www.pwc.dk

EG A/S

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

Januar 2019

Indholdsfortegnelse

1. Ledelsens udtalelse

EG A/S varetager databehandling af personoplysninger for 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" (efterfølgende "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 standard-it-drift og hosting-aktiviteter i EG A/S, 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. EG A/S bekræfter, at:

a) Den medfølgende beskrivelse, side 7 - 11, giver en retvisende beskrivelse af ydelsen, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen og databeskyttelsesloven i perioden 1. januar til 31. december 2018. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) redegør for, hvordan ydelserne 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 ydelserne 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 overvågnings-kontroller, som har været relevante for behandlingen af personoplysninger

   (ii) indeholder relevante oplysninger om ændringer i databehandlerens ydelse til behandling af personoplysninger foretaget i perioden 1. januar til 31. december 2018.

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne ydelse 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 ydelse, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i perioden 1. januar til 31. december 2018. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden 1. januar til 31. december 2018.

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.

Ballerup den 1 februar 2019

Mikkel Bardram
Adm. direktør, Koncernen

2. Uafhængig revisors erklæring

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

Til: EG A/S og EG A/S' kunder relateret til ydelsen

Omfang

Vi har fået som opgave at afgive erklæring om EG A/S' beskrivelse på side 7 - 11 af ydelser i relation til behandling af personoplysninger på vegne af dataansvarlige omfattet af EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesloven") i perioden 1. januar til 31. december 2018 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

EG A/S' ansvar

EG A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse på side 3-4, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, 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.

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

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin ydelse 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

EG A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved ydelsen, 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 ydelsen, således som det var udformet og implementeret i perioden 1. januar til 31. december 2018, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden 1. januar til 31. december 2018, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i perioden 1. januar til 31. december 2018.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår på side 12-45.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 12-45 er udelukkende tiltænkt dataansvarlige, der har anvendt EG A/S' ydelse, 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.

Aarhus, den 4. februar 2019
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
statsautoriseret revisor

3. Systembeskrivelse

3.1 Beskrivelse af ydelse

Indledning
Denne systembeskrivelse vedrører kontroller rettet mod databeskyttelse og beskyttelse af persondataoplysninger i tilknytning til standard it-drift og hosting-aktiviteter i EG A/S som er ejet af Axcel. Standard it-drift og Hosting aktiviteter leveres af EG Managed Services i denne erklæring er benævnt som EG, som det også fremgår af organisationsdiagrammet.

I perioden fra 1. januar 2018 til 25. maj 2018 har EG A/S haft etableret kontroller i relation til databeskyttelse og behandling af persondata med afsæt i den dagældende persondatalov suppleret med kravene fra sikkerhedsbekendtgørelsen. Fra 25. maj 2018 og frem har kontrollerne været etableret med afsæt i persondataforordningen. De tekniske og organisatoriske kontroller har således været gældende i hele perioden. Der er løbende implementeret opdaterede procedurer frem mod 25. maj 2018 på de områder, hvor persondataforordningen introducerede nye og/eller skærpede krav.

EG anvender Global Connect A/S som underleverandør af Datacenter- og Infrastruktur op til og med virtualiseringslaget, hvor på EG's kunder driftes fra. Global Connect er herunder ansvarlig for den fysiske sikkerhed, hardware, netværk, backup, hypervisor og storage. Bemærk at flytningen af EG A/S datacenter ydelser til underleverandøren Global Connect A/S er sket pr. 1. november 2018. Før denne dato lå ansvaret alene hos EG A/S. Global Connect udarbejder ikke en revisionserklæring for perioden 1. januar – 31. december 2018, hvorfor relevante kontroller er selvstændigt testet af PwC for ovenstående periode.

Denne erklæring er udarbejdet efter "inclusive" metoden og inkluderer således kontroller hos underleverandøren Global Connect A/S. Disse kontroller dækkes for 2019 ved modtagelse af revisionserklæring fra Global Connect A/S.

EG varetager drift og monitorering i forbindelse med it-drift og hosting-aktiviteter og er i forbindelse hermed ansvarlig for at sikre implementeringen og funktionen af kontrolsystemer med henblik på at forebygge og opdage fejl, herunder bevidste fejl, med henblik på overholdelse af kontrakter og god skik.

