Grant Thornton
An instinct for growth™

AMConsulting

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om

beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger

Januar 2019

Indholdsfortegnelse

Symbol

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

Grant Thornton | An instinct for growth™

Ledelsens udtalelse

1. Ledelses udtalelse

AMConsulting 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 rådgivningsydelser, 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 bekræfter, at:

a) Den medfølgende beskrivelse, side 8-10, giver en retvisende beskrivelse af rådgivningsydelser, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen og databeskyttelsesloven d. 10. januar 2019. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

i. redegør for, hvordan rådgivningsydelser 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

Ledelsens udtalelse (fortsat)

- 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 rådgivningsydelsers 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

ii. indeholder relevante oplysninger om ændringer i databehandlerens rådgivningsydelser til behandling af personoplysninger foretaget d. 10. januar 2019.

iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne rådgivningsydelser 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 rådgivningsydelser, 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 d. 10. januar 2019. Kriterierne anvendt for at give denne udtalelse var, at:

i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

ii. de identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse d. 10. januar 2019.

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.

Arne E. Jensen

Martin V. Olsen

10. januar 2019

Fensmarkgade 3
2200 København N

Uafhængig revisors erklæring

2. *Uafhængig revisors erklæring*

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

Til: AMConsulting og deres kunder

Omfang

Vi har fået som opgave at afgive erklæring om AMConsulting's beskrivelse på side 8-10 af sine rådgivningsydelser 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") d. 10. januar 2019 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

AMConsulting's ansvar

AMConsulting 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, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i 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 AMConsulting'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.

Uafhængig revisors erklæring (fortsat)

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 rådgivningsydelser 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 3-4.

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's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter rådgivningsydelser, 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 på side 3-4. Det er vores opfattelse,

a) at beskrivelsen af rådgivningsydelser, således som det var udformet og implementeret d. 10. januar 2019, 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 d. 10. januar 2019, 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 d. 10. januar 2019.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår på side 11-50.

Uafhængig revisors erklæring (fortsat)

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 11-50 er udelukkende tiltænkt dataansvarlige, der har anvendt AMConsulting's rådgivningsydelser, 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, 18 januar 2019

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

Ole Skou
Statsautoriseret revisor

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

3. Systembeskrivelse

3.1 Beskrivelse af AMConsulting

AMConsulting (AMC) er et konsulentfirma, der rådgiver offentlige organisationer om økonomi- og HR-styring. Rådgivningsydelserne spænder fra udvikling af økonomi- og budgetstyringsmodeller til projektledelse af it-, HR- og økonomistyringsprojekter og til at yde konkret assistance til de offentlige organisationer, der mangler inspiration, ressourcer og kompetencer i deres økonomi- eller HR-afdelinger. Dertil kommer undervisningsopgaver i at bruge statens økonomistyringssystemer, optimering af arbejdsgange og -processer mv.

Rådgivningsydelserne 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 særlige følsomme personlysninger jf. artikel 9 i databeskyttelsesforordningen. 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 personlige oplysninger 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, indgås der databehandleraftaler med kunden, og AMC behandler 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 opbevares og behandles via en klient 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 kryptérbare USB-nøgler, eller via krypteret mail.

Systembeskrivelse

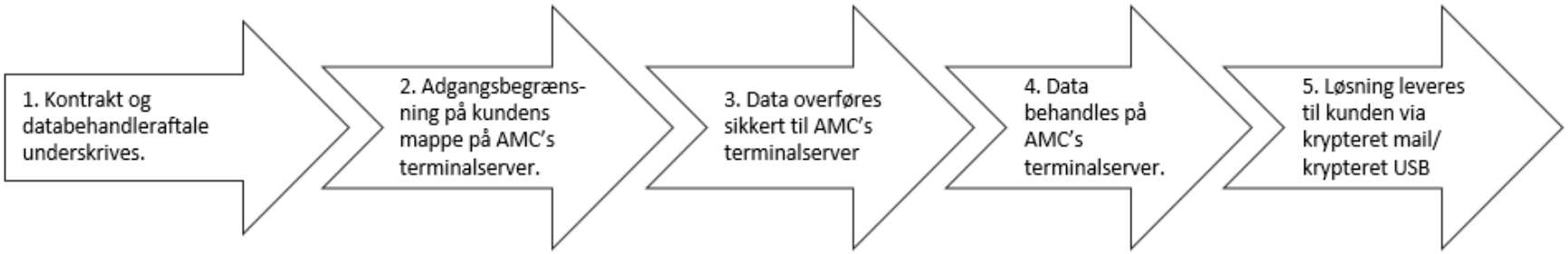
Dataflowet ift. opgaveløsningen for en kunde ser ofte ud som vist i nedenstående figur.

Sikkerheden ift. AMC's terminalserver:

- Adgangen til terminalserveren er sikret gennem en to-faktor-godkendelse.
- Terminalserveren er sikret med firewall og antivirus programmer.
- 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 kundens datasæt med personlige oplysninger, så kun relevante medarbejdere hos AMC har adgang til de enkelte kundemapper. Adgange til kundemapper tildeles via bestilling fra den enkelte projektleder til it-leverandøren og godkendes af ledelsen.

