www.pwc.dk

Unit It

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2022 til 31. december 2022 i henhold til databehandleraftale med dataansvarlige

Januar 2023

pwc

Indholdsfortegnelse

1. Ledelsens udtalelse

Unit IT A/S behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftale.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Unit IT A/S' drifts- og hosting-ydelser, 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.

Unit IT A/S anvender FrontSafe A/S, Microsoft og TOPdesk Danmark som underdatabehandlere for anvendt hosting aktiviteter. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som underdatabehandlere varetager for Unit IT A/S.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos dataansvarlige er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke egnetheden af udformningen og funktionaliteten af disse komplementære kontroller.

Unit IT A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af Unit IT A/S' informationssikkerhed og foranstaltninger i relation til drifts- og hosting-ydelser, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne i hele perioden fra 1. januar 2022 til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan informationssikkerhed og foranstaltninger i relation til drifts- og hosting-ydelser 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 Unit IT A/S' drifts- og hosting-ydelsers afgrænsning 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 drifts- og hosting-ydelser til behandling af personoplysninger foretaget i perioden fra 1. januar 2022 til 31. december 2022

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne drifts- og hosting-ydelser 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 af drifts- og hosting-ydelserne, 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 2022 til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at:

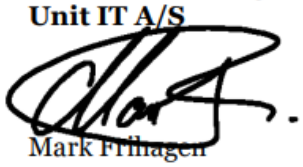
(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

(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 2022 til 31. december 2022.

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 databeskyttelsesreglerne.

Middelfart, den. 6. januar 2023
Unit IT A/S



Mark Frihagen
CEO

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2022 til 31. december 2022 i henhold til databehandleraftale med dataansvarlige

Til: Unit IT A/S og Unit IT A/S' kunder

Omfang

Vi har fået som opgave at afgive erklæring om Unit IT A/S' beskrivelse i afsnit 3 af deres drifts- og hostingydelser i henhold til databehandleraftale med dataansvarlige i hele perioden fra 1. januar 2022 til 31. december 2022 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Unit IT 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 Unit IT 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").

Unit IT A/S anvender FrontSafe A/S, Microsoft og TOPdesk Danmark som underdatabehandlere for anvendt hosting aktiviteter. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som underdatabehandlere varetager for Unit IT A/S.

Enkelte af de kontrolmål, der er anført i Unit IT's beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos dataansvarlige er hensigtsmæssigt udformet og fungerer effektivt sammen med Unit IT's kontroller. Erklæringen omfatter ikke egnetheden af udformningen og funktionaliteten af disse komplementære kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Unit IT A/S' ansvar

Unit IT 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 International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

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 Unit IT 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 gældende i Danmark, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, 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 deres drifts- og hosting-ydelser samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, 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

Unit IT 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 Unit IT A/S' drifts- og hosting-ydelser, 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 Unit IT A/S' drifts- og hosting-ydelser, således som de var udformet og implementeret i hele perioden fra 1. januar 2022 til 31. december 2022, i alle væsentlige henseender er tilfredsstillende præsenteret, 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 2022 til 31. december 2022, 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 2022 til 31. december 2022.

Beskrivelse af test af kontroller

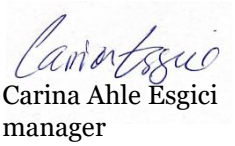
De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Unit IT A/S' drifts- og hosting-ydelser, 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 6. januar 2023
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801



Carina Ahle Esgici
manager

3. Beskrivelse af behandling

Hosting/drift: Formål, hvortil personoplysningerne behandles på vegne af den dataansvarlige.

Formålet med behandlingen er at opbevare data i Unit IT's driftscentre, såkaldt managed services, herunder at sikre stabil drift, maksimal oppetid og håndtere planlagte servicevinduer af de managed services, som leveres til virksomhedens kunder.

