Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36102030
www.deloitte.dk

IT-Forsyningen I/S

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger mod databeskyttelse og behandling af personoplysninger i henhold til databehandleraftalen med ejer-kommunerne

Erklæringen omfatter perioden fra den 1. januar 2021 til 31. december 2021

Indholdsfortegnelse

1. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger mod databeskyttelse og behandling af personoplysninger i henhold til databehandleraftalen med ejer-kommunerne omfattende perioden fra den 1. januar 2021 til 31. december 2021

Til: IT-Forsyningen I/S og IT-Forsyningen I/S' kunder

Omfang

Vi har fået til opgave at afgive erklæring om IT-Forsyningen I/S' (herefter 'IT-Forsyningen') beskrivelse i afsnit 3 af IT-Forsyningens services i henhold til databehandleraftalen med ejer-kommunerne, der anvender IT-Forsyningens services for perioden 1. januar 2021 til 31. december 2021 (beskrivelsen) samt om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

IT-Forsyningen anvender serviceunderleverandørerne Comit A/S, Comm2IG A/S, EasyIQ A/S, IT Relation A/S og Wizkids til mail-filtrering, kryptering, skrotning af hardware og brugerlogin. Serviceleverandørens systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandørerne. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandørerne.

Nogle af de kontrolmål, der er anført i IT-Forsyningens beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos IT-Forsyningen. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

IT-Forsyningens A/S' ansvar

IT-Forsyningen er ansvarlig for udarbejdelsen af beskrivelsen og den tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden hvorpå beskrivelsen og udtalelsen er præsenteret for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene og 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 IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Deloitte 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 IT-Forsyningens 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 med henblik på 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 IT-Forsyningens platform 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 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 afsnit 2.

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

IT-Forsyningens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved IT-Forsyningens services, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

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

(a) at beskrivelsen af IT-Forsyningens services, således som denne var udformet og implementeret for perioden 1. januar 2021 til 31. december 2021, i alle væsentlige henseender er retvisende
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet for perioden 1. januar 2021 til 31. december 2021
(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 2021 til 31. december 2021.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller, som fremgår af afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt IT-Forsyningens services, 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 databeskyttelsesforordningen er overholdt.

København, den 4. marts 2022

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

2. Ledelsens udtalelse

IT-Forsyningen I/S fungerer som databehandler for en række kunder i kommunerne i forbindelse med leverance af hosting og drift af teknisk infrastruktur.

Medfølgende beskrivelse er udarbejdet til brug for ejer-kommunerne, der anvender IT-Forsyningens løsninger omkring hosting og drift, og 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 EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter databeskyttelsesforordningen) er overholdt.

IT-Forsyningen I/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af IT-Forsyningens løsninger omkring hosting og drift, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen for perioden 1. januar 2021 til 31. december 2021. De kriterier, der er anvendt for at give denne udtalelse, var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan IT-Forsyningens platform 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 underretning til de registrerede
   - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandlingen 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 IT-Forsyningens platforms afgrænsning 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 tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

   (ii) Indeholder relevante oplysninger om ændringer ved databehandlerens platform til behandling af personoplysninger foretaget for perioden 1. januar 2021 til 31. december 2021.

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne IT-Forsyningen-platform til behandling af personoplysninger, under hensyntagen til at be-

skrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved IT-Forsyningens virke, som den enkelte dataansvarlige måtte anse for 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 for perioden 1. januar 2021 til 31. december 2021. De kriterier, der er anvendt for at give denne udtalelse, var, at:

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

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

   (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse for perioden 1. januar 2021 til 31. december 2021.

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.

Farum, den 4. marts 2022

IT-Forsyningen I/S

Rasmus Aagaard Winther
direktør

3. Systembeskrivelse

Denne beskrivelse er udfærdiget med henblik på at beskrive systemerne og kontrollerne relateret til behandlingen af persondata i forbindelse med leverancen af udbudte services til IT-Forsyningens ejerkommuner. Beskrivelsen indgår i ISAE 3000-erklæringen, der udarbejdes i kraft af IT-Forsyningens rolle som databehandler for ejerkommunerne.

IT-Forsyningen er et selvstændigt interessentskab reguleret via egne vedtægter. Selskabets opgave er at levere it-infrastruktur, støtte og en række beslægtede ydelser til ejerkommunerne og samtidig opnå besparelser gennem effektiviseringer i form af kompetenceløft samt harmonisering og konsolidering af de forskellige services, som IT-Forsyningen leverer til ejerkommunerne.

IT-Forsyningen er ejet af Allerød, Ballerup, Egedal og Furesø kommuner. Herefter omtalt som ejerkommunerne.

3.1 Ydelsesbeskrivelse

Selskabets vedtægter, der er godkendt af Statsforvaltningen, regulerer en række formalia om IT-Forsyningens selskabsfunktion samt beskriver selskabets formål.

Interessentskabet har som formål at overtage – herunder samle, effektivisere og videreudvikle – varetagelsen af it-forsyningsopgaven fra ejerkommunerne. Som led i varetagelse af it-forsyning kan selskabet gennemføre udbud og andre anskaffelser i nødvendigt omfang.

Selskabet er forpligtet til at varetage følgende opgaver vedrørende it-forsyningen for ejerkommunerne:

- Serverdrift
- Databasedrift
- Datalager (storage)
- Overvågning, backup og styring af it-aktiver
- ServiceDesk (brugerstøtte)
- Teknisk sikkerhed
- At stille netværks- og telefoniydelser (WAN/LAN) til rådighed
- Telefoni-infrastruktur, telefoniforsyning, herunder sammenhæng til tjenester i det offentlige telenet (mobil- og fastnet)
- Fjernadgang til pc-arbejdspladser
- Teknisk støtte til enheder på netværket (pc'er, printere etc.)
- Indkøb af it-udstyr og basissoftware
- Distribution af it-programmer til differentierede arbejdspladser
- Koordinering til eksterne it-leverandører og andre eksterne it-aktører
- Styring af it-teknisk arkitektur, inklusive telefoni
- It-faglig rådgivning og støtte.