Derudover gælder følgende for AMC's it-udstyr:

- Adgangskoder: På alle AMC-devices anvendes 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, ligesom der er sikkerhedsvagter tilknyttet lejemålet.
- Pauseskærm: Hvis udstyret efterlades i kortere tid under arbejdstiden i forbindelse med f.eks. frokost, møder eller andre kortere afbrud, skal udstyret aktivt sættes til pauseskærm, hvor afbrydelse af pauseskærm kræver anvendelse af personligt password enten til udstyret eller til teminalserver. Alt udstyr skal være indstillet til at gå på pauseskærm, når udstyret ikke har været brugt i 5 min.
- Bærbar PC: Antivirus programmet F-Secure er installeret og aktivt på pc'en.
- Mails med personlige oplysninger: Der må alene sendes mails der indeholder fortrolige eller store mængder personlige oplysninger 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 i op til 5 år efter, at kunderelationen er ophørt.

I de tilfælde gemmes disse 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 de to partnere 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.

3.2 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.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Principper for behandling af personoplysninger (artikel 5)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori der er taget stilling til følgende principper for behandling af personoplysninger: • Lovlighed, rimelighed og gennemsigtighed • Formålsbegrænsning • Dataminimering • Rigtighed • Opbevaringsbegrænsning • Integritet og fortrolighed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, der omfatter principper for behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foretages løbende - og mindst en gang årligt - vurdering af, at principper for behandling af personoplysninger overholdes, og denne vurdering er dokumenteret.	Inspiceret dokumentation for vurdering af principper for behandling af personoplysninger for at sikre, at der minimum en gang årligt foretages vurdering af principper for behandling af personoplysninger samt overholdelsen af disse.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Ledelsen har behandlet og godkendt vurderingen af overholdelse af principperne for behandling af personoplysninger.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af overholdelse af principper for behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Lovlig behandling (artikel 6)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger et lovligt grundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, der indeholder krav til lovlig behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foreligger en af den dataansvarlige godkendt databehandleraftale el.lign., som indeholder oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Inspiceret dokumentation for, på hvilket grundlag behandling af personoplysninger foretages, samt at dette er godkendt af den dataansvarlige (databehandleraftale el.lign.).	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende - og mindst en gang årligt – opdatering af den af den dataansvarlige kunde godkendte oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Inspiceret dokumentation for, at oversigt over grundlag for behandling af personoplysninger er opdateret og godkendt af dataansvarlig kunde mindst en gang årligt.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Der foretages løbende - og mindst en gang årligt - vurdering af, at der ikke er sket ulovlig behandling af personoplysninger, og denne vurdering er dokumenteret.	Inspiceret dokumentation for løbende – og mindst en gang årligt - vurdering af, at der ikke sker eller er sket ulovlig behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Ledelsen har behandlet og godkendt vurderingen af, om der er sket ulovlig behandling af personoplysninger.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af, om der er foretaget ulovlig behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Betingelser for samtykke (artikel 7 og artikel 8)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger et lovligt grundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, der indeholder krav til lovlig behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foreligger en af den dataansvarlige godkendt databehandleraftale el.lign., som indeholder oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Inspiceret dokumentation for, på hvilket grundlag behandling af personoplysninger foretages, samt at dette er godkendt af den dataansvarlige (databehandleraftale el.lign.).	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende - og mindst en gang årligt – opdatering af den af den dataansvarlige kunde godkendte oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Inspiceret dokumentation for, at oversigt over grundlag for behandling af personoplysninger er opdateret og godkendt af dataansvarlig kunde mindst en gang årligt.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Der foretages løbende - og mindst en gang årligt - vurdering af, at der ikke er sket ulovlig behandling af personoplysninger, og denne vurdering er dokumenteret.	Inspiceret dokumentation for løbende – og mindst en gang årligt - vurdering af, at der ikke sker eller er sket ulovlig behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Ledelsen har behandlet og godkendt vurderingen af, om der er sket ulovlig behandling af personoplysninger.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af, om der er foretaget ulovlig behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Behandling af særlige kategorier af personoplysninger (artikel 9 og artikel 10)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori der er taget stilling til, at der alene må ske behandling af særlige kategorier af personoplysninger hos databehandler, såfremt kriterierne for behandling er aftalt specifikt med den enkelte dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, hvori der er taget stilling til, at der alene må ske behandling af særlige kategorier af personoplysninger hos databehandler, såfremt kriterierne for behandling er aftalt specifikt med den enkelte dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foreligger en af den dataansvarlige godkendt databehandleraftale el.lign., som indeholder en opdateret oversigt over, på hvilket grundlag behandling af særlige kategorier af personoplysninger foretages.	Inspiceret dokumentation for, at behandling af særlige kategorier af personoplysninger foretages på et af den dataansvarlige godkendt grundlag.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende - og mindst en gang årligt - vurdering af, om der er sket behandling af særlige kategorier af personoplysninger uden forudgående instruks fra den dataansvarlige.	Inspiceret dokumentation for vurdering af, om der er sket behandling af særlige kategorier af personoplysninger uden forudgående instruks fra den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Ledelsen har behandlet og godkendt vurderingen af, om kravene for behandling af særlige kategorier af personoplysninger er overholdt.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af, om kravene for behandling af særlige kategorier af personoplysninger er overholdt.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Behandling, der ikke kræver identifikation (artikel 11)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, der sikrer, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, der sikrer, at der er taget stilling til, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foreligger en oversigt over kriterier for opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at kriterier for opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede er godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende - og mindst en gang årligt – opdatering af den af den dataansvarlige godkendte oversigt over kriterier for opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede.	