
cBrain A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2020 til 31. december 2020 i henhold til databehandlersaftale med dataansvarlige der anvender systemerne F2 og M4

februar 2021

Indholdsfortegnelse

1. Ledelsens udtalelse	3
2. Uafhængig revisors erklæring	5
3. Beskrivelse af behandling.....	7
4. Kontrolmål, kontrolaktivitet, test og resultat heraf	10

1. Ledelsens udtalelse

cBrain behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftale.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt systemerne F2 og M4, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den 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" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne") er overholdt.

cBrain bekræfter, at:

- a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af behandling af persondata i relation til systemerne F2 og M4, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne i hele perioden fra 1. januar 2020 – 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
 - (i) Redegør for, hvordan behandling af persondata i relation til systemerne F2 og M4 var udformet og implementeret, herunder redegør for:
 - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
 - De processer i både it-systemer og 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 underretning af de registrerede
 - De processer, der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
 - Kontroller, som vi med henvisning til behandling af persondata i relation til systemerne F2 og M4s afgrænsning har forudsat ville være implementeret af den 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 i databehandlerens behandling af persondata i relation til systemerne F2 og M4 foretaget i perioden fra 1. januar 2020 – 31. december 2020
 - (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne behandling af persondata i relation til systemerne F2 og M4 til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved behandling af persondata i relation til systemerne F2 og M4, som den enkelte dataansvarlige måtte anse vigtigt efter sine 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 fra 1. januar 2020 – 31. december 2020. 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 1. januar 2020 – 31. december 2020.
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandleretik og relevante krav til databehandlere i henhold til databeskyttelsesreglerne.

København den 2. februar 2021
cBrain A/S



Robert Lentz
Direktør/COO

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2020 til 31. december 2020 i henhold til databehandlersaftale med dataansvarlige der anvender systemerne F2 og M4

Til: cBrain og dataansvarlige der anvender systemerne F2 og M4

Omfang

Vi har fået som opgave at afgive erklæring om cBrains beskrivelse i afsnit 3 af deres behandling af persondata i relation til systemerne F2 og M4 i henhold til databehandlersaftale med dataansvarlige i hele perioden fra 1. januar 2020 – 31. december 2020 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om cBrain har udformet og effektivt udført hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4. Erklæringen omfatter ikke en vurdering af cBrains generelle efterlevelse af kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne").

Vores konklusion udtrykkes med høj grad af sikkerhed.

cBrains ansvar

cBrain 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 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 FSR – danske revisors retningslinjer for revisors etiske adfærd (Ethiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 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 cBrain s beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gældende i Danmark, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at 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 deres behandling af persondata i relation til systemerne F2 og M4 samt for kontrollerens 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 ledelsens udtalelse.

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

Begrænsninger i kontroller hos en databehandler

cBrains beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved behandling af persondata i relation til systemerne F2 og M4, som hver enkelt dataansvarlig måtte anse for vigtige efter sine 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 behandling af persondata i relation til systemerne F2 og M4, således som det var udformet og implementeret i hele perioden fra 1. januar 2020 – 31. december 2020, 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 1. januar 2020 – 31. december 2020, og
- c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2020 – 31. december 2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test 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 cBrains systemer F2 og M4, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af om kravene i databeskyttelsesreglerne er overholdt.

København, den 2. februar 2021

PricewaterhouseCoopers

Statsautoriseret Revisionspartnerselskab



Michael Clement
statsautoriseret revisor

3. *Beskrivelse af behandling*

cBrain A/S er leverandør af en lang række ydelser relateret til digitalisering af arbejdsgange og kommunikation til offentlige myndigheder og private organisationer. Kunder er placeret i Danmark og internationalt.

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

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

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

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

cBrain er leverandør af drift:

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

cBrain er leverandør af support:

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

cBrain leverer ad hoc-opgaver:

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

- konvertering af data
- opgradering
- aflevering til Rigsarkivet
- import og eksport af data
- flytning af database
- opdatering af database

Typen af data

Karakteren af det programmel, som cBrain leverer betyder, at typen af data, som kunderne lægger i systemet, kan have karakteren af følsomme personoplysninger. Det er således generelt for cBrains håndtering af persondataaftaler, at der er tale om programmel, hvor kundens dataansvarlig har med personfølsomme oplysninger at gøre.

Typen af personoplysninger som omfattes dækker eksempelvis:

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

Kategorier af registrerede personer omfattet af databehandleraftalen er:

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

Praktiske tiltag

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

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

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

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

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

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

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

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

Sentia leverer de fysiske rammer for hostingen, mens cBrain ejer og administrerer hardware og software inklusive basis software, databaser m.m. Kun cBrain-medarbejdere har adgang til cBrains servere på Sentias lokationer i Danmark. Kunders data inklusive backup er placeret i Danmark. Sentias administrative personale har ikke adgang til at forbinde til cBrains servere. Af supporthensyn for maksimal opetid og evt. fejlfinding har Sentia dog administrative rettigheder til firewall i Taastrup.

