

Uafhængig revisors ISAE 3000 - erklæring med sikkerhed om  
beskrivelsen af kontroller rettet mod databeskyttelse og behandling  
af personoplysninger for perioden  
10. januar 2019 til 27. februar 2020

AMConsulting ApS

CVR-nr.: 30 08 62 87

# Indholdsfortegnelse

	Side	Vurdering
1. Ledelsens udtalelse	3	
2. Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger	5	
3. Systembeskrivelse	7	
4. Kontrolmål, kontrolaktivitet, test og resultat heraf	9	
Efterlevelse af instruks (kontrolmål A)	10	●
Tekniske foranstaltninger (kontrolmål B)	11	●
Organisatoriske foranstaltninger (kontrolmål C)	21	●
Sletning eller tilbagelevering af personoplysninger (kontrolmål D)	25	●
Opbevaring af personoplysninger (kontrolmål E)	27	●
Brug af underdatabehandlere (kontrolmål F)	28	●
Udlevering, rettelse, sletning og begrænsning af personoplysninger (kontrolmål H)	31	●
Håndtering af sikkerhedsbrud (kontrolmål I)	32	●

**Symbol**

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



# 1. Ledelsens udtalelse

AMConsulting ApS 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").

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt rådgivning om økonomi- og HR-styring, 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.

AMConsulting ApS bekræfter, at:

- a) Den medfølgende beskrivelse, side 7-9, giver en retvisende beskrivelse af rådgivning om økonomi- og HR-styring, der har behandlet personoplysninger for dataansvarlige som er omfattet af databeskyttelsesforordningen fra d. 10. januar 2019 til 27. februar 2020. Kriterierne der er anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
  - i. redegør for, hvordan rådgivning om økonomi- og HR-styring 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 rådgivning om økonomi- og HR-styring's udformning 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 rådgivning om økonomi- og HR-styring til behandling af personoplysninger foretaget fra 10 januar 2019 til 27. februar 2020.
  - iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne rådgivning om økonomi- og HR-styring 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 rådgivning om økonomi- og HR-styring, 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 fra 10 januar 2019 til 27. 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, og
  - iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse fra 10 januar 2019 til 27. februar 2020.
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandleriskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

*Arne E. Jensen*

*Martin V. Olsen*

*3. april 2020*

*Fensmarkgade 3*

*2200 København N*

## 2. Uafhængig revisors ISAE 3000-erklæring

### Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med deres kunder.

Til: AMConsulting ApS og deres kunder

#### Omfang

Vi har fået som opgave at afgive erklæring om AMConsulting ApS' beskrivelse på side 7-9 af sin rådgivning om økonomi- og HR-styring 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") fra 10. januar 2019 til 27. februar 2020 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

#### AMConsulting ApS' ansvar

AMConsulting ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse på side 3, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere 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.

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 AMConsulting ApS' 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 sin rådgivning om økonomi- og HR-styring 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 på side 7-9.

## 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

AMConsulting ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved rådgivning om økonomi- og HR-styring, 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 rådgivning om økonomi- og HR-styring, således som denne var udformet og implementeret fra 10. januar 2019 til 27. 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 fra 10. januar 2019 til 27. 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 fra 10. januar 2019 til 27. 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 11-33.

### Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 11-33 er udelukkende tiltænkt dataansvarlige, der har anvendt AMConsulting ApS' rådgivning om økonomi- og HR-styring, 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, 3. april 2020

### Grant Thornton

Statsautoriserede revisionspartnerselskab  
CVR-nr. 34 20 99 36

Martin Bomholtz  
Statsautoriseret revisor

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

# 3. Systembeskrivelse

## 3.1 Beskrivelse af behandling

AMConsulting (AMC) er et konsulentfirma, der hovedsageligt rådgiver statslige organisationer om økonomi- og HR-styring. Rådgivningsydelseerne spænder fra udvikling af økonomi- og budgetstyringsmodeller til projektledelse af it-, HR- og økonomistyringsprojekter, samt til at yde konkret assistance til de institutioner, der mangler inspiration, hænder og kompetencer i deres økonomiafdelinger. Dertil kommer undervisningsopgaver i at bruge statens økonomistyringssystemer, optimering af arbejdsgange og processer mv.

Rådgivningsydelseerne forudsætter ofte adgang til kundens relevante økonomi- og HR-data.

### Risikovurdering

Der er tale om data inden for kategorien almindelige personoplysninger – herunder også cpr-numre (fortrolige oplysninger). Der er aldrig tale om data inden for kategorien følsomme personoplysninger. Derfor vurderes konsekvensen for tab, forringelse eller tyveri af de personlige oplysninger for den registrerede, som begrænset. Dog vil AMC altid medtage kundens egen konsekvensanalyse, hvis kunden vurderer konsekvensen for den registrerede højere end AMC.