Selskabets vedtægter er konkretiseret i et styringsgrundlag, som udarbejdes i samarbejde med ejerkommunerne i regi af IT-Samarbejdskredsen og ændringer besluttes i selskabets bestyrelse.

Formålet med styringsgrundlaget er at beskrive de opgaver, IT-Forsyningen løser for de medvirkende kommuner, opgavedelingen, samarbejdsmodellen, betingelser og mål for de tilbudte services samt sammenhængen mellem IT-Forsyningens basisbudget og den del af økonomien, som afregnes direkte med den enkelte kommune.

De tilbudte services konkretiseres yderligere i selskabets servicekatalog. Servicekataloget beskriver de services, som IT-Forsyningen leverer til ejerkommunerne. IT-Forsyningen benytter en servicebaseret forretningsmodel, som indebærer:

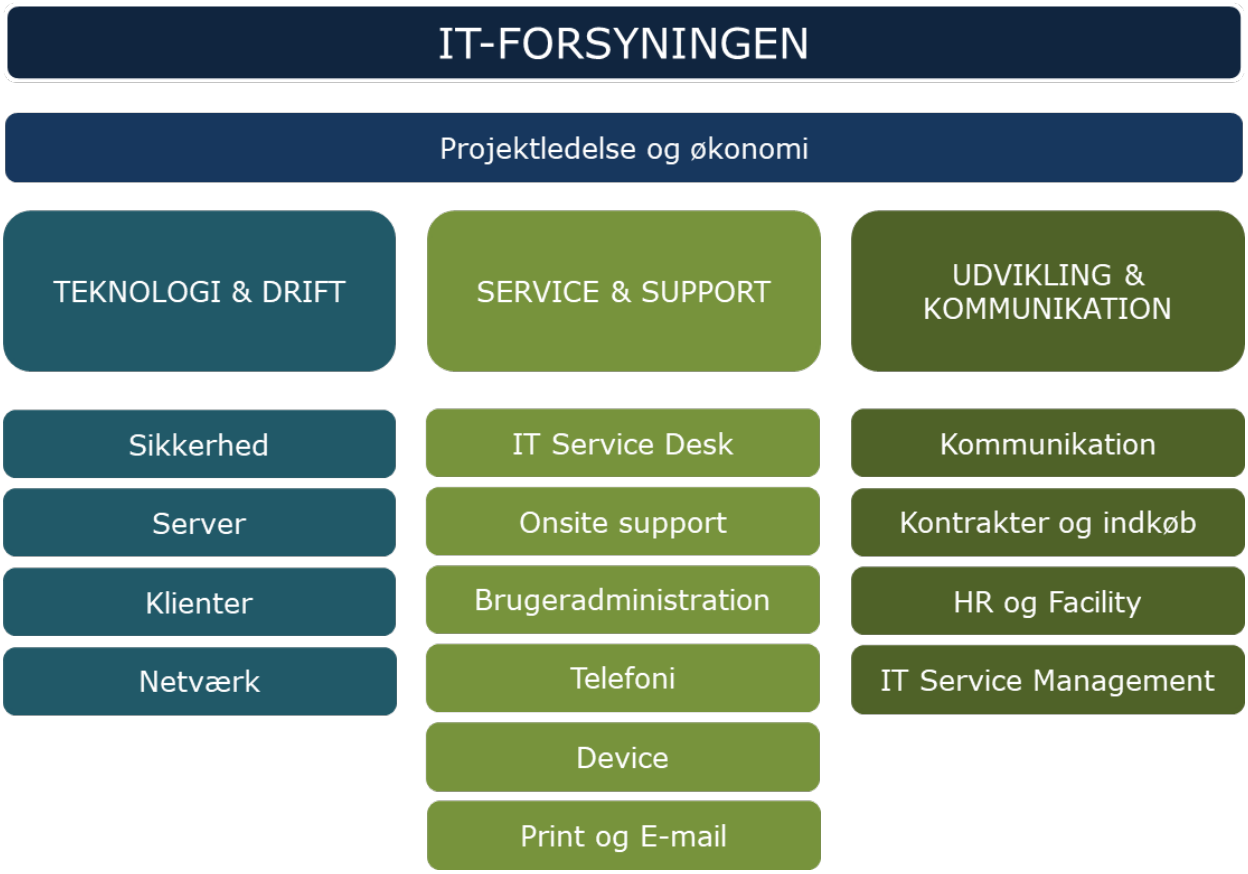
- At samtlige services (materielle som immaterielle) beskrives
- At der styres efter SLA
- At et servicekatalog benyttes
- At en bestillingsportal, hvor kommunen kan bestille og afbestille it-services, benyttes
- At der tages betaling for de services, der leveres, enten gennem direkte betaling eller forskellige former for abonnement.

Hos IT-Forsyningen arbejdes der med et servicekatalog, der er brugervendt. Det er offentligt og indeholder de services, som IT-Forsyningen tilbyder ejerkommunerne. Servicekataloget er p.t. i version 4.

3.2 IT-Forsyningens organisering

Nedenfor følger en beskrivelse af IT-Forsyningens samlede organisation.

IT-Forsyningens organisationsdiagram



IT-Forsyningen er organiseret i tre afdelinger, Service og Support, Drift og Teknologi samt Udvikling og Kommunikation. Service og Support samt Udvikling & Kommunikationsafdelingerne ledes af service- og udviklingschef, Helle Friis. Drift og Teknologi-afdelingen ledes af direktør og driftschef Rasmus Winther.

IT-Forsyningen knytter en kontaktperson til hver opgave, der bestilles, og vedkommende har sammen med ejerkommunen ansvaret for at levere det aftalte.

I udgangspunktet varetages Service Center, udkørende support samt Service Management af afdelingen Service og Support. Technical Management og IT Operations Management varetages i afdelingen Drift og Teknologi.

