrud og forbedringer
16.1.3. Styring af informationssikkerhedsbrud – Indrapportering, medarbejdere og kontrahenter
16.1.4. Styring af informationssikkerhedsbrud - Informationssikkerhedshændelser skal vurderes
16.1.5. Styring af Informationssikkerhedsbrud – Håndtering af hændelser
16.1.6. Styring af Informationssikkerhedsbrud – Analyse og root cause
16.1.7. Styring af Informationssikkerhedsbrud – Informationsopsamling og forbedring

A.18 Overensstemmelse
18.1.1. Overensstemmelse med lov- og kontraktkrav - Relevante lov-, myndigheds- og kontraktkrav
18.1.2. Overensstemmelse med lov- og kontraktkrav - Procedure
18.1.3. Overensstemmelse med lov- og kontraktkrav - Kontinuitet/Back-up
18.1.4. Overensstemmelse med lov- og kontraktkrav - Privatlivets fred

18.2.1. Gennemgang af informationssikkerhed - Organisationens styring af information sikkerhed
18.2.2. Gennemgang af informationssikkerhed - Lederne auditering
18.2.3. Gennemgang af informationssikkerhed – Auditering af systemer.

Kontrolmål I

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

MCB bistår alle henvendelser fra dataansvarlige, eller andre kilder hvor der opstår mistanke om datatab, eller databrud – herunder tab af personhenførbare informationer. Som udgangspunktet starter alle henvendelse ved MCB´s support team, som herefter eskalerer sagen.

Hvis en supporthændelse markeres som en sikkerhedshændelse, orienteres MCB sikkerhedsgruppe, og proceduren for undersøgelse og klassificering påbegyndes. Ved klassificering som en sikkerhedshændelse, orienteres de berørte kunder straks, og MCB bistår den dataansvarlige med dokumentation og omfangsbeskrivelse.

A.5 Informationssikkerhedspolitikker
5.1.1 Politikker for informationssikkerhed
5.1.2 Gennemgang af politikker for informationssikkerhed

A.16 Styring af informationssikkerhedsbrud og forbedringer
16.1.1. Styring af informationssikkerhedsbrud og forbedringer - Ledelsesansvar
16.1.2. Styring af informationssikkerhedsbrud og forbedringer - Informationssikkerhedshændelser
16.1.3. Styring af informationssikkerhedsbrud – Indrapportering, medarbejdere og kontrahenter
16.1.4. Styring af informationssikkerhedsbrud - Informationssikkerhedshændelser skal vurderes
16.1.5. Styring af Informationssikkerhedsbrud – Håndtering af hændelser
16.1.6. Styring af Informationssikkerhedsbrud – Analyse og root cause
16.1.7. Styring af Informationssikkerhedsbrud – Informationsopsamling og forbedring

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

KONTROLMÅL A:

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

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandleren 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL B:

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

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL B:

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

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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 ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Front-end (MCB) – 2 test over 30 Sek uden svar = Trigger til Alarm. • Operation er omfattet af SLA ved Lynero (DLX)	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL B:

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

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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 på erklæringstidspunktet. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret logning i systemer, databaser og netværk af følende forhold: • Sikkerhedshændelser omfattende: ○ Ændringer i logopsætninger, herunder deaktivering af logning ○ Ændringer i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	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 har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL B:

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

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.		
MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret yderligere afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL C:

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

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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 ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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, at der foreligger formaliserede procedurer, der sikrer at medarbejdere underskriver en fortrolighedsaftale ved ansættelse og bliver introduceret til informationssikkerhedspolitikken såvel som procedurerne vedrørende databehandling samt anden relevant information.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL C:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.		
MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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 fortrolighed-saftalen og generel tavshedspligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL D:

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Indtil aftalen opsiges	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 60 dage efter de aftalens ophør	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL E:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.		
MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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 ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL G:

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.

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL H:

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

MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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 ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL I:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.		
MCB A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af tilgang til personoplysninger	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 ved vores test konstateret væsentlige afvigelser.
Databehandleren 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 databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at 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	Vi har ikke ved vores test konstateret væsentlige afvigelser.