Karakteren af behandlingen

Hosting/drift: Behandlingens art

Hosting og opbevaring: Unit IT foretager ikke anden behandling end opbevaring af data. Der sker derfor ikke tilgang til data, herunder læsning eller ændring, medmindre den dataansvarlige anmoder Unit IT herom gennem den standardiserede proces for support/changes.

Personoplysninger

Hosting/drift: Kategorierne af registrerede, hvis personoplysninger behandles af databehandleren, afhænger af de data, som den dataansvarlige opbevarer ved brug af Unit IT's hosting-tjenester.

Kategorier af behandlede personoplysninger

Kategorierne af personoplysninger, der behandles af databehandleren, afhænger af de data, som den dataansvarlige opbevarer ved brug af Unit IT's hosting-tjenester.

I overensstemmelse med databehandleraftalen etableres en basissikkerhed ved at implementere en bred vifte af tekniske og organisatoriske baseline-foranstaltninger (kontroller) af både teknisk og organisatorisk art. Der henvises til nedenstående afsnit 'Praktiske tiltag' for oplysninger om de gældende sikkerhedskontroller.

Praktiske tiltag

A. I overensstemmelse med ISO 27005 udfører databehandleren som minimum en årlig risikovurdering, der evaluerer effektiviteten af nuværende kontroller og desuden vurderer aktuelle trusler og risici.

   En risikobehandlingsplan, der mindsker risici uden for databehandlerens risikoappetit, evalueres af ledelsen. Gældende kontroller udvælges og implementeres for at reducere risici til et acceptabelt niveau.

   Implementering af kontroller godkendes og overvåges af ledelsen i overensstemmelse med 'Informationssikkerhedspolitikken' og i overensstemmelse med Unit IT's Information Security Management System (ISMS).

B. I overensstemmelse med ISO 27001: 5 har den dataansvarlige en 'Informationssikkerhedspolitik', som alle medarbejdere skal følge. Politikken revideres med planlagte intervaller. Politikken styrer ISMS og ansvaret for informationssikkerhed.

C. I overensstemmelse med ISO 27001: 6 har den dataansvarlige implementeret et ledelsessystem (ISMS), der kontrollerer og fører tilsyn med implementeringen og driften af informationssikkerheden.

D. I overensstemmelse med ISO 27001: 6.21 & 6.2.2 har den dataansvarlige en politik for acceptabel brug af sine mobile aktiver og politikker for at arbejde uden for Unit IT's lokationer. Alle medarbejdere skal følge disse politikker. Desuden overvåges og monitoreres alle aktiver af databehandleren.

E. I overensstemmelse med ISO 27001: 7 uddannes databehandlerens medarbejdere løbende i informations- og cybersikkerhedsrelevant viden. Uddannelse er obligatorisk, og progression gennemgås af ledelsen med jævne mellemrum.

F. I overensstemmelse med ISO 27001: 8 ajourfører databehandleren en oversigt over aktiver (CMDB), der identificerer aktiver, den modsvarende kritikalitet og indbyrdes afhængighed. Udvalgte kritiske aktiver overvåges i en SIEM-løsning. Alle kritiske aktiver er risikovurderet i overensstemmelse med afsnit A.

- For at forhindre uautoriseret videregivelse, ændring eller ødelæggelse af den dataansvarliges data, har databehandleren implementeret et sæt strenge politikker og procedurer og adskillige tekniske og organisatoriske kontroller, der sikrer beskyttelse, overvågning og hurtig afhjælpning, hvis en hændelse skulle indtræffe.
- Databehandleren har i overensstemmelse med 8.1.3 en politik, der fastlægger regler for acceptabel brug af sine databehandlingsaktiver.