Inspiceret dokumentation for, at der løbende og mindst en gang årligt foretages opdatering af den af den dataansvarlige godkendte oversigt over kriterier for opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Behandling, der ikke kræver identifikation (artikel 11), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende - og mindst en gang årligt - vurdering af, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede sker i henhold til kriterierne fra den dataansvarlige.	Inspiceret dokumentation for, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede sker i henhold til kriterierne fra den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Ledelsen har behandlet og godkendt vurderingen af, om der foretages opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede i henhold til kriterier godkendt af den dataansvarlige.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af, om der foretages opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede, så længe dette er påkrævet i henhold til kriterier godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder (artikel 12)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at oplysninger om behandling af personoplysninger kan udleveres til den registrerede, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at oplysninger om behandling af personoplysninger kan udleveres til den registrerede eller den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foreligger en opdateret beskrivelse af oplysninger om behandling af personoplysninger, som er godkendt af den dataansvarlige.	Inspiceret beskrivelsen af oplysninger om behandling af personoplysninger for at sikre, at oplysningerne vil fremgå i en gennemsigtig, lettilgængelig og forståelig form til den registrerede. Inspiceret, at beskrivelsen af oplysninger om behandling af personoplysninger er opdateret og godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Ledelsen har sikret, at oplysninger om behandlingen af personoplysninger er opdateret og godkendt af den dataansvarlige.	Inspiceret dokumentation for, at ledelsen har sikret, at oplysninger om behandlingen af personoplysninger er opdateret og godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder (artikel 12), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foreligger skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag foretages rettidigt, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag foretages rettidigt.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Der foretages løbende - og mindst en gang årligt – sikring af, at besvarelser af anmodninger fra registrerede er gennemført rettidigt.	Inspiceret dokumentation for, at faktiske besvarelser af anmodninger fra registrerede er gennemført rettidigt og i overensstemmelse med procedurer.	Vi har ved vores test ikke fundet væsentlige afvigelser.
6	Ledelsen har sikret, at besvarelse af anmodninger fra registrerede og begrundelse af eventuelt afslag håndteres korrekt og rettidigt.	Inspiceret dokumentation for, at ledelsen har sikret, at besvarelserne håndteres korrekt og rettidigt.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Oplysningspligt ved indsamling af personoplysninger hos den registrerede (artikel 13 og artikel 14)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at den registrerede modtager oplysninger om formål med behandling af personoplysninger samt oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at den registrerede modtager oplysninger om formål med behandling af personoplysninger samt oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foreligger en opdateret beskrivelse af oplysninger om databehandlerens behandling af personoplysninger mv., som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at beskrivelse af oplysninger om behandling af personoplysninger mv. er opdateret og godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Ledelsen har sikret, at beskrivelsen af oplysninger om databehandlerens behandling af personoplysninger mv. er opdateret og godkendt af den dataansvarlige.	Inspiceret dokumentation for, at ledelsen har sikret sig, at beskrivelsen er opdateret og godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Oplysningspligt ved indsamling af personoplysninger hos den registrerede (artikel 13 og artikel 14), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foreligger skriftlige procedurer, hvori udlevering af oplysninger om retten til indsigt i, berigtigelse eller sletning samt begrænsning af behandlingen af personoplysninger til den registrerede er beskrevet, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, hvori udlevering af oplysninger om retten til indsigt i, berigtigelse eller sletning af personoplysninger samt begrænsning af behandlingen til den registrerede er beskrevet.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Der foreligger en opdateret beskrivelse af den registreredes ret til indsigt i, berigtigelse eller sletning mv. af personoplysninger, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at beskrivelse af den registreredes ret til indsigt i, berigtigelse eller sletning af personoplysninger er opdateret og godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
6	Der foretages løbende - og mindst en gang årligt – kontrol af, at alle registrerede har modtaget beskrivelsen af den registreredes ret til indsigt i, berigtigelse eller sletning af personoplysninger.	Inspiceret dokumentation for kontrol af, at alle registrerede har modtaget beskrivelsen af den registreredes ret til indsigt i, berigtigelse eller sletning af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Oplysningspligt ved indsamling af personoplysninger hos den registrerede (artikel 13 og artikel 14), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7	Ledelsen har sikret, at beskrivelsen af oplysninger om den registreredes ret til indsigt, berigtigelse mv. er opdateret og godkendt af den dataansvarlige, samt kommunikeret til alle de registrerede.	Inspiceret dokumentation for, at ledelsen har sikret, at beskrivelsen af oplysninger om den registreredes ret til indsigt, berigtigelse mv. er opdateret og godkendt af den dataansvarlige, samt at alle registrerede har modtaget beskrivelsen.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Den registreredes indsigtsret (artikel 15)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori håndtering af de registreredes anmodninger om indsigt i behandlingen af egne personoplysninger er beskrevet, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, hvori håndtering af de registreredes anmodninger om indsigt i behandlingen af egne personoplysninger er beskrevet.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandler har en beskrivelse til den registrerede af, hvordan personoplysninger indsamles, behandles og opbevares, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at beskrivelsen af, hvordan personoplysningerne bliver behandlet, er godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandleren har et fast defineret format for udtræk af personoplysninger (kopi af de personoplysninger, som er registreret og behandles) til den registrerede, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at indholdet af udtrækket af personoplysninger er godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Den registreredes indsigtsret (artikel 15), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt udtrækket af personoplysninger til den registrerede og beskrivelsen af, hvordan personoplysningerne bliver behandlet, er opdateret og korrekt.	Inspiceret dokumentation for, at udtrækket af personoplysninger til den registrerede og beskrivelsen af, hvordan personoplysningerne bliver behandlet, er opdateret og korrekt.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Der foretages løbende - og mindst en gang årligt – sikring af, at besvarelser af anmodninger fra de registrerede er gennemført rettidigt.	Inspiceret dokumentation for, at faktiske besvarelser af anmodninger fra de registrerede er gennemført rettidigt og i overensstemmelse med procedurer.	Vi har ved vores test ikke fundet væsentlige afvigelser.