Denne beskrivelse er afgrænset til generelle standarder for administration, som beskrevet i EG's standardkontrakt. Specifikke forhold – der er relateret til individuelle kundekontrakter – er ikke omfattet.

Med baggrund i den ovenstående afgrænsning og nedenfor nærmere angivne systembeskrivelse vurderer EG, at vi i alle væsentlige forhold har opretholdt effektive kontroller. EG er opmærksom på at der kontinuerligt sker udvikling indenfor området, og EG arbejder kontinuerligt på at forbedre kontrollerne.

Arbejdet omkring GDPR er delt i to fokusområder – det interne, som vedrører alle interne processer hvor vi som virksomhed har med persondata at gøre (eksempelvis HR, it, marketing og økonomi) og det kunderettede, som denne erklæring omfatter, som vedrører alle de områder hvor vi interagerer med vores kunder og potentielt kunne komme i berøring med persondata.

EG drifter IT og udvikler software, som naturligvis er i overensstemmelse med gældende lovgivningsmæssige krav, herunder EU persondataforordningen, og vi har som udgangspunkt ikke berøring med kundernes persondata.

Beskrivelse af ydelser, der er omfattet af erklæringen
De ydelser, som EG leverer, er tilpasset flere forskellige typer af kunder. Betingelserne for de enkelte kunder er angivet i kontrakter, hvor der for hvert forretningsområde tages udgangspunkt i standardkontrakter, som kan indeholde individuelle tilretninger og optioner. Til specifikke kunder er disse betingelser angivet i driftshåndbøger, som er udleveret til kunden og fungerer som systemdokumentation. Følgende områder dækker over de ydelser, som EG tilbyder:

Housing: Omfatter kunder, som udelukkende får stillet den fysiske EG-infrastruktur til rådighed, og som selv kontrollerer systemsoftware og applikationssoftware. EG har ansvar for den fysiske sikkerhed.

Hostede kunder: Omfatter kunder, hvis systemer er hostet på dedikerede fysiske eller virtuelle servere. EG har ansvar for den fysiske sikkerhed samt backup. EG har ansvar for vedligeholdelse af systemsoftware, mens tredjepart har ansvaret for applikationssoftware.

IaaS-kunder: Omfatter kunder, som er hostet på delte miljøer. EG har ansvar for den fysiske sikkerhed samt backup. EG har ligeledes ansvar for vedligeholdelse af systemsoftware, mens tredjepart har ansvaret for applikationssoftware.

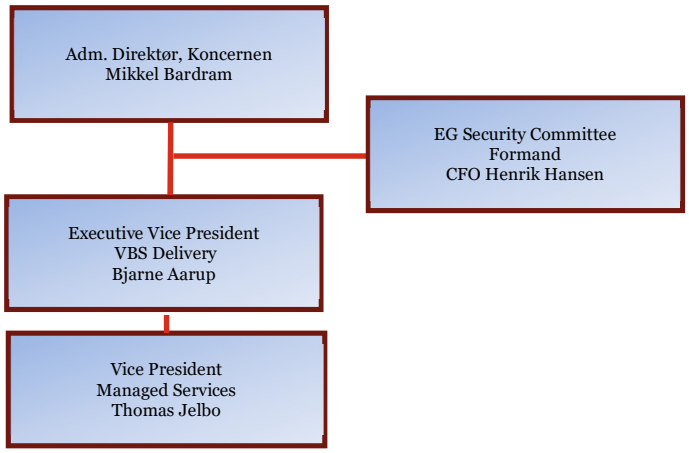
IBM iSeries: Omfatter kunder, som er hostet på et delte Power-maskiner. Der er tale om EG-kunder, som benytter branchesystemer. Disse branchesystemer er udviklet i EG. EG har ansvar for den fysiske sikkerhed samt backup.

Styring af overholdelse af krav mv.

Overholdelse af kravene i relation til databeskyttelse og beskyttelse af persondata følger den organisation, som allerede er etableret i relation til håndtering af it- og informationssikkerhed.

