
EG A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2020 til 31. december 2020 i henhold til databehandlersaftale i relation til udviklings- og driftsydelser i relation til EG Digital Welfare

Marts 2021

Indholdsfortegnelse

1. Ledelsens udtalelse	3
2. Uafhængig revisors erklæring	5
3. Beskrivelse af behandling.....	8
4. Kontrolmål, kontrolaktivitet, test og resultat heraf.....	12

1. Ledelsens udtalelse

EG A/S behandler personoplysninger på vegne af EG A/S' kunder i henhold til databehandleraftale om udviklings- og driftsydelser i relation til EG Digital Welfare.

Medfølgende beskrivelse er udarbejdet til brug for EG A/S' kunder, der har anvendt EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne") er overholdt.

EG A/S anvender Global Connect A/S og team.blue Denmark A/S som underdatabehandlere for anvendte housing-, netværks- og logningsydelser. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Global Connect A/S eller team.blue Denmark A/S varetager for EG A/S.

EG A/S anvender B4Restore A/S som underdatabehandler for anvendte backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som B4Restore A/S varetager for EG A/S.

EG A/S bekræfter, at:

- a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne i hele perioden fra 1. januar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
 - (i) Redegør for, hvordan EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare var udformet og implementeret, herunder redegør for:
 - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
 - De processer i både it-systemer og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
 - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
 - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
 - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
 - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning af de registrerede
 - De processer, der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

- Kontroller, som vi med henvisning til afgrænsningen af EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare har forudsat ville være implementeret af den dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
 - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger
- (ii) Indeholder relevante oplysninger om ændringer i databehandlerens udviklings- og driftsydelser i relation til EG Digital Welfare til behandling af personoplysninger foretaget i perioden fra 1. januar 2020 til 31. december 2020
- (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne udviklings- og driftsydelser i relation til EG Digital Welfare 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 udviklings- og driftsydelse i relation til EG Digital Welfare, som den enkelte dataansvarlige måtte anse vigtigt efter sine særlige forhold.
- b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2020 til 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at:
- (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
 - (ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og
 - (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2020 til 31. december 2020.
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandleretik og relevante krav til databehandlere i henhold til databeskyttelsesreglerne.

Odense, 8. marts 2021



Steffen Kugtvad
Direktør

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2020 til 31. december 2020 i henhold til databehandleraftale i relation til udviklings- og driftsydelser i relation til EG Digital Welfare

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

Omfang

Vi har fået som opgave at afgive erklæring om EG A/S' beskrivelse i afsnit 3 af EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare i henhold til databehandleraftale med dataansvarlige i hele perioden fra 1. januar 2020 til 31. december 2020 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

EG A/S anvender Global Connect A/S og team.blue Denmark A/S som underdatabehandlere for anvendte housing-, netværks- og logningsydelser. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Global Connect A/S eller team.blue Denmark A/S varetager for EG A/S.

EG A/S anvender B4Restore A/S som underdatabehandler for anvendte backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som B4Restore A/S varetager for EG A/S.

Vores konklusion udtrykkes med høj grad af sikkerhed.

EG A/S' ansvar

EG A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisors retningslinjer for revisors etiske adfærd (Ethiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om EG A/S' beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gæl-

dende i Danmark, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

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

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

Begrænsninger i kontroller hos en databehandler

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 EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare, som hver enkelt dataansvarlig måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

- a) at beskrivelsen af EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare, således som de var udformet og implementeret i hele perioden fra 1. januar 2020 til 31. december 2020, i alle væsentlige henseender er retvisende, og
- b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2020 til 31. december 2020, og
- c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2020 til 31. december 2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.


Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt EG A/S' udviklings- og driftsydelser i relation til EG Digital Welfare, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af om kravene i databeskyttelsesreglerne er overholdt.

Aarhus, den 8. marts 2021

PricewaterhouseCoopers

Statsautoriseret Revisionspartnerselskab



Jesper P. Madsen
statsautoriseret revisor

3. *Beskrivelse af behandling*

Indledning

Denne systembeskrivelse vedrører kontroller rettet mod databeskyttelse og beskyttelse af persondataoplysninger i tilknytning til EG's udviklings- og driftsydelser hos EG Managed Services og EG Digital Welfare ApS i EG A/S som er ejet af kapitalfonden Fransisco Partners. EG's udviklings- og driftsydelser hos EG Managed Services og EG Digital Welfare ApS i denne erklæring er benævnt som EG.