G. I overensstemmelse med ISO 27001: 9 har databehandleren implementeret kontroller, der sikrer en kontrolleret og samlet tilgang til at administrere og håndhæve brugerrettigheder og adgangsstyring. Dette inkluderer, men er ikke begrænset til:

- Privilegerede brugere kan kun oprettes efter en proces, der følger 4-øjneprincippet (SOD.)
- Brugere tildeles adgang efter en tilgang med mindste privilegier. Forøgelse af adgangsrettigheder kræver godkendelse af nærmeste leder.
- Brugernavn og adgangskode skal følge politikken, der håndhæver kompleksitet og roterende principper.
- Brugerkonti og adgang til systemer gennemgås med jævne mellemrum.
- Adgang til systemer overvåges af en SIEM-løsning, og unormale hændelser advarer sikkerhedsteamet.
- Teknisk adgangskontrol er implementeret på tværs, hvilket sikrer, at systemer er hærdet mod forsøg på at logge på med magt.

H. I overensstemmelse med ISO 27001: 10 har databehandleren implementeret kryptografiske kontroller. Disse kontroller varierer baseret på databehandlerens infrastruktur og opsætning, og hvis data er i transit eller i hvile.

I. I overensstemmelse med ISO 27001: 11 har databehandleren implementeret fysiske og organisatoriske kontroller, der begrænser adgangen til drifts- og bygningsfaciliteter.

- Kun nøglepersoner har adgang til driftsfaciliteter.
- Faciliteter er beskyttet mod uautoriseret adgang af fysiske og logiske kontroller.
- Faciliteter er beskyttet mod brand, lynnedslag, oversvømmelser og naturkatastrofer.
- Faciliteter er bygget i et redundant setup, der sikrer maksimal tilgængelighed i tilfælde af fx strømsvigt (strømafbrydelser, samkøringsafbrydelser osv.).
- Faciliteter er beskyttet mod overspænding i elnettet.
- Faciliteter overvåges 24/7.
- Ovenstående nævnte kontroller (ikke begrænset til) gennemgås af uafhængig instans minimum årligt.

J. I overensstemmelse med ISO 27001: 12 har databehandleren implementeret politikker og procedurer, der sikrer korrekt og sikker drift. Disse kontroller er, men begrænser sig ikke til:

- Dokumenterede operationelle procedurer, der skitserer kontraktlige forpligtelser over for den dataansvarlige.
- En proces for ændringsstyring og godkendelse af databehandleren, før ændringer foretages.
- Beskyttelse mod virus og malware i faciliteter. Hvor databehandleren er ansvarlig for slutbrugerenheder, omfatter dette også bærbare computere, som bruges af databehandleren.
- Sikkerhedskopier foretages med jævne mellemrum, og sikkerhedskopier testes jævnligt.
- Sikkerhedskopier opbevares redundant fysisk væk fra den normale drift.
- Systemer og enheder overvåges, og hvor det er relevant (baseret på aftale med den dataansvarlige), videresendes logge til databehandlerens SIEM-løsning, der advarer sikkerhedspersonale hos databehandlerens sikkerhedsteam.

K. I overensstemmelse med ISO 27001: 13 har databehandleren implementeret en række kontroller, der beskytter netværk og understøtter informationsbehandlingsfaciliteter. Disse kontroller er, men begrænser sig ikke til:

- Netværk og deres udstyr styres og overvåges.
- Firewalls har minimumsregler på IP- og porttrafik (udgangspunkt lukket).
- Netværksudstyr opdateres med jævne mellemrum, eller når producenten frigiver sårbarhedsrettelser for et bestemt mærke/en bestemt model.
- Systemer testes løbende for svagheder og sårbarheder (sårbarhedsscanning).

L. I overensstemmelse med ISO 27001: 14 har databehandleren som en del af kontrollerne nævnt i afsnit J implementeret yderligere kontroller, der sikrer kvalitet i ændringer – ikke kun til systemer, men også håndhævelse af restriktioner for ændringer, der etableres, samt strenge godkendelsesprocesser af enten de dataansvarliges eller databehandlernes CAB.