6	Ledelsen har sikret, at udtrækket af personoplysninger og beskrivelsen af, hvordan personoplysningerne bliver behandlet, er opdateret og godkendt af den dataansvarlige, samt at besvarelse af anmodninger er håndteret rettidigt.	Inspiceret dokumentation for, at ledelsen har sikret, at udtrækket af personoplysninger og beskrivelsen af, hvordan personoplysningerne bliver behandlet, er opdateret og godkendt af den datasvarlige, samt at besvarelse af anmodninger er håndteret rettidigt.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Ret til berigtigelse (artikel 16 og artikel 19)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori håndtering af de registreredes ret til berigtigelse af personoplysninger er beskrevet, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af de registreredes ret til berigtigelse af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer, at berigtigelse af personoplysninger kan gennemføres.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer til berigtigelse af personoplysninger. Inspiceret dokumentation for, at berigtigelse af personoplysninger alene sker ved anvendelse af de etablerede tekniske foranstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende – og mindst en gang årligt – vurdering af, at berigtigelse af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for kontrol af, at berigtigelse af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Ledelsen har behandlet og godkendt vurderingen af, om berigtigelse af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for, at ledelsen har sikret, at berigtigelse af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Ret til sletning ("retten til at blive glemt") (artikel 17 og artikel 19)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori håndtering af de registreredes ret til sletning af personoplysninger er beskrevet, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af de registreredes ret til sletning af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer, at sletning af personoplysninger kan gennemføres.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer til sletning af personoplysninger. Inspiceret dokumentation for, at sletning af personoplysninger alene sker ved anvendelse af de etablerede tekniske foranstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende – og mindst en gang årligt – vurdering af, at sletning af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for kontrol af, at sletning af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Ledelsen har behandlet og godkendt vurderingen af, om sletning af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for, at ledelsen har sikret, at sletning af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Ret til begrænsning af behandling (artikel 18 og artikel 19)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori håndtering af de registreredes ret til begrænsning af behandling af personoplysninger er beskrevet, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af de registreredes ret til begrænsning af behandling af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer, at begrænsning af behandling af personoplysninger kan gennemføres.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer til begrænsning af behandling af personoplysninger. Inspiceret dokumentation for, at begrænsning af behandling af personoplysninger alene sker ved anvendelse af de etablerede tekniske foranstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende – og mindst en gang årligt – vurdering af, at begrænsning af behandling af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for kontrol af, at begrænsning af behandling af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Ledelsen har behandlet og godkendt vurderingen af, om begrænsning af behandling af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for, at ledelsen har sikret, at begrænsning af behandling af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Ret til dataportabilitet (artikel 20)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori behandling af de registreredes ret til overførsel af egne afgivne personoplysninger til en anden dataansvarlig er beskrevet, eller hvordan databehandler kan bistå den dataansvarlige hermed. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for behandling af de registreredes ret til overførsel af egne afgivne personoplysninger til en anden dataansvarlig.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer, at overførsel af personoplysninger er mulig.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer, at overførsel af personoplysninger er mulig. Inspiceret dokumentation for, at overførsel af personoplysninger alene sker ved anvendelse af de tekniske foranstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandleren har et fast defineret format for udtræk af personoplysninger (kopi af de personoplysninger, som er registreret og behandles) til den registrerede eller en anden dataansvarlig/databehandler, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at udtrækket af personoplysninger til overførsel er godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Ret til dataportabilitet (artikel 20), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende – og mindst en gang årligt – vurdering af, at overførsel af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for kontrol af, at overførsel af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Ledelsen har behandlet og godkendt vurderingen af, om overførsel af personoplysninger er sket korrekt og uden unødig forsinkelse.	Inspiceret dokumentation for, at ledelsen har sikret, at overførsel af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Den dataansvarliges ansvar – implementering af passende databeskyttelse (artikel 24)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Databehandler har modtaget instruks for behandling og beskyttelse af personoplysninger fra den dataansvarlige.	Inspiceret dokumentation for, at den dataansvarlige har givet databehandleren instruks for behandling og beskyttelse af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandleren har overordnede skriftlige procedurer og kontroller, herunder beskrivelse af de tekniske og organisatoriske foranstaltninger, til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at den dataansvarlige har godkendt databehandlerens overordnede skriftlige procedurer og kontroller, herunder tekniske og organisatoriske foranstaltninger, til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandleren har en beskrivelse af anvendelsen af underdatabehandlere, herunder beskrivelse af underdatabehandlernes tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at den dataansvarlige har godkendt databehandlerens underdatabehandlere, herunder deres tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Den dataansvarliges ansvar – implementering af passende databeskyttelse (artikel 24), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende – og mindst en gang årligt – vurdering af, at beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er sket i overensstemmelse med instruksen fra den dataansvarlige og de godkendte procedurer.	Inspiceret dokumentation for kontrol af, at beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er sket i overensstemmelse med instruks og godkendte procedurer.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Ledelsen har behandlet og godkendt vurderingen af, om beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er sket i overensstemmelse med instruksen fra den dataansvarlige og de godkendte procedurer.	Inspiceret dokumentation for, at ledelsen har sikret, at beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er sket i overensstemmelse med instruksen fra den dataansvarlige og de godkendte procedurer.