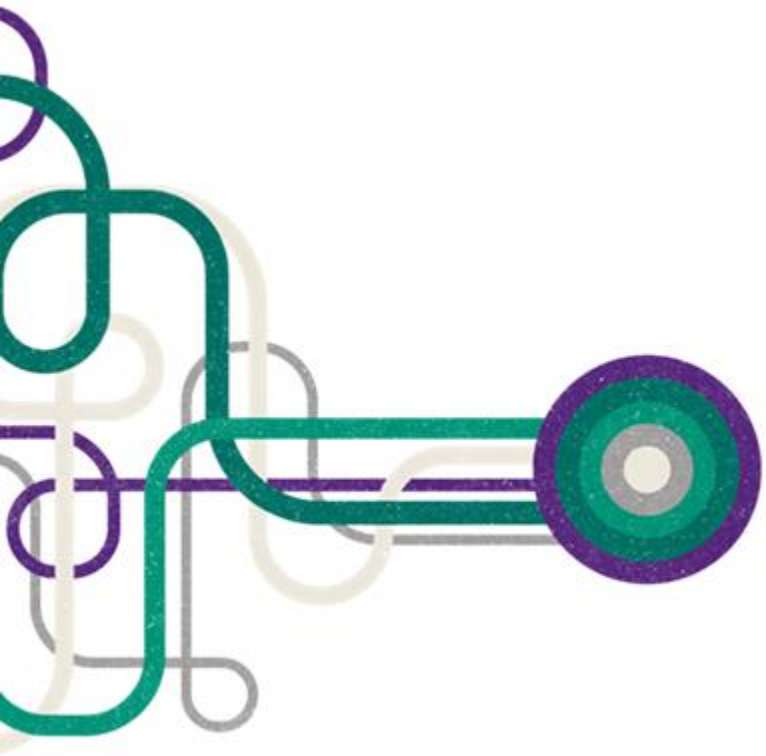
Grant Thornton

An instinct for growth™



Uafhængig revisors ISAE 3000 Type II - erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger for 1. marts 2019 til 29. februar 2020

IDQ A/S

CVR-nr.: 34 04 62 20

Maj 2020

Indholdsfortegnelse

Symbol

- Vores gennemgang har ikke ført til bemærkninger.
- Der er konstateret enkelte svagheder.
- Der er fundet væsentlige svagheder eller mangler.

1. Ledelsens udtalelse

IDQ A/S varetager databehandling af personoplysninger for vores kunder, der er dataansvarlige i henhold til EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") 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 "databeskyttelsesloven").

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt ydelser relateret til behandling og berigelse af data, 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 databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

IDQ A/S bekræfter, at:

a) Den medfølgende beskrivelse, side 7-8, giver en retvisende beskrivelse af ydelser relateret til behandling og berigelse af data, der har behandlet personoplysninger for dataansvarlige som er omfattet af databeskyttelsesforordningen i perioden 1. marts 2019 til 29. februar 2020. Kriterierne der er anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   i. redegør for, hvordan ydelser relateret til behandling og berigelse af data var udformet og implementeret, herunder redegør for:

      - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger.
      - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger.
      - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
      - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
      - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
      - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede.
      - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af persondata 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 ydelsen, har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen.
      - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

1. Ledelsens udtalelse (fortsat)

ii. indeholder relevante oplysninger om ændringer i databehandlerens ydelser relateret til behandling og berigelse af data til behandling af personoplysninger foretaget i perioden 1. marts 2019 til 29. februar 2020.

iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne ydelser relateret til behandling og berigelse af data 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 ydelser relateret til behandling og berigelse af data, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i perioden 1. marts 2019 til 29. februar 2020. Kriterierne som er 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.

iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden 1. marts 2019 til 29. februar 2020.

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 og databeskyttelsesloven.

København, 4. maj 2020
IDQ A/S

Henrik Saustrup
Direktør

2. Uafhængig revisors ISAE 3000-erklæring

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

Til: IDQ A/S og IDQ A/S' kunder

Omfang

Vi har fået som opgave at afgive erklæring om IDQ A/S' beskrivelse på side 7-8 af sine ydelser relateret til behandling og berigelse af data til behandling af personoplysninger på vegne af dataansvarlige omfattet af EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") 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 "databeskyttelsesloven") i perioden 1. marts 2019 til 29. februar 2020 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

IDQ A/S' ansvar

IDQ A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse på side 3-4, 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 anførte kontrolmål.

Revisors 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.

Grant Thornton 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 IDQ A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sine ydelser relateret til behandling og berigelse af data samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet på side 7-8.