Organisationsform og ledelse bygger på en funktionsopdelt struktur, hvor lederen for den enkelte afdeling har personaleansvar. Sikkerhedsansvaret i de enkelte processer er tildelt henholdsvis ansvarlige og udførende. Den ansvarlige har ansvar for driften og dokumentationen af de enkelte processer hos de ansatte.

Organisationsdiagram – EG



Politikker og organisering

For at sikre sammenhæng mellem arbejdet med databeskyttelse / it-sikkerhed og organisationen er der oprettet et it-sikkerhedsudvalg (EG Security Commitee). It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse og strategisk udvalgte medarbejdere. It-sikkerhedsudvalget refererer direkte til direktionen i EG.

Udvalget er normgivende og fastsætter på grundlag af den vedtagne it-sikkerhedspolitik de principper og retningslinjer, der skal sikre målopfyldelsen. Tilsvarende gælder for databeskyttelsespolitikken 'GDPR rules in EG'.

Udvalget behandler alle it-sikkerhedsspørgsmål og databeskyttelsesspørgsmål af principiel karakter.

EG har udarbejdet en sikkerhedspolitik med afsæt i ISO 27001 standarden og udvalget foretager en årlig vurdering af denne it-sikkerhedspolitik samt de tilknyttede retningslinjer – herunder at disse lever op til de

eksterne forpligtelser, udtrykt i lovgivning og kontrakter/aftaler. Udvalget vurderer samtidig, om der er behov for fornyet risikovurdering. Sikkerhedshændelser inkl. brud på persondatasikkerhed rapporteres til medlemmer af it–sikkerhedsudvalget.

Det overordnede ansvar for it-sikkerheden for 'Standard it-drift og Hosting aktiviteter leveret af EG Managed Services', ligger hos direktøren for VBS Delivery. CISO hos EG sender awareness træning, ændringer i SOP/policies mv. direkte til medarbejderne og det verificeres vha. SecureAware dels at alle har læst/se materialet og dels at alle består den quiz der ofte følger med. De lokale it-sikkerhedskoordinatorer / Security Incident Managers er ansvarlig for håndteringen af hændelser. Det er medarbejdernes daglige leder, der er ansvarlig for at kommunikere retningslinjerne, der understøtter it-sikkerhedspolitikken og databeskyttelsespolitikken, ud til den enkelte ansatte.

Når politikker og procedurer (standard operating procedures) opdateres, kommunikeres dette til medarbejdere. Politikker og proceduren er tilgængelige i ISMS værktøjet, SecureAware, hvor medarbejderne altid kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til it-sikkerhedskoordinatoren, der sørger for relevante rettelser.

EG har ikke en DPO, da den primære aktivitet for kerneforretningen i koncernen ikke omfatter behandling af persondata. EG har dog en funktion (Data Protection Office) der varetager DPO relaterede opgaver.

Procedurer og kontroller

EG har etableret en række politikker og procedurer, som medarbejdere har modtaget og er trænet i efterlevelse af, bl.a. bestående af:

- it sikkerhedspolitikker
- Persondatapolitikker
- Procedurer (SOP)

For hvert løsningsområde og tværgående proces jf. de forrige afsnit er der lavet en risikovurdering af setup'et set i forhold til efterlevelse af den registreredes rettigheder, herunder vurdering af, hvorvidt der er etableret de passende tekniske og organisatoriske kontroller på områderne.

EG har med afsæt i risikovurderingen etableret relevante procedurer.

EG behandler ikke persondata uden indgået databehandleraftale med den dataansvarlige (kunden). Når en aftale indgås, gennemgås denne efter nogle faste tjekpunkter, og alle indgåede databehandleraftaler journaliseres med beskrivelse af særlige krav fra den dataansvarlige (fx svarfrister og/eller krav til særlige kontroller). Eventuelle særlige krav kommunikeres til de relevante teams internt til efterlevelse i deres servicering af kunderne.

Tekniske og organisatoriske kontroller

I relation til tekniske og organisatoriske kontroller henvises til de udarbejdede ISAE 3402 erklæringer.