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databeskyttelse gennem design og standardindstillinger (artikel 25)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori sikring af databeskyttelse gennem design og standardindstillinger er beskrevet, herunder hvordan databehandler kan bistå den dataansvarlige med sikring heraf. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for sikring af databeskyttelse gennem design og standardindstillinger, herunder hvordan databehandler kan bistå den dataansvarlige med sikring heraf.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandler har etableret tekniske og organisatoriske sikringsforanstaltninger, som svarer til den dataansvarliges krav til tekniske og organisatoriske sikringsforanstaltninger og databeskyttelse såsom pseudonymisering og dataminimering mv.	Inspiceret dokumentation for, at der er etableret de tekniske og organisatoriske sikringsforanstaltninger, som svarer til den dataansvarliges krav til tekniske og organisatoriske sikringsforanstaltninger og databeskyttelse. Inspiceret dokumentation for, at de etablerede tekniske og organisatoriske sikringsforanstaltninger har fungeret effektivt i erklæringsperioden.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	De af databehandler etablerede tekniske og organisatoriske sikringsforanstaltninger er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at den dataansvarlige har godkendt de etablerede tekniske og organisatoriske sikringsforanstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databeskyttelse gennem design og standardindstillinger (artikel 25), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende – og mindst en gang årligt – vurdering af, at de tekniske og organisatoriske sikringsforanstaltninger og databeskyttelsen er i overensstemmelse med den dataansvarliges krav hertil.	Inspiceret dokumentation for kontrol af, at de tekniske og organisatoriske sikringsforanstaltninger og databeskyttelsen er i overensstemmelse med den dataansvarliges krav hertil.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Databehandler har modtaget instruks fra den dataansvarlige om, hvilke personoplysninger der er nødvendige (dataminimering), og hvordan disse skal behandles i forhold til det/de enkelte specifikke behandlingsformål.	Inspiceret dokumentation for dataansvarliges instruks til databehandleren om, hvilke personoplysninger der er nødvendige, og hvordan disse skal behandles i forhold til det/de specifikke behandlingsformål.	Vi har ved vores test ikke fundet væsentlige afvigelser.
6	Der foretages løbende – og mindst en gang årligt – vurdering af, at der alene foretages behandling af de personoplysninger, som er nødvendige i forhold til det enkelte specifikke behandlingsformål og den modtagne instruks.	Inspiceret dokumentation for kontrol af, at behandling af personoplysninger er begrænset til det specifikke formål i overensstemmelse med instruks.	Vi har ved vores test ikke fundet væsentlige afvigelser.
7	Ledelsen har behandlet og godkendt vurderingen af de tekniske og organisatoriske sikringsforanstaltninger og databeskyttelsen og sikret, at behandlingen af personoplysninger er sket i overensstemmelse med krav og instruks fra den dataansvarlige og de godkendte procedurer.	Inspiceret dokumentation for, at ledelsen har sikret, at de tekniske og organisatoriske sikringsforanstaltninger og databeskyttelsen samt behandlingen af personoplysninger er sket i overensstemmelse med krav og instruks fra den dataansvarlige og de godkendte procedurer.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der er indgået kontrakt eller et andet retligt bindende dokument (databehandleraftale) mellem databehandler og den dataansvarlige, som beskriver de tekniske og organisatoriske sikringsforanstaltninger, som databehandler har etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven samt sikrer beskyttelse af den registreredes rettigheder.	Inspiceret dokumentation for, at databehandleraftalen beskriver de tekniske og organisatoriske sikringsforanstaltninger, som databehandler har etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven samt sikrer beskyttelse af den registreredes rettigheder.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandler har modtaget - specifikt eller generelt – godkendelse fra den dataansvarlige for anvendelse af andre underdatabehandlere. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere.	Inspiceret dokumentation for, at den dataansvarlige har godkendt anvendelsen af andre underdatabehandlere. Inspiceret dokumentation for, at planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere er sket ved underretning til den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandler har modtaget den dataansvarliges instruks for behandling og beskyttelse af personoplysninger hos databehandleren.	Inspiceret dokumentation for, at den dataansvarlige har givet databehandleren instruks for behandling og beskyttelse af personoplysninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foreligger skriftlige procedurer, som beskriver, at databehandler alene må behandle personoplysninger, herunder overførsel af personoplysninger til et tredjeland eller en international organisation, efter dokumenteret instruks fra den dataansvarlige eller i henhold til EU-ret eller national ret. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for, at databehandler alene må behandle og overføre personoplysninger efter dokumenteret instruks fra den dataansvarlige eller i henhold til EU-ret eller national ret.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Der foreligger skriftlige procedurer, som beskriver, at databehandler sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.	Vi har ved vores test ikke fundet væsentlige afvigelser.
6	Der foreligger skriftlige procedurer, som – ved databehandlers brug af underdatabehandlere til udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige - beskriver databehandlers kontroller til sikring af, at underdatabehandler overholder de samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandleraftalen mellem den dataansvarlige og databehandler. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver databehandlers kontroller til sikring af, at underdatabehandlere overholder de samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandleraftalen mellem den dataansvarlige og databehandler.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7	Der foreligger skriftlige procedurer, som beskriver, hvordan databehandler så vidt muligt bistår den dataansvarlige med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder ved hjælp af passende tekniske og organisatoriske foranstaltninger. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler bistår den dataansvarlige med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder ved hjælp af passende tekniske og organisatoriske foranstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
8	Der foreligger skriftlige procedurer, som beskriver, hvordan databehandler - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren - bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i forhold til: • Behandlingssikkerhed (artikel 32) • Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (artikel 33) • Underretning om brud på persondatasikkerheden til den registrerede (artikel 34) • Konsekvensanalyse vedrørende databeskyttelse (artikel 35) • Forudgående høring (artikel 36) Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
9	Der foreligger skriftlige procedurer, som beskriver, hvordan databehandler efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier, medmindre EU-ret eller national ret foreskriver opbevaring af personoplysningerne. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier.	Vi har ved vores test ikke fundet væsentlige afvigelser.
10	Der foreligger skriftlige procedurer, som beskriver, hvordan databehandler stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige samt giver mulighed for og bidrager til revisioner, inspektioner mv., der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige samt giver mulighed for og bidrager til revisioner, inspektioner mv.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