3.3 Applikations-/platformbeskrivelse

Selskabets ydelser leveres på platforme, således at ejerkommunernes data er adskilt logisk, og der tildeles adgange baseret på de aftaler, som er indgået med kommunerne.

IT-Forsyningens primære ydelser er drift af netværk, pc'er og servere samt support heraf. De væsentligste systemer for IT-Forsyningen er derfor infrastrukturkomponenter som datacenter, netværksenheder og systemer til softwareudrulning og -virtualisering samt overvågning.

IT-Forsyningen yder ikke support på anvendelsen af it-fagsystemer og har derfor som udgangspunkt ikke adgang til data i ejerkommunernes fagsystemer. Opgaven er derimod at sikre, at de aftalte enheder, netværk, programmer, herunder mailsystem og filservere, er tilgængelige.

Til sagshåndtering af fejl, bestillinger og ændringer og dermed det primære værktøj i kommunikation med brugerne anvendes Cherwell. I Cherwell gives alle it-brugere i kommunen en basal adgang til oprette og se egne sager. Sagsbehandlingsfunktioner i Cherwell kræver tildeling af yderligere rettigheder.

Under support behandler vi typisk almindelige personoplysninger på medarbejdere i ejerkommunerne (brugerne), herunder løst- og fastansatte samt eksterne leverandører.

3.4 Underdatabehandlere

Der er indgået enslydende databehandleraftaler mellem ejerkommunerne og IT-Forsyningen.

Af disse fremgår, at IT-Forsyningen må gøre brug af en underdatabehandler uden forudgående specifik godkendelse fra kommunen, forudsat at IT-Forsyningen skriftligt senest fire uger forinden det planlagte opstartstidspunkt underretter kommunen herom. Kommunen har herefter fire uger til at gøre indsigelse mod ændringer eller tilføjelser.

For at vurdere, hvem der er dataansvarlig og databehandler, benyttes nedenstående skema som udgangspunkt.

Persondata om	**Ejerkommune**	**IT-Forsyningen**	**Leverandør til ITF**
Borgere og brugere i kommunen	Dataansvarlig	Databehandler	Underdatabehandler
Ansat, løstansat mv. i kommunen	Dataansvarlig	Databehandler	Underdatabehandler
Ansat i IT-Forsyningen	-	Dataansvarlig	Databehandler

Se afsnit 3.8.6 for oversigt over godkendte underdatabehandlere.

3.5 Karakteren af behandlingen

IT-Forsyningen behandler under instruks persondata i forbindelse med:

- brugersupport (service desk)
- serverdrift, databasedrift og datalager (storage)
- overvågning og backup
- netværks- og telefoniydelser (WAN/LAN)
- teknisk støtte til enheder på netværket (pc'er, printere etc.).

3.6 Personoplysninger

Jævnfør databehandleraftalerne med kommunerne berettiges IT-Forsyningen til at behandle nedenstående typer personoplysninger i forbindelse med de aftalte services.

- Almindelige personoplysninger jf. Databeskyttelsesforordningens artikel 6: F.eks. navn, e-mailadresse, telefonnummer, stillingsbetegnelse og oplysninger om økonomiske forhold

- Følsomme personoplysninger jf. Databeskyttelsesforordningens artikel 9, herunder race og etnisk oprindelse, politisk overbevisning, religiøs overbevisning, filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger, seksuelle forhold eller seksuel orientering
- Personoplysninger om straffedomme og lovovertrædelser jf. Databeskyttelsesforordningens artikel 10, herunder oplysninger om straffedomme, børneattester og lovovertrædelser
- Oplysninger om CPR-nummer jf. Databeskyttelsesforordningens artikel 11.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- personer, som er nuværende og tidligere politikere
- ansatte og løstansatte hos ejerkommunerne, herunder eksterne leverandører
- borgere bosat i ejerkommunerne (herunder børn og unge)
- brugere på administrative netværk, pædagogiske- og offentlige netværk (herunder børn og unge).

3.7 Risikovurdering

Ledelsen mødes ugentligt for at diskutere bl.a. forretningsrisici, inklusiv økonomiske og teknologiske risici. Ledermøder gennemføres efter et månedshjul, således at første møde i hver måned omhandler regnskab og kontrakter, andet møde omhandler projekter og mål, tredje møde omhandler sikkerhed og fjerde møde omhandler statistik og personale. Herudover har hvert ledermøde faste punkter omkring status fra afdelingerne, kritiske forhold, kommunikation, nye opgaver og kommende møder mv.

Der afholdes månedligt personalemøder for alle medarbejdere, hvor der orienteres om og drøftes forhold omkring virksomhedens drift og udvikling.

Identificerede risici af væsentlig betydning for virksomhedens drift tages uden ugrundet ophold op i virksomhedens bestyrelse og andre relevante samarbejdsfora. Bestyrelsen er tillige ansvarlige for godkendelse af IT-Forsyningens informationssikkerhedspolitik og risikovurdering.

IT-Forsyningen indgår i dialog med ejerkommunerne omkring udarbejdelser og tilpasning af deres it-sikkerhedspolitikker, så snitflader mellem ejerkommunernes og IT-Forsyningens roller og ansvar afklares og defineres. CSI-kredsen med deltagelse af digitaliseringschefer og IT-Forsyningens ledelse har påtaget sig ansvaret for koordinering af opgaver relateret til persondatasikkerhed.

Der foretages løbende en vurdering af, hvad der er passende tekniske og organisatoriske foranstaltninger til at understøtte, at persondataforordningen overholdes, og dette dokumenteres i IT-Forsyningens risikovurdering.

Risikovurdering af leverandører sker som led i dokumenterede processer ved indgåelse og ved årligt tilsyn. Endvidere er foretaget gennemgang af procedurer internt i selskabet med dokumentation af risikovurdering. Resultaterne af gennemgangene er udmøntet i instruks for behandling af persondata samt i tilpasning af enkelte arbejdsgange.