Disse omfatter områder som

- Medarbejdersikkerhed
- Styring af informationsrelaterede aktiver
- Adgangsstyring
- Kryptering
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold

- Styring af sikkerhedshændelser
- Nød-, beredskabs- og reetableringsstyring

Henvendelser fra de dataansvarlige

EG har en procedure for håndtering og dokumentation af henvendelser fra dataansvarlige i relation til bistand for håndtering af de registreredes rettigheder (indsigtsret, sletning, berigtigelse mv.).

Dokumentation af henvendelser fra dataansvarlige vedr. f. eks. indsigtsret, sletning, berigtigelse mv. håndteres i vores supportsystem.

EG bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder i henhold til Databeskyttelsesforordningen.

I det omfang EG forestår behandling af persondata på vegne af og efter instruks fra den dataansvarlige, bistår EG den dataansvarlige med at sikre overholdelsen af:

- forpligtelsen til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et niveau, der er tilpasset de risici, der er forbundet med behandlingen.
- forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
- forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.
- forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.
- forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko pga. mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3.2 Komplementerende kontroller hos de dataansvarlige

Som led i levering af ydelserne er der kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i beskrivelsen. Dette omfatter bl.a.:

- Stillingtagen til konsekvenser i relation til persondatabeskyttelse når der ændres i eksisterende løsninger (Privacy by design og Privacy by default) og fremsættelse af ændringsanmodning hertil til EG i relevant omfang.
- Stillingtagen til / test af nye versioner af løsninger ifm. implementering (Change Management).
- Opsætning og styring af egne brugere i løsningen i produktionsmiljøet (Identity and Access Management).
- Opsætning og styring af brugere fra EG, som har adgang til kundens miljø (Identity and Access Management).
- Sikring af at personfølsomme oplysninger ikke medsendes i supportsager til EG via tickets mv..

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Formål og omfang

Vores arbejde er udført i overensstemmelse ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår i afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos de tilsluttede virksomheder er ikke omfattet af vores testhandlinger.

Vores test af funktionaliteten har omfattet de kontrolaktiviteter, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden 1. januar til 31. december 2018.

4.2 Udførte testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrolaktiviteternes funktionalitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af, og stillingtagen til, rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er implementeret og har fungeret i perioden 1. januar til 31. december 2018. Dette omfatter bl.a. vurdering af patch-niveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af passende personale. Forespørgsler har omfattet, hvordan kontrollerne udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentag den relevante kontrol. Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

4.3 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	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

Lovlig behandling (artikel 6)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.).	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

Betingelser for samtykke (artikel 7 og 8)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer for indhentelse af skriftligt samtykke til behandling af personoplysninger. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Selskabet er ikke ansvarlig for indhentelse af samtykker, og kontrollerne er ikke aktuelle.	Ingen anmærkninger.
2	Der foretages løbende - og mindst en gang årligt - kontrol af, at der er indhentet skriftligt samtykke til behandling af personoplysninger.	Selskabet er ikke ansvarlig for indhentelse af samtykker, og kontrollerne er ikke aktuelle.	Ingen anmærkninger.
3	Ledelsen har behandlet og godkendt kontrol af, at der er indhentet skriftligt samtykke til behandling af personoplysninger.	Selskabet er ikke ansvarlig for indhentelse af samtykker, og kontrollerne er ikke aktuelle.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af særlige kategorier af personoplysninger alene sker under hensyntagen til fastlagte kriterier, betingelser og de fornødne garantier.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