11	Der foretages løbende – og mindst en gang årligt – vurdering af, at databehandler har overholdt de tekniske og organisatoriske sikringsforanstaltninger, som er etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven, samt sikrer beskyttelse af den registreredes rettigheder, samt at behandling af personoplysninger er foretaget i overensstemmelse med den dataansvarliges instruks.	Inspiceret dokumentation for kontrol af, at databehandler har overholdt de tekniske og organisatoriske sikringsforanstaltninger, som er etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven, samt sikrer beskyttelse af den registreredes rettigheder, samt at behandling af personoplysninger er foretaget i overensstemmelse med den dataansvarliges instruks.	Vi har ved vores test ikke fundet væsentlige afvigelser.
12	Ledelsen har behandlet og godkendt vurderingen af overholdelsen af de tekniske og organisatoriske sikringsforanstaltninger og databeskyttelsen, samt at behandlingen af personoplysninger er sket i overensstemmelse med instruks fra den dataansvarlige.	Inspiceret dokumentation for, at ledelsen har sikret overholdelsen af de tekniske og organisatoriske sikringsforanstaltninger og databeskyttelsen, samt at behandlingen af personoplysninger er sket i overensstemmelse med instruks fra den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Fortegnelse over behandlingsaktiviteter (artikel 30)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige, som indeholder: • navn på og kontaktoplysninger for databehandleren for hver dataansvarlig og – hvis det er relevant - den dataansvarliges databeskyttelsesrådgiver • de kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige • overførsler af personoplysninger til et tredjeland eller en international organisation, og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier • en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.	Inspiceret dokumentation for, at der foreligger en fortegnelse over kategorier af behandlingsaktiviteter for den enkelte dataansvarlige med angivelse af den nødvendige information.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	Inspiceret dokumentation for, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er opdateret og korrekt.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Inspiceret dokumentation for, at ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Behandlingssikkerhed (artikel 32)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Databehandler har foretaget en selvstændig risikovurdering af behandlingen af personoplysninger for den enkelte dataansvarlige.	Inspiceret dokumentation for, at der er foretaget en selvstændig risikovurdering af behandlingen af personoplysninger for den enkelte dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandler har etableret passende tekniske og organisatoriske sikringsforanstaltninger for at sikre et sikkerhedsniveau, som passer til risiciene i databehandlerens risikovurdering.	Inspiceret dokumentation for, at der er etableret passende tekniske og organisatoriske sikringsforanstaltninger, som sikrer et sikkerhedsniveau, som passer til risiciene i databehandlerens risikovurdering. Inspiceret dokumentation for, at de etablerede tekniske og organisatoriske sikringsforanstaltninger har fungeret effektivt i erklæringsperioden.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandlers etablerede tekniske og organisatoriske sikringsforanstaltninger er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at den dataansvarlige har godkendt de etablerede tekniske og organisatoriske sikringsforanstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Behandlingssikkerhed (artikel 32) (fortsat)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt risikovurderingen er opdateret og passende.	Inspiceret dokumentation for, at databehandlers risikovurdering er opdateret og passende.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt de tekniske og organisatoriske sikringsforanstaltninger afdækker risiciene i databehandlerens opdaterede risikovurdering.	Inspiceret dokumentation for, at de tekniske og organisatoriske sikringsforanstaltninger sikrer et sikkerhedsniveau, som passer til risiciene i databehandlerens opdaterede risikovurdering.	Vi har ved vores test ikke fundet væsentlige afvigelser.
6	Fysiske personer hos databehandleren og underdatabehandlere er instrueret i håndtering af personoplysninger i henhold til den dataansvarliges instruks.	Inspiceret dokumentation for, at fysiske personer hos databehandleren og underdatabehandlere er instrueret i håndtering af personoplysninger i henhold til den dataansvarliges instruks.	Vi har ved vores test ikke fundet væsentlige afvigelser.
7	Ledelsen har behandlet og godkendt risikovurderinger.	Inspiceret dokumentation for, at ledelsen har behandlet og godkendt de risikovurderinger, som har været gældende i revisionsperioden.	Vi har ved vores test ikke fundet væsentlige afvigelser.
8	Ledelsen har behandlet og godkendt de etablerede tekniske og organisatoriske sikringsforanstaltninger.	Inspiceret dokumentation for, at ledelsen har behandlet og godkendt de etablerede tekniske og organisatoriske sikringsforanstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (artikel 33 og artikel 34)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af brud på persondatasikkerheden, herunder at rettidig kommunikation til den dataansvarlige er beskrevet.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandler sikrer registrering af alle brud på persondatasikkerheden.	Inspiceret dokumentation for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandler fremsender dokumentation omfattende som minimum de faktiske omstændigheder ved bruddet, dets virkning og omfang samt de trufne afhjælpende foranstaltninger til den dataansvarlige.	Inspiceret dokumentation for, at databehandler har fremsendt dokumentation omfattende som minimum de faktiske omstændigheder ved bruddet, dets virkning og omfang samt de trufne afhjælpende foranstaltninger til den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige.	Inspiceret dokumentation for, at ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Konsekvensanalyse vedrørende databeskyttelse (artikel 35)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Databehandler har modtaget den del af resultatet af den dataansvarliges konsekvensanalyse for behandlingen af personoplysninger, som er relevant for databehandlers databehandling for den enkelte dataansvarlige, og databehandlers ledelse har vurderet behovet for at gennemføre egne konsekvensanalyser.	Inspiceret dokumentation for, at ledelsen har modtaget relevante resultater fra de dataansvarliges konsekvensanalyser. Inspiceret dokumentation for ledelsens vurdering af nødvendigheden af at gennemføre egne konsekvensanalyser på hele eller dele af databehandlingen for den enkelte dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandler har etableret passende procedurer, tekniske og organisatoriske sikringsforanstaltninger, som sikrer behandling af personoplysninger i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Inspiceret dokumentation for databehandlers etablering af procedurer samt tekniske og organisatoriske sikringsforanstaltning til at sikre, at persondatabehandlingen sker i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandlers etablerede procedurer, tekniske og organisatoriske sikringsforanstaltninger til databeskyttelse er godkendt af den dataansvarlige, inden der foretages behandling af personoplysninger.	Inspiceret dokumentation for, at de af databehandler etablerede procedurer, tekniske og organisatoriske sikringsforanstaltninger er godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Konsekvensanalyse vedrørende databeskyttelse (artikel 35), fortsat