Data vedrører typisk nuværende og tidligere ansatte hos kunden, nuværende og tidligere tilskudsmodtagere/tilskudsgivere eller nuværende og tidligere leverandører til kunden.

### Overordnet kontrolmiljø og –aktiviteter

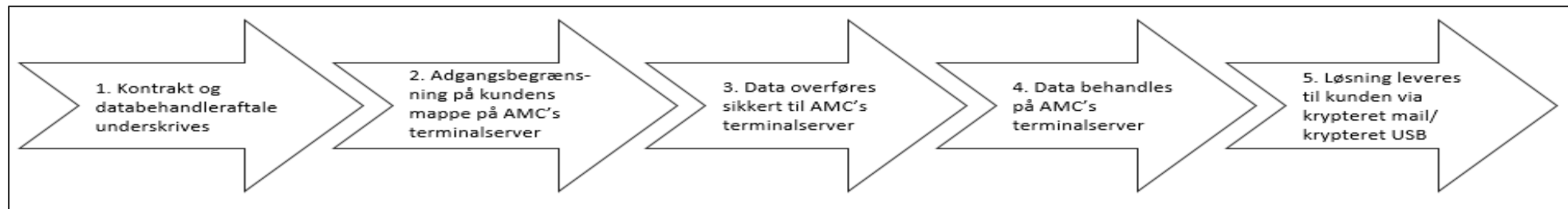
AMC kan arbejde med persondata for kunden på tre forskellige måder:

- a) AMC arbejder med kundens personlige oplysninger via AMC's it-udstyr og på AMC's terminalserver
- b) AMC arbejder med kundens personlige oplysninger hos kunden på kundens it-udstyr, men via AMC's terminalserver
- c) AMC arbejder med kundens personlige oplysninger på kundens it-udstyr og på kundens it-systemer og -server.

I tilfælde a og b, hvor AMC behandler kundens personlige oplysninger på egen terminalserver, søges databehandleraftaler med kunden indgået, og AMC handler først og fremmest på instruks fra kunden (dataansvarlige). Hvis der ikke er givet instruks, følges AMC's egen instruks - se nedenfor.

AMC har valgt, at al data, inkl. personlige oplysninger for kunderne, behandles og opbevares på en terminalserver. Det er således ikke tilladt for de ansatte at arbejde med kundens data uden for terminalserveren. Skal hele eller dele af kundens data flyttes til og fra kunden, sker dette alene via krypterbare USB-nøgler, der er udleveret til alle ansatte i AMC, eller via krypteret mail.

Dataflowet ift. opgaveløsningen for en kunde ser typisk således ud:



### 3. Systembeskrivelse (fortsat)

Sikkerheden ift. AMC's terminalserver:

- Adgangen til terminalserveren er sikret gennem en to-faktor-godkendelse.
- Terminalserveren er sikret med firewall og antivirus programmer.
- Der foretages sårbarhedsscanninger og penetrationstest løbende over året, minimum to gange årligt.
- Der føres en log over adgange på filniveau og ift. adgangen til terminalserveren, så AMC i tilfælde af virus, brud på datasikkerhed eller forsøg på hacking eller lign., ud fra loggen kan se, hvem der har haft adgang.
- Der kan ikke downloades nye programmer til terminalserveren uden om AMC's it-hosting/it-leverandør, og dette skal først godkendes af ledelsen i AMC.
- Der er begrænset adgang til mapper og drev med personhenførbare data, så kun relevante medarbejdere hos AMConsulting har adgang til de enkelte kundemapper. Adgange til kundemapper tildeles via bestilling til administrationschefen, der godkender og videresender til it-leverandøren.

Derudover gælder følgende for AMC's it-udstyr:

- Adgangskoder: På alle AMC-devices anvendes adgangskoder.
- Opbevaring: Alt it-udstyr opbevares aflåst uden for arbejdstiden. I AMC's lokaler sker dette ved, at lokalerne er aflåst i tidsrummet fra arbejdets ophør til næste morgen. Der er desuden etableret adgangssikkerhed til lokalerne.

- Pauseskærm: Hvis udstyret forlades i kortere tid i arbejdstiden, i forbindelse med f.eks. frokost, møder eller andre kortere afbrud, skal udstyret aktivt sættes til pauseskærm. Afbrydelse af pauseskærm kræver anvendelse af personligt password enten til udstyret eller til terminalserver. Alt udstyr skal være indstillet til at gå på pauseskærm, når udstyret ikke har været i brug i 5 min.
- Bærbare PC: Antivirus programmet F-Secure er installeret og aktivt på pc'en.
- Mails med persondata: Der må alene sendes mails, der indeholder fortrolige eller store mængder persondata via krypteret mail (MS Office 365).