Behandling, der ikke kræver identifikation (artikel 11)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at oplysninger om behandlingen af personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at udøvelsen af den registreredes rettigheder sker rettidigt, herunder besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	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.	Ingen anmærkninger.
2	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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
3	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.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Selskabet er ikke ansvarlig for håndtering af oplysningspligten overfor de registrerede, og kontrollerne ikke er aktuelle.	Ingen anmærkninger.
2	Der foreligger en opdateret beskrivelse af oplysninger om databehandlerens behandling af personoplysninger mv., som er godkendt af den dataansvarlige.	Selskabet er ikke ansvarlig for håndtering af oplysningspligten overfor de registrerede, og kontrollerne ikke er aktuelle.	Ingen anmærkninger.
3	Ledelsen har sikret, at beskrivelsen af oplysninger om databehandlerens behandling af personoplysninger mv. er opdateret og godkendt af den dataansvarlige.	Selskabet er ikke ansvarlig for håndtering af oplysningspligten overfor de registrerede, og kontrollerne ikke er aktuelle.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registrerede har modtaget oplysning om retten til indsigt i, berigtigelse eller sletning af personoplysninger samt begrænsning af behandlingen.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	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.	Selskabet er ikke ansvarlig for håndtering af oplysningspligten overfor de registrerede, og kontrollerne ikke er aktuelle.	Ingen anmærkninger.
2	Der foreligger en opdateret beskrivelse af den registrerede des ret til indsigt i, berigtigelse eller sletning mv. af personoplysninger, som er godkendt af den dataansvarlige.	Selskabet er ikke ansvarlig for håndtering af oplysningspligten overfor de registrerede, og kontrollerne ikke er aktuelle.	Ingen anmærkninger.
3	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.	Selskabet er ikke ansvarlig for håndtering af oplysningspligten overfor de registrerede, og kontrollerne ikke er aktuelle.	Ingen anmærkninger.
4	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.	Selskabet er ikke ansvarlig for håndtering af oplysningspligten overfor de registrerede, og kontrollerne ikke er aktuelle.	Ingen anmærkninger.

Den registreredes indsigtsret (artikel 15)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til indsigt i egne registrerede personoplysninger og behandlingen heraf er overholdt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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 personoplysnin-	Ingen anmærkninger.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til indsigt i egne registrerede personoplysninger og behandlingen heraf er overholdt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
		gerne bliver behandlet, er opdateret og godkendt af den datasvarlige, samt at besvarelse af anmodninger er håndteret rettidigt.	

Ret til berigtigelse (artikel 16 og artikel 19)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til berigtigelse af egne registrerede personoplysninger er overholdt, herunder berigtigelse hos modtagere af personoplysningerne.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.

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.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til sletning af egne registrerede personoplysninger er overholdt, herunder sletning hos modtagere af personoplysningerne.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

Ret til begrænsning af behandling (artikel 18 og 19)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til begrænsning af behandling af egne registrerede personoplysninger er overholdt, herunder begrænsning hos modtagere af personoplysningerne.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

Ret til dataportabilitet (artikel 20)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til at overføre egne registrerede personoplysninger til en anden dataansvarlig er overholdt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller som sikrer, at tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger fungerer i overensstemmelse med den dataansvarliges retningslinjer.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

Databeskyttelse gennem design og standardindstillinger (artikel 25)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse gennem design og standardindstillinger i databehandlerens tekniske og organisatoriske sikringsforanstaltninger fungerer effektivt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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 per-	Ingen anmærkninger.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse gennem design og standardindstillinger i databehandlerens tekniske og organisatoriske sikringsforanstaltninger fungerer effektivt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
		sonoplysninger der er nødvendige, og hvordan disse skal behandles i forhold til det/de specifikke behandlingsformål.	
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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)	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser.	Ingen anmærkninger.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
	• 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.		
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.

Fortegnelse over behandlingsaktiviteter (artikel 30)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlingsaktiviteter , der foretages på vegne af de dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Der er ikke udarbejdet en oversigt med databehandling på vegne af kunder. Ingen yderligere bemærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.
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.	Der er ikke udarbejdet en oversigt med databehandling på vegne af kunder. Ingen yderligere bemærkninger.

Behandlingssikkerhed (artikel 32)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Der er ikke foretaget en specifik risikovurdering rettet mod beskyttelse af persondata. Der er lavet en risikovurdering på it-sikkerhed i relation til de ydelser, som kunderne køber. Ingen yderligere anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.
7	Ledelsen har behandlet og godkendt risikovurderinger.	Inspiceret dokumentation for, at ledelsen har behandlet og godkendt de risikovurderinger, som har været gældende i revisionsperioden.	Ingen anmærkninger.
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.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden, samt underretning til de registrerede, hvis personoplysninger er omfattet af bruddet.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Ingen anmærkninger.
2	Databehandler sikrer registrering af alle brud på persondatasikkerheden.	Inspiceret dokumentation for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Ingen anmærkninger.
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.	Ingen anmærkninger.
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.	Ingen anmærkninger.