2. Uafhængig revisors ISAE 3000-erklæring (fortsat)

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

Begrænsninger i kontroller hos en dataansvarlig

IDQ 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 ydelser relateret til behandling og berigelse af data, 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 ydelser relateret til behandling og berigelse af data, således som denne var udformet og implementeret i perioden 1. marts 2019 til 29. februar 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 perioden 1. marts 2019 til 29. februar 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 perioden 1. marts 2019 til 29. februar 2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår på side 10-32.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 10–32 er udelukkende tiltænkt dataansvarlige, der har anvendt IDQ A/S' ydelser relateret til behandling og berigelse af data, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, 4. maj 2020

Grant Thornton
Statsautoriserede revisionspartnerselskab
CVR-nr. 34 20 99 36

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Anders Grønning-Kjærgaard
Director, Head of IT Audit & Advisory

3. Systembeskrivelse

3.1 Beskrivelse af behandling

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

- Kreditvurdering
- Forbedring af datakvalitet
- Teknologiske ydelser (såsom IT-infrastruktur, hosting, software)

IDQ arbejder typisk med følgende opgaver:

- Berigelse af data med ekstra/nye dataelementer
- Anonymisering af data
- Dataopslag
- Formidling af data eller på anden måde at gøre data tilgængelige for 3. part
- Datasøgning
- Indsamling af data
- Match og kombination af data
- Normalisering/tilretning af data
- Opbevaring af data
- Rådgivning om data
- Sletning af data
- Strukturering af data
- Udtræk og overførsel af data
- Vask/opdatering af data

Personoplysninger

IDQ behandler typisk følgende kategorier af persondata, hvoraf "almindelige persondata" står for langt hovedparten af behandlingerne.

Almindelige persondata:

- Købstransaktionsdata (fx beløb, produkter, kundeværdi osv.)
- Stamdata (fx navn, adresse, telefon, e-mail osv.)
- Offentlige identifikationsnumre (fx CVR-/P-nummer osv.)
- Data fra offentlige datakilder/grunddatakilder (fx OIS/BBR, Statstidende, Tingbogen)
- Bruger- og logindata

CPR-nummer:

- CPR-nummer

Følsomme persondata:

- Ingen

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Den dataansvarliges kunder og emner
- Offentligt tilgængelige persondata (fx Robinson-listen, telefonbogsdata osv.)
- Ansatte

3. Systembeskrivelse

Overordnet kontrolmiljø

Dokumentation for IDQs kontrolmiljø og sikkerheden herfor er dokumenteret i IDQs overordnede IT-sikkerhedspolitik og medarbejdervendte IT-sikkerhedspolitik. Politikken bliver årligt opdateret jf. IDQs årshjul, som bliver kontrolleret af den årlige IT-revision. Sikkerhedspolitikken tager afsæt i IDQs risikovurdering, som ligeledes bliver kontrolleret/opdateret årligt jf. IDQs årshjul.

Risikovurdering

Risikoanalysen tager sit udgangspunkt i de i IT-sikkerhedspolitikken fastsatte mål, og har til formål at analysere og konkretisere de forhold der er væsentlige for vores virksomheds mulighed for at fastholde og udbygge forretningen. Det er i risikoanalysen at alle væsentlige forudsætninger er håndteret. Risikoanalysen afspejler til enhver tid vores virksomheds virkelighed, hvorfor risici løbende vurderes, behandles og dokumenteres, og en samlet gennemgang af vores risikoanalyse finder sted i forlængelse af den årlige opdatering af IT-sikkerhedspolitikken.

Vi fokuserer på et effektivt værn mod alle former for IT-sikkerhedsmæssige trusler, så virksomhedens produkter, image, og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt.

Vores fokusområder er:

- Høj driftssikkerhed (TILGÆNGELIGHED)
- Korrekt funktion af systemerne, herunder minimeret risiko for manipulation af og fejl i data og systemer (INTEGRITET)
- Fortrolighed i behandling, opbevaring og transmission (FORTROLIGHED)
- Gensidig sikkerhed omkring de involverede parter (AUTENCITET)
- Gensidig og dokumenterbar kontakt (UAFVISELIGHED)

Identifikation, analyse og vurdering af risici med betydning for vores forretning kan tage afsæt i både udefra kommende trusler og interne forhold. Til dette formål er sammensat en arbejdsgruppe af medarbejdere der tilsammen repræsenterer alle dele af forretningen. Gruppen ledes af virksomhedens direktør, som ligeledes har ansvaret for beskaffenheden af virksomhedens produkter og beskyttelse af samme. Alle aktiver som indgår i forretningen skal vurderes og prioriteres efter samme model.

Klassificering og scoring af risici kan findes i IDQs risikoanalyse, som bliver kontrolleret årligt som en del af IDQs årshjul. Årshjulet kontrolleres i forbindelse med den årlige IT-revision.

Kontrol aktiviteter

IDQs kontrolaktiviteter er dokumenteret i IDQs årshjul, som bliver valideret og kontrolleret i forbindelse med den årlige IT-revision. IDQ har udarbejdet et årshjul med årskontroller, som skal sikre at alle relevante kontroller i forhold til IT-sikkerhed og GDPR, som minimum bliver gennemført en gang årligt.