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt databeskyttelsen er foretaget i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Inspiceret dokumentation for, at der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt databeskyttelsen er foretaget i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Forudgående høring (artikel 36)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Databehandler har modtaget den del af resultatet af den dataansvarliges høring hos tilsynsmyndigheden, som er relevant for databehandlers databehandling for den enkelte dataansvarlige.	Inspiceret dokumentation for, at ledelsen har modtaget den del af resultatet af den dataansvarliges høring hos tilsynsmyndigheden, som er relevant for databehandlers databehandling for den enkelte dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Databehandler har etableret de procedurer, tekniske og organisatoriske sikringsforanstaltninger, som er påkrævet af tilsynsmyndigheden for behandling af de specifikke personoplysninger.	Inspiceret dokumentation for, at krav fra tilsynsmyndighederne er indarbejdet i procedurer, tekniske og organisatoriske sikringsforanstaltninger.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Databehandlers etablerede procedurer, tekniske og organisatoriske sikringsforanstaltninger til sikring af tilsynsmyndighedens krav er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at den dataansvarlige har godkendt de af databehandler etablerede procedurer, tekniske og organisatoriske sikringsforanstaltninger til sikring af tilsynsmyndighedens krav.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt databehandlingen er foretaget i overensstemmelse med tilsynsmyndighedens krav.	Inspiceret dokumentation for løbende opfølgning på overholdelsen af tilsynsmyndighedernes krav til databehandlingen.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databeskyttelsesrådgiver (artikel 37)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
a	Databehandler har udpeget en databeskyttelsesrådgiver, som lever op til krav om tilstrækkelig kompetence.	Inspiceret dokumentation for databehandlerens vurdering af, hvorvidt den udpegede databeskyttelsesrådgiver har de nødvendige kompetencer.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.	Inspiceret dokumentation for, at kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Kontaktoplysninger på databeskyttelsesrådgiveren er meddelt tilsynsmyndigheden.	Inspiceret dokumentation for, at kontaktoplysninger på databeskyttelsesrådgiveren er meddelt tilsynsmyndigheden.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Ledelsen har behandlet og godkendt udpegningen af databeskyttelsesrådgiveren og vurderingen af dennes kompetencer.	Inspiceret dokumentation for ledelsens behandling og godkendelse af udpegningen af databeskyttelsesrådgiveren, herunder sikring af databeskyttelsesrådgiverens kompetencer.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databeskyttelsesrådgiverens stilling (artikel 38)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der er udarbejdet skriftlige procedurer, hvori databeskyttelsesrådgiverens involvering, virke og rapportering er beskrevet. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for databeskyttelsesrådgiverens involvering, virke og rapportering, for at sikre, at denne er fyldestgørende og opdateret.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Ledelsen har sikret, at det er muligt for de registrerede at kontakte databeskyttelsesrådgiveren angående spørgsmål om behandling af deres personoplysninger og deres rettigheder.	Inspiceret dokumentation for, at de registrerede har mulighed for at tage kontakt til databeskyttelsesrådgiveren.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Ledelsen har sikret, at databeskyttelsesrådgiveren er underlagt tavshedspligt og fortrolighed vedrørende udførelsen af sine opgaver.	Inspiceret dokumentation for, at ledelsen har pålagt databeskyttelsesrådgiveren tavshedspligt og krav om fortrolighed.	Vi har ved vores test ikke fundet væsentlige afvigelser.
4	Ledelsen har sikret, at databeskyttelsesrådgiveren ikke udfører andre opgaver eller har andre pligter, som kan medføre interessekonflikt med databeskyttelsesrådgiverens opgaver og pligter.	Inspiceret dokumentation for, at ledelsen har sikret, at databeskyttelsesrådgiveren ikke udfører andre opgaver eller har andre pligter, som kan medføre interessekonflikt med databeskyttelsesrådgiverens opgaver og pligter.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Databeskyttelsesrådgiverens opgaver (artikel 39)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Skriftlige procedurer for databeskyttelsesrådgiverens opgaver omfatter: • At underrette og rådgive om forpligtelser i henhold til denne forordning mv. • At overvåge overholdelsen af denne forordning mv. og af databehandlerens politikker om beskyttelse af personoplysninger • At rådgive med hensyn til konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse • At samarbejde med tilsynsmyndigheden • At fungere som tilsynsmyndighedens kontaktpunkt Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for databeskyttelsesrådgiverens opgaver for at sikre, at disse er fyldestgørende og opdateret.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Ledelsen har sikret, at databeskyttelsesrådgiveren har udført sine opgaver i henhold til de foreliggende procedurer.	Inspiceret dokumentation for, at ledelsen har sikret, at databeskyttelsesrådgiveren har udført sine opgaver i henhold til de foreliggende procedurer.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Overførsel af personoplysninger (artikel 44, artikel 45, artikel 46, artikel 47, artikel 48, artikel 49 og artikel 50)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
1	Der foreligger skriftlige procedurer, hvori overførsel af personoplysninger til et af Kommissionen anerkendt tredjeland eller en af Kommissionen anerkendt international organisation er beskrevet. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede procedurer for overførsel af personoplysninger til et af Kommissionen anerkendt tredjeland eller en af Kommissionen anerkendt international organisation, for at sikre, at disse er fyldestgørende.	Vi har ved vores test ikke fundet væsentlige afvigelser.
2	Der foreligger skriftlige procedurer, hvori sikring af fornødne garantier mv. ved overførsel af personoplysninger til et tredjeland eller en international organisation, som *ikke* er anerkendt af Kommissionen, er beskrevet. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede procedurer for overførsel af personoplysninger til et tredjeland eller en international organisation, som *ikke* er anerkendt af Kommissionen, for at sikre, at disse er fyldestgørende.	Vi har ved vores test ikke fundet væsentlige afvigelser.
3	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt tredjelande eller internationale organisationer, hvortil der overføres personoplysninger, fortsat er anerkendt af Kommissionen.	Forespurgt ledelsen om, hvorvidt der foretages overførsel af personoplysninger til anerkendte tredjelande/internationale organisationer. Inspiceret dokumentation for, at databehandler løbende - og mindst en gang årligt – sikrer, at et tredjeland eller en international organisation, hvortil der overføres personoplysninger, fortsat er anerkendt af Kommissionen.	Vi har ved vores test ikke fundet væsentlige afvigelser.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Overførsel af personoplysninger (artikel 44, artikel 45, artikel 46, artikel 47, artikel 48, artikel 49 og artikel 50) (fortsat)