Applikationsudviklingen omfatter bl.a. applikationerne EG Sensum, EG Sensum Bosted og EG Sensum Shareplan, Netforvaltning Begravelseshjælp, Mediconnect, Mediconnect Proces, Netforvaltning Sundhed, Netforvaltning Vielse, Netforvaltning Ejendomshandel, EG On Kultur & Fritid, EG On Hjælpemidler, EG On Klagenævn, EG On Helbredstillæg, Netblanket, EG Selvbetjening, OIB Borger, Netforvaltning Offentligt Arrangement, Netforvaltning Udbetaling og NemJournalisering.

EG anvender Global Connect A/S som underleverandør af datacenter- og infrastruktur op til og med virtualiseringslaget, hvor EG's kunder driftes fra. Global Connect er herunder ansvarlig for fysisk sikkerhed, hardware, netværk, backup, hypervisor og storage.

Denne erklæring er udarbejdet efter "exclusive"-metoden og inkluderer således ikke kontroller hos underleverandøren Global Connect A/S. Disse kontroller dækkes for 2020 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 for 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 inden for området, og EG arbejder kontinuerligt på at forbedre kontrollerne.

Arbejdet med 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, der 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 kunders 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:

- **Hostede kunder:** Omfatter kunder, hvis systemer er hostet på dedikerede fysiske eller virtuelle servere. EG har det samlede ansvar for setuppet, men udfører primært udvikling og vedligehold af applikationssoftware.
- **Udvikling af applikationer:** Omfatter kunder, som får udviklet applikationer hos EG. Denne erklæring omfatter kun EG Digital Welfare ApS.

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.

Politikker og organisering

For at sikre sammenhæng mellem arbejdet med databeskyttelse/it-sikkerhed og organisationen er der oprettet et it-sikkerhedsudvalg (EG Security Committee).

It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse, mellemledere samt driftsmedarbejdere. It-sikkerhedsudvalget refererer direkte til direktionen i EG.

EG's it-sikkerhedsudvalg består af:

- CFO Henrik Hansen, formand
- CEO Mikkel Bardram
- EVP Jesper Andersen
- EVP Johnny Iversen
- EVP Erik Tomren
- VP Corporate IT Brian Wested Laursen
- Director Compliance Søren Wolstrup.

Udvalget er normgivende og fastsætter på grundlag af den vedtagne it-sikkerhedspolitik de principper og retningslinjer, der skal sikre målopfyldelsen.

Medlemmer af it-sikkerhedsudvalget deltager løbende i relevant efteruddannelse inden for it-sikkerhed mv. It-sikkerheden er effektueret igennem intern strategi, politikker, standarder, procedurer og guidelines.

VP for Corporate IT er medlem af it-sikkerhedsudvalget samt ansvarlig for den operationelle drift i henhold til de udarbejdede retningslinjer og den daglige ledelse.

Det er medarbejdernes daglige leder, der er ansvarlig for at kommunikere retningslinjerne, der understøtter it-sikkerhedspolitikken, ud til den enkelte ansatte.

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.

Når politikker og procedurer (standard operating procedures) opdateres, kommunikeres dette til medarbejdere. Politikker og procedurer 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 medarbejderne har modtaget og er trænet i efterlevelse af. Disse består bl.a. af:

- It-sikkerhedspolitikker
- Persondatapolitikker

- Procedurer (SOP).

For hvert løsningsområde og tværgående proces jf. de forrige afsnit er der lavet en risikovurdering af setuppet og applikationen 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 service-
ring 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 bi-stand til håndtering af de registreredes rettigheder (indsigtsret, sletning, berigtigelse mv.).

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

Under hensyntagen til behandlingens karakter bistår EG 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 unødigt 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 unødigt 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.