Gennem IT-Forsyningens årshjul for it-sikkerhedsopfølgning sikres løbende opfølgning på alle relevante områder inden for it-sikkerhed og GDPR. Status på opfølgning gennemføres månedligt på ledermøderne.

3.8 Kontrolforanstaltninger

IT-Forsyningen har implementeret kontroller vedr. behandling af personoplysninger inden for følgende områder:

- Databehandleraftaler og instruks (kontrolmål A)
- Tekniske sikringsforanstaltninger (kontrolmål B)
- Organisatoriske foranstaltninger (kontrolmål C)
- Sletning og tilbagelevering af personoplysninger (kontrolmål D)
- Opbevaring af personoplysninger (kontrolmål E)

- Anvendelse af underdatabehandlere (kontrolmål F)
- Overførsel til tredjelande (kontrolmål G)
- Bistand til den dataansvarlige (kontrolmål H)
- Håndtering af sikkerhedsbrud (kontrolmål I).

I afsnit 4 er de kontrolforanstaltninger, IT-Forsyningen anser for relevante for behandlingen af persondata, beskrevet. Nedenfor findes en uddybende beskrivelse af et udvalg af relevante kontrolforanstaltninger.

3.8.1 Generelle procedurer for behandling af personoplysninger (kontrolmål A)

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

Anvendte procedurer og kontroller
IT-Forsyningen samarbejder med ejerkommunerne omkring udarbejdelse og tilpasning af deres it-sikkerhedspolitikker, således at snitflader mellem ejerkommunernes og IT-Forsyningens roller og ansvar er afklarede og definerede.

Identificerede risici tages op i selskabets ledelse og noteres i IT-Forsyningens it-risikomodel. Risici af væsentlig betydning for virksomhedens drift tages uden ugrundet ophold op i virksomhedens bestyrelse. Bestyrelsen er tillige ansvarlig for godkendelse af IT-Forsyningens informationssikkerhedspolitik og risikovurdering.

I 2019 blev der etableret en tværgående informationssikkerhedsgruppe med deltagelse af IT-Forsyningens og ejerkommunernes informationssikkerhedskoordinatorer. Gruppen mødes ca. seks gange om året.

Informationssikkerhedspolitikken beskriver det ledelsesgodkendte niveau for sikkerhed. Informationssikkerhedspolitikken behandles i tværkommunale fora og godkendes af selskabets bestyrelse bestående af kommunale direktører, som repræsenterer hver af ejerkommunerne. Informationssikkerhedspolitikken udmøntes i konkrete politikker, procedurer og instrukser, som gøres tilgængelige for IT-Forsyningens ansatte og medarbejdere i ejerkommunerne i it-sikkerhedshåndbogen.

Der sker løbende opfølgning på, om indhold i it-sikkerhedshåndbogen skal opdateres. Opfølgningen, herunder kontroller, tilrettelægges via årshjul for it-sikkerhedsopfølgning.

I sikkerhedshåndbogen indgår instruks for behandling af persondata på ansatte og borgere i ejerkommunerne. Instruksen, som er gennemgået for IT-Forsyningens medarbejdere, indeholder en opsummering af de instrukser, som ejerkommunerne har givet IT-Forsyningen. Tillige indeholder dokumentet information til de ansatte om kun at udføre behandlinger baseret på instruks. Instruksen er endvidere handlingsanvisende på en række specifikke områder, som relaterer sig til behandling af personoplysninger, f.eks. i supportsituationer.

3.8.2 Tekniske sikringsforanstaltninger (kontrolmål B)

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

Anvendte procedurer og kontroller
Nedenfor fremgår et uddrag af relevante tiltag og kontroller for de tekniske sikringsforanstaltninger.

Netværk
Der er etableret antivirus på alle pc'er samt alle servere, som er opkoblet til central administrationskonsol. Antivirus er konfigureret til automatisk opdatering.

Webtrafik filtreres via ekstern leverandør, der blokerer for sider med potentielt skadevoldende indhold. Filtreringer er etableret for IT-Forsyningen og ejerkommunerne.

Der foretages virus-, malware- og spamscanning af alle indgående og udgående e-mails fra ejerkommunernes og IT-Forsyningens mailsystemer.

Netværk er segmenterede, så personoplysninger ikke kan tilgås af uvedkommende.

Adgang til personoplysninger
Kommunernes applikationsmiljøer er adskilt fra hinanden, hvis der ikke er aftalt og etableret fælles løsning i det delte domæne. Oprettelse og nedlæggelse af administrative rettigheder til ejerkommunernes brugerdomæner udføres for IT-Forsyningens ansatte af IT-Forsyningens brugeradministration og kræver autorisation af leder i IT-Forsyningen. Oprettelser og nedlæggelser dokumenteres i IT-Forsyningens sagsstyringssystem.

IT-Forsyningen tildeles ikke administrative rettigheder til ejerkommunens fagsystemer. I enkelte fagsystemer kan IT-Forsyningens medarbejdere, af ejerkommunens systemejere, tildeles loginadgang med minimale rettigheder med det formål at kunne teste og overvåge den specifikke applikations installation og tilgængelighed.

IT-Forsyningens ansatte kan via fjernadgang opnå adgang til selskabets systemer. Adgang sikres med to-faktor-login samt datatransport via krypterede forbindelser.

Logning
Der er etableret logning af brugeraktivitet, undtagelser og fejl på servere og databaser. Logning gennemgås reaktivt ved behov og ved mistanke om uregelmæssighed. Logoplysninger opbevares på servere, så det kræver specifikt tildelte rettigheder at tilgå logs.

Der er etableret central logningsfunktionalitet, hvor der opsamles hændelseslogning af sikkerhedslogge vedrørende brugeraktivitet og rettighedstildeling samt undtagelser og fejl fra system- og applikationslogge fra alle domain controllere på domæner håndteret af IT-Forsyningen. For væsentlige områder sendes besked om nødvendig gennemgang af security logs til udvalgte teknikere. Drift- og Teknologichef fastlægger områder og opfølgning.