Gennem ejerskabet af servere m.m., som både er placeret hos Sentia og i cBrains kontorlokaler kan cBrain sikre, at personer fra sikre/usikre tredjelande eller internationale organisationer ikke har adgang til at behandle data eksempelvis via support (herunder "se-adgang").

På cBrains kontorlokaler på Dampfærgevej kræves der adgangskort samt kode for at tilgå serverlokalet. Adgang til kontorlokalerne kræver adgangskort i dagtimerne og adgangskort og kode uden for normale åbningstid.

De generelle aftaler omkring behandling af data og instrukser er anført i databehandleraftalen, men herudover har cBrain indført en yderligere angivelse af instruks for de ad hoc-opgaver, som udføres. Dermed bliver de relevante medarbejder hos kunden og hos cBrain opmærksom på instruksen, der relaterer sig til opgaven.

Risikovurdering

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

cBrains ledelse har kvartalsvis Management Review møder, som bl.a. behandler compliance i forhold til ISO og ISAE. De seneste møder har bl.a. behandlet forhold omkring håndtering af Covid-19 pandemien. Analyse og vurdering af eventuelle konsekvenser har både inkluderet behovet for en løbende kommunikation til medarbejdere, vurdering af fortsat opretholdelse af vigtige ressourceforhold og behov for ændringer til sikkerhed for udstyr der nu i højere grad anvendes på hjemmearbejdspladser. Den daglige drift af kunders IT-systemer og applikationer, samt det tilhørende kontrol-miljø har ikke være påvirket af Covid-19 pandemien.

Kontrolforanstaltninger

Der er indført en lang række kontrolforanstaltninger, som til dels er anbefalet i forhold til ISAE 3000-aktiviteter målrettet beskyttelse af persondata og i forhold til ISO 27001 aktiviteter. Kontrolforanstaltninger bliver løbende justeret og revideret i forhold til risikovurderinger, ændringer i markedsforhold og lovgivningen generelt.

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

Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige har følgende forpligtelser:

- at sikre sig, at instruksen er lovlige set i forhold til den til enhver tid gældende persondataretlige regulering,
- at instruksen er hensigtsmæssig i forhold til databehandleraftale og ydelsen
- at sikre sig, at den dataansvarliges brugere er ajourførte,
- at sikre sig, at adgangsforhold lever op til markedsstandarder for sikker adgang, herunder egne brugers adgang til data.
- at sikre sig, at dataansvarlige lever op til det ansvar, som er angivet i databehandleraftalen herunder advisering ved tilfælde af brud på datasikkerheden.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
A.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	<p>Inspiceret, at ledelsen sikrer, at behandlingen af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret ved stikprøve på behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
A.3	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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.</p> <p>Inspiceret, at den dataansvarlige er underrettet, i tilfælde hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.</p>	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 behandlings-sikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved stikprøve på databehandleraftaler, at der er etableret de aftalte sikkerhedsforanstaltninger.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
B.2	<p>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 sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandleren foretager en risikovurdering for at opnå en passende sikkerhed.</p> <p>Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Inspiceret, at databehandleren har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
B.3	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.</p>	<p>Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware.</p> <p>Inspiceret, at antivirussoftware er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
B.4	<p>Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.</p>	<p>Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.</p> <p>Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.5	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 konstateret, at cBrain på baggrund af en risikoanalyse, ikke har etableret segmentering af det interne netværk. Vi har ikke ved vores test konstateret andre væsentlige afvigelser.
B.6	Adgang til personoplysninger er isoleret til brugere med et 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 brugernes 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 ved stikprøve på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.7	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.	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 behandlings-sikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	<p>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.</p> <p>Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden.</p> <p>Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.</p> <p>Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.</p>	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.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> • brugeraktiviteter og • ændringer i brugere og rettigheder. <p>Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.</p>	<p>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.</p> <p>Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.</p> <p>Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.</p> <p>Inspiceret ved stikprøve på logning, at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser.</p> <p>Inspiceret ved stikprøve på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder</p>	<p>Vi har konstateret, at der ikke i hele 2020, har været opsat fyldestgørende logning på produktionsservere.</p> <p>Vi har endvidere konstateret at der ikke er opsat fyldestgørende intern beskyttelse af logoplysninger indsamlet fra produktionsservere.</p> <p>Vi har ikke ved vores test konstateret andre væsentlige afvigelser.</p>
B.10	<p>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.</p>	<p>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.</p> <p>Inspiceret ved stikprøve på udviklings- og testdatabaser, at personoplysningerne heri er pseudonymiseret eller anonymiseret.</p> <p>Inspiceret ved stikprøve på udviklings- og testdatabaser, hvor personoplysningerne ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrations-tests.	<p>Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests.</p> <p>Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.</p> <p>Inspiceret, at eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt til de dataansvarlige i behørigt omfang.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	<p>Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.</p> <p>Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.</p>	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.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, herunder om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	<p>Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Inspiceret ved stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.</p> <p>Inspiceret ved stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.</p> <p>Inspiceret, at der foreligger dokumentation for en regelmæssig – mindst årlig – vurdering og godkendelse af tildelte brugeradgange.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede, sker som minimum ved anvendelse af tofaktorautentifikation.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede.</p> <p>Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	<p>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.</p> <p>Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.</p>	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.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.1	<p>Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.</p>	<p>Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
C.2	<p>Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.</p>	<p>Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.</p> <p>Inspiceret ved stikprøve på databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
C.3	<p>Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang:</p> <ul style="list-style-type: none"> • Referencer fra tidligere ansættelser • Eksamensbeviser 	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.</p> <p>Inspiceret ved stikprøve på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning.</p> <p>Inspiceret ved stikprøve på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet:</p> <ul style="list-style-type: none"> • Referencer fra tidligere ansættelser • Eksamensbeviser 	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.4	Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver medarbejderne introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejdernes behandling af personoplysninger.	<p>Inspiceret ved stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale.</p> <p>Inspiceret ved stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til:</p> <ul style="list-style-type: none"> • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information. 	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	<p>Inspiceret procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelsen, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages.</p> <p>Inspiceret ved stikprøve på fratrådte medarbejdere i erklæringsperioden, at rettighederne er inaktiveret eller ophørt, samt at aktiverne er inddraget.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, som databehandleren udfører for de dataansvarlige.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.</p> <p>Inspiceret ved stikprøve på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftalen og generel tavshedspligt.</p>	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.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.7	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 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.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
D.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
D.2	<p>Der aftales specifikke krav til databehandlerens opbevaringsperiode og sletterrutiner med den dataansvarlige.</p>	<p>Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterrutiner.</p> <p>Inspiceret ved stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.</p> <p>Inspiceret ved stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysningerne er slettet i overensstemmelse med de aftalte sletterrutiner.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
D.3	<p>Ved ophør af behandlingen af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:</p> <ul style="list-style-type: none"> • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning. 	<p>Inspiceret, at der foreligger formaliserede procedurer for behandlingen af den dataansvarliges data ved ophør af behandlingen af personoplysninger.</p> <p>Inspiceret ved stikprøve på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål E:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
E.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
E.2	<p>Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.</p>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.</p> <p>Inspiceret ved 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.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål F:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.1	<p>Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi er ved interview oplyst, at der ikke anvendes underdatabehandlere.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
F.2	<p>Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.</p>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere.</p> <p>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.</p>	<p>Vi er ved interview oplyst, at der ikke anvendes underdatabehandlere.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
F.3	<p>Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelsen af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelsen af underdatabehandlere.</p> <p>Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændringer i anvendelsen af underdatabehandlerne i erklæringsperioden.</p>	<p>Vi er ved interview oplyst, at der ikke anvendes underdatabehandlere.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
F.4	<p>Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.</p>	<p>Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.</p> <p>Inspiceret ved stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.</p>	<p>Vi er ved interview oplyst, at der ikke anvendes underdatabehandlere.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål F:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.5	<p>Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af:</p> <ul style="list-style-type: none"> • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen. 	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.</p> <p>Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.</p>	<p>Vi er ved interview oplyst, at der ikke anvendes underdatabehandlere.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
F.6	<p>På baggrund af en ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, foretager databehandleren en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.</p> <p>Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.</p> <p>Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelandes overførselsgrundlag og lignende.</p> <p>Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.</p>	<p>Vi er ved interview oplyst, at der ikke anvendes underdatabehandlere.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

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.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
G.1	<p>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.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>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.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
G.2	<p>Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.</p>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.</p> <p>Inspiceret ved 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.</p>	<p>Vi er ved interview oplyst, at der ikke er foretaget overførelser af denne type.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
G.3	<p>Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved stikprøve på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.</p>	<p>Vi er ved interview oplyst, at der ikke er foretaget overførelser af denne type.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

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.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
H.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
H.2	<p>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.</p>	<p>Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. <p>Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> • Awareness hos medarbejdere 	<p>Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
I.3	<p>Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.</p>	<p>Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p> <p>Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden</p> <p>Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.</p>	<p>Vi er ved interview blevet oplyst, at der ikke har været nogle brud i perioden, og yderligere test har derfor ikke været mulig.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Disse procedurer skal indeholde anvisninger på beskrivelser af:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede anvisninger på:</p> <ul style="list-style-type: none"> • 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. <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>