M. I overensstemmelse med ISO 27001: 15 har databehandleren implementeret en proces, der fører tilsyn med underleverandører og underdatabehandlere. Med processen følger et sæt kontroller, der sikrer, at databehandleren med jævne mellemrum følger op på underleverandørers og underdatabehandleres evne til at overholde de aftalte kontraktlige forpligtelsen. Disse kontroller omfatter, men er ikke begrænset til:

- En årlig indsamling af ISAE'er fra underleverandørens uafhængige tilsyn, hvis det er relevant i forhold til underleverandørens kritikalitet
- En årlig indsamling af underleverandørernes ISO 27001-certifikat, hvis det er relevant i forhold til underleverandørens kritikalitet
- Revision af fysisk lokation mv., hvis det er relevant i forhold til underleverandørens kritikalitet.

N. I overensstemmelse med ISO 27001: 16 har databehandleren implementeret en proces til hændelsesstyring og informationssikkerhedshåndtering. Der er implementeret en bred vifte af kontroller, der sikrer en rettidig, effektiv og konsistent tilgang til hændelser og reaktiv indsats på sikkerhedshændelser eller opståede svagheder.

O. I overensstemmelse med ISO 27001: 17 har databehandleren implementeret et sæt kontroller, der opretholder informations- og cybersikkerheden, hvis der skulle indtræffe en krisesituation. Databehandleren anvender ISO 22301 i sin tilgang til driftskontinuitet. Dette inkluderer planlægning og test af beredskabet efter planlagte intervaller (mindst årligt). Kontroller for ansvar og kommunikation er implementeret og testes med jævne mellemrum.

P. I overensstemmelse med ISO 27001: 18 har databehandleren implementeret et sæt kontroller, der sikrer, at juridiske og kontraktlige forpligtelser gennemgås regelmæssigt, og udvalgte relevante kontroller implementeres for at opfylde kravene. Kontrolelementerne er, men begrænser sig ikke til:

- Organisatorisk ansvar for at vurdere og overvåge databehandlerens kapaciteter er indført.
- Gældende love og regler er blevet identificeret.
- Personhenførbare oplysninger er blevet identificeret, og flere udvalgte kontroller er blevet implementeret for at begrænse, bevare og slette samt beskytte data og analoge informationer.
- Informationssikkerhedskontroller gennemgås årligt af uafhængig instans. I tillæg føres internt tilsyn med informationssikkerheden. Resultater heraf rapporteres direkte til CEO og sikkerhedsudvalg.

Risikovurdering

Unit IT antager selv, at behandlingen af kundernes data omfatter en ikke-defineret mængde data om datasubjekter.

Unit IT's kunder oplyser ikke altid om mængder eller kategorier, samt løbende ændringer hertil, af data, som er personhenførbare, hvorfor Unit IT ud fra følgende kriterier har fastlagt en række baseline-kontroller defineret i ISMS'et.

Det må antages, at data også omfatter mængder af særlige kategorier jf. forordningens artikel 9, som derved skal ydes en særlig beskyttelse.

Unit IT har på baggrund heraf implementeret både almindelige og særlige kontroller, som er beskrevet i databehandleraftalens Anneks III og i ovenstående afsnit 'Praktiske tiltag'.

Til behandlingen af egne data anvender Unit IT en række underdatabehandlere. Omfanget af kategorierne samt underdatabehandlere fremgår af artikel 30-fortegnelsen for personaleadministration.

Unit IT har taget udgangspunkt i, at virksomheder (kunderne) opbevarer persondata i driftscentrene. På baggrund heraf er der etableret et ISMS og herigennem udpeget en række kontroller ud fra ISO 27002-kontrolrammeværket til at nedbringe risici. Kontrollerne er både tekniske og organisatoriske og er udvalgt efter forordningens artikel 32. Kontrollerne er nærmere beskrevet i afsnittet 'Praktiske tiltag'.