IT-Forsyningens hovedfokus for logmanagement er drift af infrastrukturen. Logopsamling og –opfølgning fra fagsystemer hører under ejerkommunernes ansvar.

Systemovervågning
Der forefindes formelle ledelsesinformations- og rapporteringssystemer, der sikrer, at ledelsen kan overvåge nøglekontrol- og performancemål. IT-Forsyningens ledelse etablerer og vedligeholder standarder for udvalgte driftsovervågningsområder.

Der er endvidere etableret systemer til overvågning af servere og systemer. Systemer kategoriseret af ejerkommunerne som meget kritiske systemer overvåges 24x7 for oppetid, tilgængelighed, diskplads og services. Såfremt kritisk niveau nås, eller udfald registreres, alarmeres IT-Forsyningens teknikere og rådighedsvagter via SMS.

Sikkerhedshændelser opdages via monitorering eller brugernes indmeldinger, håndteres af udvalgte medlemmer af IT-Forsyningens personale og håndbæres umiddelbart efter opdagelse er sket. Sikkerhedshændelser rapporteres til leder. Procedure herfor er beskrevet og fremgår af IT-Forsyningens sikkerhedshåndbog.

Kryptering og pseudonymisering
IT-Forsyningen kan aldrig anvende personoplysninger på ansatte og borgere i ejerkommunerne til eget brug i forbindelse med udvikling, test eller lign. På samme måde må der aldrig sendes produktionsdata til ejerkommunerne til brug for udvikling, test eller lign. Dette fremgår af selskabets instruks til de ansatte, tillige med at personoplysninger, der anvendes til udvikling, test eller lign., altid skal være i pseudonymiseret eller anonymiseret form.

Pc'ers harddiske krypteres, og kommunikation af informationer sker krypteret, primært via selskabets sagsstyringssystem eller via benyttelse af tunnelmail.

Ændringer til systemer, databaser og netværk
Alle ændringer er underlagt og udføres i henhold til IT-Forsyningens change-procedure, hvis formål er at sikre, at ændringer i IT-Forsyningens driftsmiljø gennemføres i henhold til de aftalte rammer uden gene for brugerne.

Change orders gennemgås på et ugentligt CAB-møde, hvor de faste deltagere er service- og support-chef, drifts- og teknologichef, change manager og eventuelt change-bestillere.

Før ændringer, der påvirker brugerne, udføres, høres den ansvarlige i den påvirkede ejerkommunes digitaliseringsafdeling om, hvorvidt ændringen kan godkendes tidsmæssigt.

Fysisk adgangssikkerhed
IT-Forsyningen har etableret formelle politikker og procedurer for adgangskontrol til systemer, faciliteter og datacentre.

Adgangen til datacentrene er sikret af elektroniske læsere af adgangskort, som er forbundet med centralt adgangskontrolsystem. Adgang til datacentrene gives ud fra jobansvar af IT-Forsyningens ledelse og administreres af udvalgt sikkerhedspersonale i hhv. Ballerup, Furesø, Allerød og Egedal Kommune. Sikkerhedsadministratoren skal kræve, at IT-Forsyningens ledelse autoriserer adgang, før kort udarbejdes og udleveres. IT-Forsyningen rekvirerer periodisk lister over medarbejdere med adgang til datacentrene og anmoder sikkerhedsadministratoren om justering af brugeradgange. Ansvarlig leder i IT-Forsyningen har ansvar for at afmelde adgange til datacentre ved medarbejderes ansættelsesophør.

Løbende test af tekniske foranstaltninger
Der gennemføres løbende test af tekniske foranstaltninger. Minimum årligt gennemføres sårbarhedsskanning af firewall og bagvedliggende systemer. Opfølgning på testresultaterne gennemføres med henblik på en stadig forbedring af sikringstiltag.

3.8.3 Organisatoriske foranstaltninger (kontrolmål C)

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

Anvendte procedurer og kontroller
IT-Forsyningens ansatte gøres bekendt med sikkerhedspolitikker og -procedurer samt instruks vedrørende behandling af personoplysninger ved opdatering af disse samt ved ansættelse. Ved ophør af ansættelse gøres ansatte endvidere opmærksom på den fortsatte tavshedspligt.

Nye ansatte screenes, og den ansættende leder følger faste tjeklister ved både ansættelse og ophør af ansættelse. Procedurerne omfatter blandt andet instruktion om politikker og arbejdsgange, håndtering af adgange til systemer og lokaler samt håndtering af udleveret udstyr.

Årshjulet indeholder processer, som sikrer løbende awareness af medarbejderne, og i tillæg hertil har IT-Forsyningen processer med særligt fokus på medarbejdernes håndtering af persondata for ejerkommunerne.

Ved ansættelse præsenteres nye medarbejdere for instruks vedrørende behandling af personoplysninger. IT-Forsyningen har kortlagt sine databehandleraktiviteter via interviews af medarbejdere. På baggrund af interviews og kortlægning blev der udarbejdet instruks vedrørende behandling af personoplysninger i sparring med de centrale medarbejdere, som blev interviewet. Bl.a. instrueres om håndtering af persondata i supportsituationer. Opfølgning på instruksen samt andre sikkerhedstiltag sker periodisk på blandt andet månedlige personalemøder. Endelig har IT-Forsyningen en DPO-ordning med advokatkontor, som foretager audit og årligt underviser i GDPR-emner, som er særligt aktuelle for IT-Forsyningen.

3.8.4 Sletning og tilbagelevering (kontrolmål D)

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

Anvendte procedurer og kontroller
Ejerkommunerne har selvstændigt ansvar, som dataansvarlige, for at sikre de registreredes rettigheder for borgere og ansatte. IT-Forsyningen bistår som databehandler herved, jævnfør de givne aftaler i databehandleraftalen samt servicekataloget.

Aftaler om backup og genetablering fremgår af servicebeskrivelse i servicekataloget.

IT-Forsyningen vedligeholder egne beskrivelser i opbevarings- og slettepolitik.