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

Kontrolmål A:

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

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

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved en stikprøve på databehandleraftaler, at der er etableret de aftalte sikkerhedsforanstaltninger.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
B.2	<p>Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandleren foretager en risikovurdering for at opnå en passende sikkerhed.</p> <p>Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Inspiceret, at databehandleren har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.</p>	<p>Vi har ved vores test konstateret, at 6 ud af 25 stikprøver ikke er klassificeret ud fra en risiko om GDPR</p> <p>Vi har fået oplyst, at de pågældende sager ikke er relateret til risikofyldte ændringer. Vi har observeret at forholdet er udbedret 18. maj 2020.</p> <p>Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.</p>
B.3	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.</p>	<p>Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware.</p> <p>Inspiceret, at antivirussoftware er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
B.4	<p>Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.</p>	<p>Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.</p> <p>Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret ved en stikprøve på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering, eksempelvis i tilfælde af kompromittering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at der ved en stikprøve på alarmer er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.8	<p>Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.</p> <p>TLS kryptering i forbindelse med transmission af e-mails overholder Datatilsynets krav på området.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.</p> <p>Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden.</p> <p>Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.</p> <p>Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.</p>	<p>Vi har ved vores test konstateret, at ikke alt kommunikation er sat op med TLS 1.2 eller højere.</p> <p>Forholdet gælder Kultur og Fritid, Klagenævn, Mediconnect og Sensum.</p> <p>EG A/S har udarbejdet handlingsplaner for udbedring af forholdet, dette forventes implementeret Q2 2021.</p> <p>Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.</p>

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> ○ Ændringer i logopsætninger, herunder deaktivering af logning ○ Ændringer i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk. <p>Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang af og opfølgning på logge.</p> <p>Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.</p> <p>Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og sletning.</p> <p>Inspiceret ved en stikprøve på logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser.</p> <p>Inspiceret ved en stikprøve på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
B.10	<p>Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form.</p> <p>Inspiceret ved stikprøver på udviklings- og testdatabaser, at personoplysningerne heri er pseudonymiseret eller anonymiseret.</p> <p>Inspiceret ved en stikprøve på udviklings- og testdatabaser, hvor personoplysningerne ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.11	<p>De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrations-tests.</p> <p>Væsentlige sårbarheder udbedres inden for en fastsat og acceptabel tidshorisont.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests.</p> <p>Inspiceret ved en stikprøve, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.</p> <p>Inspiceret, at eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt til de dataansvarlige i behørigt omfang.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
B.12	<p>Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.</p> <p>Sikkerhedspatches installeres jf. leverandørens anbefalinger og udgivelsescyklus.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.</p> <p>Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.</p>	<p>Vi har ved vores test konstateret, at flere Windows servere ikke var patchet med seneste sikkerhedspakker. Vi har modtaget dokumentation for at forholdet er udbedret ultimo februar 2021.</p> <p>Vi har ved vores test konstateret, at flere Unix servere ikke var patchet med seneste sikkerhedspakker. Vi har modtaget dokumentation for at forholdet er udbedret ultimo januar 2021.</p> <p>Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.</p>

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, og minimum hver 6. måned, herunder om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	<p>Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Inspiceret ved en stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.</p> <p>Inspiceret ved en stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.</p> <p>Inspiceret, at der foreligger dokumentation for en regelmæssig vurdering og godkendelse af tildelte brugeradgange.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede, sker som minimum ved anvendelse af tofaktorautentifikation eller via en sikret jumphost-løsning.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede.</p> <p>Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.</p> <p>Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C:

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

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

Kontrolmål C:

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

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

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	<p>Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.</p> <p>Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D:

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

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

Kontrolmål E:

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

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

Kontrolmål F:

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

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

Kontrolmål F:

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

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

Kontrolmål G:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

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

Kontrolmål H:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

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

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af adgang til personoplysninger. 	<p>Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p> <p>Inspiceret dokumentation for, at netværkstrafikken overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv.</p> <p>Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse og i overensstemmelse med databehandleraftalen efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	<p>Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p> <p>Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden</p> <p>Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.</p> <p>Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødigt forsinkelse og i overensstemmelse med databehandleraftaler, efter at databehandleren er blevet opmærksom på brud på persondatasikkerheden.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål I:

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

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