Konsekvensanalyse vedrørende databeskyttelse (artikel 35)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges konsekvensanalyse vedrørende databeskyttelse, inden der foretages behandling af personoplysninger, samt at der foretages en fornyet konsekvensanalyse ved ændring i den risiko, som behandlingsaktiviteterne udgør.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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. Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	Ingen anmærkninger.
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. Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	Ingen anmærkninger.

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. Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	Ingen anmærkninger.
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. Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	Der er ikke etableret en procedure for årlig opfølgning på procedurer mv. Ingen yderligere anmærkninger.

Forudgående høring (artikel 36)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges høring hos tilsynsmyndigheden, såfremt konsekvensanalysen viser, at behandlingen af personoplysninger vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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. Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	Ingen anmærkninger.
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. Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	Ingen anmærkninger.
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.	Ingen anmærkninger.

		Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	
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. Der har endnu ikke været henvendelser fra de dataansvarlige herom. Selskabet har procedurer og kontroller på plads til at håndtere eventuelle henvendelser herom.	Ingen anmærkninger.

Databeskyttelsesrådgiver (artikel 37)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der - i de tilfælde, hvor det er krævet - er udpeget en databeskyttelsesrådgiver, som opfylder krav om tilstrækkelig kompetence, og som er anmeldt til tilsynsmyndigheden.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Databehandler har udpeget en databeskyttelsesrådgiver, som lever op til krav om tilstrækkelig kompetence.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.
2	Kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.
3	Kontaktoplysninger på databeskyttelsesrådgiveren er meddelt tilsynsmyndigheden.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.
4	Ledelsen har behandlet og godkendt udpegningen af databeskyttelsesrådgiveren og vurderingen af dennes kompetencer.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.

Databeskyttelsesrådgiverens stilling (artikel 38)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer databeskyttelsesrådgiverens stilling, herunder at en databeskyttelsesrådgiver ikke modtager instrukser vedrørende udførelsen af dennes opgaver, samt at en databeskyttelsesrådgiver ikke udfører opgaver eller har andre pligter, som kan medføre interessekonflikt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.
2	Ledelsen har sikret, at det er muligt for de registrerede at kontakte databeskyttelsesrådgiveren angående spørgsmål om behandling af deres personoplysninger og deres rettigheder.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.
3	Ledelsen har sikret, at databeskyttelsesrådgiveren er underlagt tavshedspligt og fortrolighed vedrørende udførelsen af sine opgaver.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.
4	Ledelsen har sikret, at databeskyttelsesrådgiveren ikke udfører andre opgaver eller har andre pligter, som kan medføre interessekonflikt med databeskyttelsesrådgiverens opgaver og pligter.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.

Databeskyttelsesrådgiverens opgaver (artikel 39)

Kontrolmål:

Der efterleves procedurer og kontroller , som sikrer, at databeskyttelsesrådgiveren er bekendt med omfanget af sine opgaver, inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger samt rapporterer direkte til ledelsen hos den dataansvarlige eller hos databehandleren.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.
2	Ledelsen har sikret, at databeskyttelsesrådgiveren har udført sine opgaver i henhold til de foreliggende procedurer.	Selskabet har ikke en databeskyttelsesrådgiver, hvorfor kontrollerne ikke er aktuelle.	Ingen anmærkninger.

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

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der alene sker overførsel af personoplysninger til et tredjeland eller en international organisation, hvis Kommissionen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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.	Der overføres ikke oplysninger til tredjeland som led i levering af ydelserne.	Ingen anmærkninger.
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.	Der overføres ikke oplysninger til tredjeland som led i levering af ydelserne.	Ingen anmærkninger.
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.	Der overføres ikke oplysninger til tredjeland som led i levering af ydelserne.	Ingen anmærkninger.
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.	Der overføres ikke oplysninger til tredjeland som led i levering af ydelserne.	Ingen anmærkninger.
5	Overførsel af personoplysninger til et tredjeland eller en international organisation – anerkendt eller ikke- anerkendt af Kommissionen – er godkendt af den dataansvarlige.	Der overføres ikke oplysninger til tredjeland som led i levering af ydelserne.	Ingen anmærkninger.