3.2 Komplementerende kontroller hos de dataansvarlige

Den dataansvarliges kontrollerne skal blandt andet sikre at;

- personoplysningerne er ajourførte.
- at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretslige regulering.
- at instruksen er hensigtsmæssig set i forhold til databehandleraftalen og hovedydelsen.
- at den dataansvarliges brugere er ajourførte.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som IDQ A/S har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været nået i perioden 1. marts 2019 til 29. februar 2020.

Vi har således ikke nødvendigvis testet alle de kontroller, som IDQ A/S har nævnt i sin beskrivelse på side 7-8. Kontroller udført hos IDQ A/S' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

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

Vi har udført vores tests af kontroller hos IDQ A/S ud fra nedenstående metoder:

Metode	Overordnet beskrivelse
Forespørgelse	Interview af udvalgte medarbejdere angående kontroller
Observation	Observation af hvordan kontroller udførelse (Design)
Inspektion	Gennemgang af politikker, procedurer og dokumentation af kontrollernes udførelse (Implementering)
Test af kontrol	Gennemførelse af kontrolhandlinger, som vi selv har udført eller som har observeret gennemført af ansvarlige medarbejdere (Udførelse)

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Efterlevelse af instruks (kontrolmål A)

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på tre behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Efterlevelse af instruks (kontrolmål A) - fortsat

Kontrolmål: **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	***Databehandlerens kontrolaktivitet***	***Revisors udførte test***	***Resultat af revisors test***
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B)

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Inspiceret ved en stikprøve på tre databehandler-aftaler, at der er etableret de aftalte sikringsforanstaltninger.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.2	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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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 net-værksdokumentation for at sikre behørig segmentering.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Forespurgt om brugeres adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Windows Event Log (Azure Security Center) • Driftsstabilitet via Sentia • Brugeradfærd på Search og Alert • Kilder	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Forespurgt om der sket opfølgning på alarmer, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.8	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. Forespurgt om teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Forespurgt om der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: o Ændringer i logopsætninger, herunder deaktivering af logning o Ændringer i systemrettigheder til brugere o 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 bruger-aktivitet i logs er beskyttet mod manipulation og sletning.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret, 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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.11	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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerheds-patches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.13	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. Forespurgt, om medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Forespurgt om der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.14	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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Underleverandørens erklæring dækker kun perioden fra 1. januar 2019 til 31. december 2019. Derudover har vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C)

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på tre databehandler-aftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C) - fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Eksamensbeviser	Forespurgt om der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på tre databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. • Referencer fra tidligere ansættelser • Eksamensbeviser	Vores gennemgang har ikke ført til væsentlige bemærkninger.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret en nyansat medarbejder i erklæringsperioden, at den pågældende medarbejder har underskrevet en fortrolighedsaftale. Inspiceret en nyansat medarbejder i erklæringsperioden, at den pågældende medarbejder er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C) - fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.5	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 Forespurgt om fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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, 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. Inspiceret ved en stikprøve på en fratrådt medarbejder i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C) - fortsat

Kontrolmål: **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	***Databehandlerens kontrolaktivitet***	***Revisors udførte test***	***Resultat af revisors 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. Forespurgt om dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Sletning eller tilbagelevering af personoplysninger (kontrolmål D)

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • 5 år for oplysninger underlagt bogføringsloven • 6 måneder for alle kunder	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Opbevaring af personoplysninger (kontrolmål E)

Kontrolmål: **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	***Databehandlerens kontrolaktivitet***	***Revisors udførte test***	***Resultat af revisors test***
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på fire 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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Brug af underdatabehandlere (kontrolmål F)

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på tre 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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Brug af underdatabehandlere (kontrolmål F) - fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.3	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i data-behandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på en underdatabehandleraftale, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
F.4	Databehandleren har en oversigt over godkendte underdata-behandlere 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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Brug af underdatabehandlere (kontrolmål F) - fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.5	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Udlevering, rettelse, sletning og begrænsning af personoplysninger (kontrolmål H)

Kontrolmål:

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*	*Revisors udførte test*	*Resultat af revisors test*
H.1	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. Inspiceret, at procedurerne er opdateret.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Håndtering af sikkerhedsbrud (kontrolmål I)

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
I.2	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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Håndtering af sikkerhedsbrud (kontrolmål I) - fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
I.4	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. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

Grant Thornton
An instinct for growth™

PENNEO

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

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

Anders Grønning Kjærgaard
Revisor
Serienummer: PID:9208-2002-2-822661869402
IP: 213.32.xxx.xxx
2020-05-04 05:16:48Z
NEM ID

Jacob Helly Juell-Hansen
Statsautoriseret revisor
Serienummer: CVR:34209936-RID:50904197
IP: 62.243.xxx.xxx
2020-05-04 06:08:03Z
NEM ID

Henrik Saustrup
Underskriver
Serienummer: CVR:34046220-RID:14399917
IP: 87.60.xxx.xxx
2020-05-04 13:31:04Z
NEM ID