Kontrolforanstaltninger

Kontrollerne er både tekniske og organisatoriske og er udvalgt efter forordningens artikel 32. Kontrollerne er nærmere beskrevet i afsnittet 'Praktiske tiltag'.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

Komplementære kontroller hos den dataansvarlige

Som en del af leverancen af ydelserne skal den dataansvarlige implementere visse kontroller, som er vigtige for at nå de kontrolmål, der er anført i beskrivelsen. Disse omfatter:

- Løbende foretage risikovurderinger jf. forordningens artikel 32 og på baggrund heraf orientere Unit IT om yderligere tekniske eller organisatoriske foranstaltninger, som ønskes implementeret
- Orientere Unit IT om ændringer i risici og behandlingen eller kategorierne af data, som kan have indflydelse på typen af behandling, som foretages på vegne af den dataansvarlige.

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	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurerne er opdateret.	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.	Inspiceret, at ledelsen sikrer, at behandlingen af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på seks behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Vi har konstateret, at der ikke er indgået databehandleraftaler med to ud af seks dataansvarlige udtaget til stikprøvetest, hvorfor behandling af data ikke foregår i overensstemmelse med instruks. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

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.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet, i tilfælde hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	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	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på seks databehandleraftaler, at der er etableret de aftalte sikkerhedsforanstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandleren foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandleren har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Inspiceret, at antivirussoftware er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor.	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.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 et 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 stikprøvetest 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. Overvågningen omfatter.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at der ved stikprøvetest 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	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	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. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	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.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold:
	• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
	• Sikkerhedshændelser omfattende:
	  ○ Ændringer i logopsætninger, herunder deaktivering af logning
	  ○ Ændringer i systemrettigheder til brugere
	  ○ Fejlede forsøg på log-on til systemer, databaser og netværk.
	Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.
		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.
		Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.
		Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og sletning.
		Inspiceret ved stikprøvetest 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.
		Inspiceret ved stikprøvetest på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.
			Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.	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.	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.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt til de dataansvarlige i behørigt omfang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Vi har konstateret, at Unit It har en intern Microsoft Windows Server kørende, som ikke længere er supporteret. Vi har ikke ved vores test konstateret yderligere 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.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, herunder om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved stikprøvetest på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved stikprøvetest på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for en regelmæssig – mindst årlig – vurdering og godkendelse af tildelte brugeradgange.	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.	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.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	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	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på seks databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på seks databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved stikprøvetest på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser.	Vi har konstateret, at der ikke er implementeret procedurer for efterprøvning af medarbejdere i forbindelse med ansættelse, herunder vurdering af, hvorvidt der skal ske indhentning af straffeattest, eksamensbeviser og øvrig dokumentation inden ansættelsen af ny medarbejder. Vi har ikke ved vores test konstateret yderligere 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.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.	Inspiceret ved stikprøvetest på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved stikprøvetest på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • 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.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelsen, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Inspiceret ved stikprøvetest på fratrådte medarbejdere i erklæringsperioden, at rettighederne er inaktiveret eller ophørt, samt at aktiverne er inddraget.	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved stikprøvetest på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	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.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	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	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. •	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på seks databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på seksdatabehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysningerne er slettet i overensstemmelse med de aftalte sletterutiner.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
D.3	Ved ophør af behandlingen 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.	Inspiceret, at der foreligger formaliserede procedurer for behandlingen af den dataansvarliges data ved ophør af behandlingen af personoplysninger. Inspiceret ved stikprøvetest på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på seks databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på seks 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.	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 sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	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.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved stikprøvetest 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.	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.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelsen af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændringer i anvendelsen af underdatabehandlerne i erklæringsperioden.	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.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved stikprøvetest på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har konstateret, at to ud af seks databehandleraftaler ikke indeholder en opdateret liste over anvendte underdatabehandlere. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Kontrolmål F:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • 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, tredjelands 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	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	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. Inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved stikprøvetest på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Inspiceret ved stikprøvetest 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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.	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. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	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.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af adgang til personoplysninger.	Inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafikken overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden. Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.	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	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Disse procedurer skal indeholde anvisninger på beskrivelser af: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede anvisninger på: • 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. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.