Ved brug af kundens it-udstyr til opgaveløsningen efterleves kundens regler for data- og it-sikkerhed. Hvis disse er mere lempelige end AMC's regler, følges AMC's regler.

Alle personlige oplysninger for kunder opbevares og behandles alene ud fra det formål, der er aftalt med kunden ift. den konkrete opgave. AMC opbevarer kun personlige oplysninger, så længe det er nødvendigt ift. opgavens formål, enten for arbejdets udførelse eller som dokumentation for det udførte arbejde.

AMC er underlagt et dokumentationskrav ift. de løsninger, vi laver for kunderne. Det betyder, at AMC skal kunne dokumentere, at løsningen virker på det sæt af data, AMC fik udleveret af kunden til brug for løsning af opgaven. Derfor opbevarer AMC data for kunden i op til 5 år efter, at kunderelationen er ophørt.

I de tilfælde gemmes data på følgende måde:

- Data gemmes og låses via en ZIP-fil med en krypteringsnøgle, der rummer to kodedele. Den ene del har partner A og den anden del partner B. Ved at kombinere de to dele kode, kan data dekrypteres i de tilfælde, der er brug for data til dokumentation af løsningen for kunden.
- De to kode-dele opbevares i et aflåst skab, som kun ledelsen har adgang til i to kuverter, der angiver partnerens navn og er forseglede. Det vil fremgå af en særskilt manuel log i AMC, hvornår og hvorfor kuverterne har været åbnet.



---

## 3. Systembeskrivelse (fortsat)

### 3.2 Komplementerende kontroller hos de dataansvarlige

Det er den dataansvarliges ansvar at sikre de registreredes rettigheder ift. indsigtsret, berigtigelse, begrænsning i behandling og sletning samt dataportabilitet.

Hvis AMC modtager henvendelse fra en registreret i en kundes datasæt om ovenstående, vil der blive henvist til kundens DPO, idet AMC som databehandler handler på kundens (den dataansvarliges) instruks.

## 4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som AMConsulting ApS 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 10. januar 2019 til 27. februar 2020.

Vi har således ikke nødvendigvis testet alle de kontroller, som AMConsulting ApS har nævnt i sin beskrivelse på side 7-9. Kontroller udført hos AMConsulting ApS' 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 AMConsulting ApS 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 indgæede databehandleraftale.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 3 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en 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 procedurer er opdateret.</p> <p>Inspiceret ved en stikprøve på 3 databehandler-aftaler, at der er etableret de aftalte sikringsforanstaltninger.</p>	<p>Vores gennemgang har ikke ført til væsentlige bemærkninger.</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 med dataansvarlige aftalte sikringsforanstaltninger.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler 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 databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.</p>	<p>Vores gennemgang har ikke ført til væsentlige bemærkninger.</p>

## 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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.

## 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	<p>Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger.</p> <p>Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.</p> <p>Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.</p> <p>Forespurgt om brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.</p>	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.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 er tilgængelige og aktiveret på erklæringstidspunktet.</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 på erklæringstidspunktet, samt om de dataansvarlige er behørigt orienteret herom.</p>	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"><li>• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder</li><li>• Sikkerhedshændelser omfattende:<ul style="list-style-type: none"><li>○ Ændringer i logopsætninger, herunder deaktivering af logning</li><li>○ Ændringer i systemrettigheder til brugere</li><li>○ Fejlede forsøg på log-on til systemer, databaser og netværk</li></ul></li></ul> <p>Logoplysninger 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, herunder gennemgang og opfølgning på logs.</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>Vores gennemgang har ikke ført til væsentlige bemærkninger.</p>

## 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Forespurgt om der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse 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.	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgang revurderes regelmæssigt, herunder at 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 en stikprøve på 2 medarbejders adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.</p> <p>Inspiceret ved en stikprøve på 1 fratrådt medarbejder, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.</p> <p>Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.</p>	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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.	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 3 databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikens 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: <ul style="list-style-type: none"><li>• Referencer fra tidligere ansættelse</li><li>• Eksamensbeviser</li></ul>	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.  Inspiceret ved en stikprøve på en nyansat medarbejder i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet: <ul style="list-style-type: none"><li>• Referencer fra tidligere ansættelser</li><li>• Eksamensbeviser</li></ul>	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 ved en stikprøve på 1 nyansat medarbejder i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale.  Inspiceret ved en stikprøve på 1 nyansat medarbejder i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: <ul style="list-style-type: none"><li>• Informationssikkerhedspolitikken</li><li>• Procedurer vedrørende databehandling, samt anden relevant information</li></ul>	Vores gennemgang har ikke ført til væsentlige bemærkninger.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Forespurgt om der er procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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.	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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: <ul style="list-style-type: none"><li>• Opbevares til behandlingen ophører.</li></ul>	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.  Inspiceret databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