I selskabets instruks til medarbejderne fremgår, hvorledes selskabet skal bistå i forhold til sletning og tilbagelevering af data på anmodning fra dataansvarlig.

3.8.5 Opbevaring af data (kontrolmål E)

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

Anvendte procedurer og kontroller
Der føres fortegnelser over behandling af personoplysninger, både i selskabets kapacitet som databehandler for ejerkommunerne og som dataansvarlig for egne medarbejdere. Fortegnelserne er forbundet til kategorierne af services, som er beskrevet i servicekataloget.

Jævnfør aftale med ejerkommunerne vedligeholdes liste over godkendte lokaliteter for behandlingens udførsel. Listen er tilgængelig i sikkerhedshåndbogen og følger aftalte retningslinjer for ændring.

3.8.6 Anvendelse af underdatabehandlere (kontrolmål F)

Formål
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.

Anvendte procedurer og kontroller
Ibrugtagning, ændring og ophør af databehandleraftaler med underleverandører følger dokumenterede arbejdsgange og er placeret organisatorisk, så aftaler ikke overses. Der følges procedurer og tjeklister, som sikrer identifikation af databehandling i nye og eksisterende aftaler, risikovurdering af underleverandører ved indgåelse og under tilsyn samt eventuelt indgåelse af databehandleraftaler og fortrolighedserklæringer og dokumentation heraf. Varsling af ejerkommuner i aftalte situationer indgår tillige i procedurerne.

Der føres lister over kontrakter med angivelse af, om leverandør er underdatabehandler, samt hvorledes der årligt skal føres tilsyn. Liste over godkendte underdatabehandlere føres i sikkerhedshåndbogen og varsling af ejerkommunerne ved ibrugtagning og ændring af eksisterende underdatabehandlere følger aftalt procedure.

Nedenstående liste indeholder de p.t. godkendte underdatabehandlere, jævnfør gældende databehandleraftale.

Navn på underleverandør og CVR-nr.	Adresse på underdatabehandler	Land, hvor personoplysningerne opbevares	Typer af personoplysninger	Formålet med overførslen m.v.
Comit A/S **CVR 20716908**	Gammel Strandvej 18 2990 Nivå	Danmark	Almindelige Følsomme CPR-numre Oplysninger om strafbare forhold	Ifm. mailfiltrering behandles personoplysninger.
COMM2IG A/S **CVR 20719907**	Kokkedal Industripark 104 2980 Kokkedal	Danmark	Almindelige Følsomme CPR-numre Oplysninger om strafbare forhold	Sikker skrotning af hardware indebærer sletning (behandling) af eventuelle personoplysninger.
EasyIQ A/S **CVR 36476656**	Godthåbsvej 89 8660 Skanderborg	Danmark og EU Datacenter-placering: Skanderborg, Kolding og Holland	Almindelige CPR-numre	I forbindelse med håndtering af brugerlogin og synkronisering af brugeroplysninger behandles personoplysninger.
IT Relation A/S **CVR 27001092**	Dalgas Plads 7b, 1 7400 Herning	Danmark	Almindelige Følsomme CPR-numre Oplysninger om strafbare forhold	Ifm. kryptering og dekryptering af sikkermail behandles personoplysninger.
Wizkids **CVR 28706898**	Roskildevej 8 2620 Albertslund	Danmark	Almindelige CPR-numre	I forbindelse med håndtering af brugerlogin og synkronisering af brugeroplysninger behandles personoplysninger.

3.8.7 Overførsel til tredjelande (kontrolmål G)

Formål
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.

Anvendte procedurer og kontroller
Der efterleves procedurer og kontroller, som sikrer, at IT-Forsyningen ikke overfører persondata til tredjelande i sin egenskab af databehandler, idet selskabet i databehandleraftalerne med ejerkommunerne har forpligtet sig til ikke at sende personoplysninger til tredjelande. I forhold til anvendelsen af Microsoft Office 365 indestår ejerkommunerne for sikring af overførselsgrundlaget herfor.

IT-Forsyningen sikrer sig løbende i diverse processer, at der ikke overføres persondata til tredjelande. Instruks vedrørende behandling af personoplysninger gentager forbuddet mod overførsel af persondata til tredjelande. Når der indgås aftaler med leverandører, foreligger der processer, som sikrer, at leverandører, som overfører persondata til tredjelande, afvises. Databehandleraftaler med underdatabehandlere indeholder forbud mod overførsel til tredjelande. Ved det årlige tilsyn af ejerkommunernes underdatabehandlere følges endvidere op på, at leverandører fortsat ikke overfører persondata til tredjelande.

Skulle behovet for, at en leverandør overfører til et tredjeland, opstå, er ejerkommunerne og IT-Forsyningen ifølge databehandleraftalerne i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.

3.8.8 Bistand til dataansvarlige (kontrolmål H)

Formål
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.

Anvendte procedurer og kontroller
Det er ejerkommunernes ansvar at iagttage de registreredes rettigheder, og IT-Forsyningen er forpligtet til at bistå ejerkommunerne med håndteringen heraf. I selskabets instruks til medarbejderne fremgår, hvorledes selskabets ansvar for at bistå samt fristerne herfor skal håndteres efter anmodning fra dataansvarlig.

Henvendelser direkte fra en registreret om udøvelse af sine rettigheder videresendes uden ophold til den berørte ejerkommune.

3.8.9 Sikkerhedsbrud (kontrolmål I)

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

Anvendte procedurer og kontroller
De ansatte i IT-Forsyningen holdes orienterede omkring sikkerhedshændelser og -trusler via interne møder og mails samt opfordres til at søge viden herom.

Der er udarbejdet procedure for håndtering af eventuelle brud på håndtering af persondata. Proceduren indeholder blandt andet varslingsprocedure, frister, håndtering af bruddet samt vejledning til bistand til berørt ejerkommune. Tillige fremgår, hvilke informationer som er væsentlige at få dokumenteret i relation til ejerkommunens anmeldelse af eventuelt brud til Datatilsynet.