Kontrolmål: Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
4	Der foretages løbende - og mindst en gang årligt – vurdering af, hvorvidt fornødne garantier mv. fra *ikke*- anerkendte tredjelande eller internationale organisationer, hvortil der overføres personoplysninger, fortsat er tilstrækkelige, kan håndhæves og er effektive.	Forespurgt ledelsen om, hvorvidt der foretages overførsel af personoplysninger til *ikke*-anerkendte tredjelande/internationale organisationer. Inspiceret dokumentation for, at databehandler løbende - og mindst en gang årligt – vurderer, hvorvidt fornødne garantier mv. fra *ikke*-anerkendte tredjelande eller internationale organisationer, hvortil der overføres personoplysninger, fortsat er tilstrækkelige, kan håndhæves og er effektive.	Vi har ved vores test ikke fundet væsentlige afvigelser.
5	Overførsel af personoplysninger til et tredjeland eller en international organisation – anerkendt eller ikke-anerkendt af Kommissionen – er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at overførsel af personoplysninger til et tredjeland eller en international organisation – anerkendt eller ikke-anerkendt af Kommissionen – er godkendt af den dataansvarlige.	Vi har ved vores test ikke fundet væsentlige afvigelser.

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: 62.243.xxx.xxx
2019-01-18 12:43:20Z
NEM ID

Ole Skou
Statsautoriseret revisor
Serienummer: PID:9208-2002-2-260031819805
IP: 62.243.xxx.xxx
2019-01-18 15:15:41Z
NEM ID