## 4. Kontrolmål, kontrolaktivitet, test og resultat heraf

### Sletning eller tilbagelevering af personoplysninger (kontrolmål D) - fortsat

#### Kontrolmål:

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: <ul style="list-style-type: none"><li>• Tilbageleveret til den dataansvarlige og/eller</li><li>• Slettet, hvor det ikke er i modstrid med anden lovgivning.</li></ul>	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.  Inspiceret ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.  Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.  Inspiceret, at procedurerne er opdateret.  Inspiceret databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	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.	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 2 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.  Inspiceret ved en stikprøve på 1 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.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: <ul style="list-style-type: none"><li>• Navn</li><li>• CVR-nr.</li><li>• Adresse</li><li>• Beskrivelse af behandlingen</li></ul>	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
F.6	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.	<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, tredjelands 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>	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vores gennemgang har ikke ført til væsentlige bemærkninger.</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"><li>• Udlevering af oplysninger</li><li>• Rettelse af oplysninger</li><li>• Sletning af oplysninger</li><li>• Begrænsning af behandling af personoplysninger</li><li>• Oplysning om behandling af personoplysninger til den registrerede.</li></ul> <p>Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.</p>	<p>Vores gennemgang har ikke ført til væsentlige bemærkninger.</p>

## 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 en gang årligt – vurdering af, om procedurene 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 proceduren er opdateret.</p>	<p>Vores gennemgang har ikke ført til væsentlige bemærkninger.</p>
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"><li>• Awareness hos medarbejdere</li><li>• Overvågning af netværkstrafik</li><li>• Opfølgning på logning af tilgang til personoplysninger</li></ul>	<p>Forespurgt, om databehandler udbyder awareness træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p> <p>Forespurgt, om netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv.</p> <p>Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.</p>	<p>Vores gennemgang har ikke ført til væsentlige bemærkninger.</p>



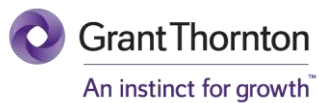
## 4. Kontrolmål, kontrolaktivitet, test og resultat heraf

### 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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
I.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"><li>• Karakteren af bruddet på persondatasikkerheden</li><li>• Sandsynlige konsekvenser af bruddet på persondatasikkerheden</li><li>• Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.</li></ul>	<p>Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"><li>• Beskrivelse af karakteren af bruddet på persondatasikkerheden</li><li>• Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden</li><li>• Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.</li></ul> <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på person-datasikkerheden.</p>	<p>Vores gennemgang har ikke ført til væsentlige bemærkninger.</p>



© 2020 Grant Thornton International Denmark - All rights reserved.

"Grant Thornton" henviser til det brand, hvorunder Grant Thorntons medlemsfirmaer leverer tjenesteydelser indenfor revision, regnskab, skat og rådgivning til deres kunder og/eller til et eller flere medlemsfirmaer, afhængig af konteksten.

Grant Thornton Danmark er medlem af firmaet Grant Thornton International Ltd (GTIL). GTIL og medlemsvirksomhederne er ikke et globalt partnerskab. GTIL og hvert enkelt medlemsfirma udgør hver især en separat juridisk enhed. Tjenesteydelser leveres af medlemsfirmaerne. GTIL leverer ikke tjenesteydelser til kunder. GTIL og dets medlemmer repræsenterer og forpligter ikke hinanden og er heller ikke ansvarlige for hinandens handlinger og forsømmelser.

# PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registeret, 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

2020-04-03 09:33:57Z

NEM ID 

## Martin Bomholtz

Statsautoriseret revisor

Serienummer: PID:9208-2002-2-013768766685

IP: 93.163.xxx.xxx

2020-04-03 09:34:55Z

NEM ID 

## Arne Erling Jensen

Underskriver

Serienummer: PID:9208-2002-2-695512872184

IP: 195.191.xxx.xxx

2020-04-03 12:31:10Z

NEM ID 

## Martin Vesterskov Olsen

Underskriver

Serienummer: PID:9208-2002-2-684510064349

IP: 195.191.xxx.xxx

2020-04-03 12:34:32Z

NEM ID 

Penneo dokumentnøgle: N7KVU-G7XZT-ES03E-24Z5C-NEOF8-MUX5L

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

### Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service** <[penneo@penneo.com](mailto:penneo@penneo.com)>. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: <https://penneo.com/validate>