3.9 Komplementerende kontroller hos de dataansvarlige

Ejerkommunerne har i kraft af deres rolle som dataansvarlige og de indgåede aftaler forpligtelse til at:

- sikre hjemmel til at behandle de personoplysninger, som kommunen instruerer IT-Forsyningen i at behandle.
- instruks til IT-Forsyningen er lovlig i forhold til den til hver tid gældende persondataretlige regulering.
- instruks er hensigtsmæssig og i overensstemmelse med databehandleraftale og de aftalte services.
- håndtere eget ansvar for fagsystemerne, herunder opfølgning på adgange, logning af hændelser heri, samt at personoplysninger er ajourførte og slettefrister overholdes.
- sikre, at tidligere slettede personoplysninger ikke bliver tilgængelige igen efter en gendannelse.
- at informationer relevante for, at IT-Forsyningen kan udføre sin rolle som databehandler uden ophold videregives til selskabet, herunder men ikke begrænset til videregivelse af information om ændret lovgivning, krav og aftaler.
- oplyse databehandleren om mulige sikkerhedshændelser eller -brud, som kan have relevans for selskabets levering af de aftalte serviceydelser.
- oplyse om eventuelle behandlingsaktiviteter og systemer, som er omfattet af den såkaldte krigsregel i databeskyttelseslovens § 3, stk. 9.
- sikre, at der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i det omfang disse personer ikke er medarbejdere hos IT-Forsyningen.

4 IT-Forsyningens kontrolmål, kontroller, test og resultat heraf

4.1 Introduktion

Denne rapport er udformet med henblik på at informere IT-Forsyningens kunder om IT-Forsyningens services og kontroller, som kan påvirke behandlingen af personoplysninger og samtidig informere de dataansvarlige, for hvem IT-Forsyningen behandler personoplysninger, om funktionaliteten af de kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne hos de dataansvarlige, har til hensigt at hjælpe de dataansvarlige til at vurdere risici forbundet med den outsourcede behandling af personoplysninger, som muligvis påvirkes af kontrollerne hos IT-Forsyningen.

Vores test af IT-Forsyningens kontroller er begrænset til de kontrolmål og relaterede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller kontroller, som forventes at være implementeret hos de dataansvarlige for at opfylde kontrolmålene.

Det er den dataansvarliges ansvar at evaluere denne information i forhold til de kontroller, som eksisterer hos den dataansvarlige. Hvis bestemte komplementerende kontroller ikke er til stede hos den dataansvarlige, kan IT-Forsyningens kontroller muligvis ikke kompensere for sådanne svagheder.

4.2 Test af kontroller

De udførte test i forbindelse med fastlæggelse af kontrollers funktionalitet består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos IT-Forsyningen
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som angiver udførelse af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat

4.3 Kontrolmål, kontroller og resultater af test

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

4.4 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.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Deloitte har inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behovet for opdatering. Deloitte har inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Deloitte har inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Deloitte har stikprøvevist inspiceret, at der i databehandleraftaler er anført instruks.	Ingen afvigelser konstateret.
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.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Deloitte har inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger, og at procedurerne er opdateret. Deloitte har stikprøvevist inspiceret, at der er etableret de aftalte sikringsforanstaltninger i indgåede databehandleraftaler.	Ingen afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at IT-Forsyningen foretager en risikovurdering for at opnå en passende sikkerhed. Deloitte har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger, og at IT-Forsyningen har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Deloitte har stikprøvevist påset, at IT-Forsyningen har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret.
B.3	Der er for de systemer, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Deloitte har inspiceret, at der for de systemer, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Deloitte har inspiceret, at antivirussoftware er opdateret.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Deloitte har inspiceret, at ekstern adgang til systemer, der anvendes til behandling af personoplysninger, alene sker gennem en firewall, og at firewall er konfigureret i henhold til den interne politik herfor.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Deloitte har forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Deloitte har inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er begrænset til brugere med et arbejdsbetinget behov herfor.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger, og at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Endvidere har Deloitte inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelse af begrænsning i brugernes arbejdsbetingede adgang til personoplysninger. Deloitte har for en stikprøve inspiceret, at autorisationer til systemer og data er godkendt og begrænset til arbejdsbetingede behov.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Alarmering ved fejlede forsøg på adgang • Alarmering ved ændringer af administrative brugerrettigheder • Alarmering ved brug af speciallogin, jf. retningslinje herfor.	Deloitte har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret systemovervågning med alarmering. Deloitte har stikprøvevist inspiceret, at incidents bliver vurderet og håndteret af IT-Forsyningen.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Deloitte har 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. Deloitte har inspiceret, at IT-Forsyningen anvender TunnelMail-kryptering.	Ingen afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder f.eks.: o Alarmering ved fejlede forsøg på adgang o Alarmering ved ændringer af administrative brugerrettigheder o Alarmering ved brug af speciallogin, jf. retningslinje herfor. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Deloitte har 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. Deloitte har inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Deloitte har inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at personoplysninger alene anvendes i pseudonymiseret eller anonymiseret form. Deloitte har inspiceret dokumentation for, at der ved anvendelse af personoplysninger i testmiljø, som ikke er pseudonymiseret eller anonymiseret, er udført efter aftale med dataansvarlig.	Det er konstateret, at der i et enkelt tilfælde er blevet oprettet et TEST-miljø for en kommune, hvor personoplysninger ikke blev pseudonymiseret eller anonymiseret. Vi har påset dokumentation for, at oprettelsen er sket efter aftale med den dataansvarlige og på dennes vegne. Ingen yderligere afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for løbende test af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstest. Deloitte har stikprøvevist inspiceret, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Deloitte har stikprøvevist inspiceret, at ændringer til systemer, databaser og netværk, inklusive relevante opdateringer, patches og sikkerhedspatches er blevet håndteret i overensstemmelse med de formaliserede procedurer.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang, som anvendes til behandling af personoplysninger. Deloitte har stikprøvevist inspiceret, at tildelte brugeradgange er godkendte, og at der er et arbejdsbetinget behov. Deloitte har for en stikprøve inspiceret, at fratrådte medarbejdere er blevet rettidigt deaktiveret. Deloitte har inspiceret, at der foreligger dokumentation for regelmæssig vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor-autentifikation.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor-autentifikation anvendes ved behandling af personoplysninger, der medfører en høj risiko for de registrerede. Deloitte har observeret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører en høj risiko for de registrerede, alene kan ske ved anvendelse af to-faktor-autentifikation.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer hos IT-forsyningen kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Deloitte har 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. Deloitte har inspiceret, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Deloitte har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Deloitte har inspiceret, at der forefindes dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder IT-Forsyningens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Deloitte har inspiceret dokumentation for ledelsens vurdering af, hvorvidt informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerhed i indgåede databehandleraftaler. Deloitte har stikprøvevist inspiceret, at kravene i databehandleraftalerne er omfattet af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerhed.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Straffeattest/ børneattest • Eksamensbeviser Børne- og straffeattester gemmes ikke i rekrutteringsplatformen.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af IT-Forsyningens medarbejdere i forbindelse med ansættelse. Deloitte har stikprøvevist inspiceret dokumentation for, at der er gennemført efterprøvning af medarbejdere i henhold til procedurer. Deloitte har påset, at børne- og straffeattest er gennemgået ved ansættelse for udvalgte stikprøver.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
C.4	Ved ansættelse bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger. Alle medarbejdende er underlagt forvaltningsloven, hvor de automatisk er underlagt fortroligheden.	Deloitte har stikprøvevist inspiceret dokumentation for, at nyansatte medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information.	Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Deloitte har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder deaktiveres eller ophører ved fratrædelse, og at aktiver såsom adgangskort, pc, mobiltelefon mv. inddrages. Deloitte har stikprøvevist inspiceret, at fratrådte medarbejderes rettigheder er blevet deaktiveret eller ophørt, og at aktiver er inddraget.	Ingen afvigelser konstateret.
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.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og deres generelle tavshedspligt. Deloitte har stikprøvevist inspiceret dokumentation for, at fratrådte medarbejdere er blevet orienteret om opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes 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.	Deloitte har inspiceret, at IT-Forsyningen udbyder awareness-træning til medarbejderne i generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Deloitte har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen afvigelser konstateret.

Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige, og at procedurerne er opdateret.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Deloitte har inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner, og forespurgt, om der er foretaget sletning i forbindelse med ophør af aftaler.	Det har ikke været muligt at teste krav omkring opbevaringsperioder og sletterutiner for IT-Forsyningen, da der ikke er udformet specifikke krav til dette i databehandleraftalerne. Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for sletning og tilbagelevering af personoplysninger til den dataansvarlige.	Vi har fået oplyst, at der ikke har været ophør af aftaler frem til erklæringstidspunktet. Ingen afvigelser konstateret.

Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne, og at procedurerne er opdateret. Deloitte har stikprøvevist påset, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalerne.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Deloitte har inspiceret, at IT-Forsyningen har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Deloitte har stikprøvevist inspiceret, at der er dokumentation for, at databehandling, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen eller i øvrigt er godkendt af de dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og 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.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks, og at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Deloitte har inspiceret, at IT-Forsyningen har en samlet og opdateret oversigt over anvendte underdatabehandlere. Deloitte har stikprøvevist inspiceret dokumentation for, at underdatabehandleres databehandling fremgår af databehandleraftalerne eller i øvrigt er godkendt af de dataansvarlige.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Deloitte har stikprøvevist inspiceret dokumentation for, at de dataansvarlige er blevet underrettet ved ændring i anvendelse af underdatabehandlerne.	Ingen afvigelser konstateret.

Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og 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.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Deloitte har inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af IT-Forsyningens oversigt. Deloitte har stikprøvevist inspiceret indgåede underdatabehandleraftaler for at påse, at de indeholder samme krav og forpligtelser, som er IT-Forsyningen er underlagt i databehandleraftalerne med de dataansvarlige.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Deloitte har inspiceret, at IT-Forsyningen har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Deloitte har inspiceret, at oversigten som minimum indeholder de påkrævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Deloitte har forespurgt, hvorvidt der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Deloitte har inspiceret dokumentation for, at der er foretaget en løbende opfølgning af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.	Ingen afvigelser konstateret.

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.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
G.1	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. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. IT-Forsyningen overfører ikke personoplysninger til tredjelande eller internationale organisationer.	Deloitte har 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. Deloitte har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.

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.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for IT-Forsyningens bistand til den dataansvarlige i relation til de registreredes rettigheder, og at procedurerne er opdateret.	Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Deloitte har inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede.	Vi har konstateret, at der - grundet behandlingens karakter - ikke forefindes skriftlige procedurer, som beskriver, hvorledes IT-Forsyningen konkret skal bistå kunderne i forbindelse med overholdelse af kundernes forpligtelser som angivet i kontrolbeskrivelsen. Vi har dog konstateret, at IT-Forsyningen har etableret generelle instrukser og retningslinjer for håndtering af henvendelser fra kunderne. Ingen yderligere afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden, og at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af tilgang til personoplysninger.	Deloitte har inspiceret, at IT-Forsyningen udbyder awareness-træning til medarbejderne i identificering af eventuelle brud på persondatasikkerheden. Deloitte har inspiceret dokumentation for, at netværkstrafik overvåges, og at der sker opfølgning på anormaliteter og overvågningsalarmer. Deloitte har inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger.	Der henvises til kontrol B.7, B.9 og C.7. Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Deloitte har inspiceret, at IT-Forsyningen har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Deloitte har inspiceret registrerede brud på persondatasikkerheden og vurderet, om disse er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 24 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	**IT-Forsyningens kontrolaktivitet**	**Deloittes test**	**Resultat af test**
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Deloitte har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af de sandsynlige konsekvenser ved bruddet på persondatasikkerheden • Beskrivelse af de foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Deloitte har inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.