www.pwc.dk

IT Relation A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2023 til 31. december 2023 i henhold til databehandleraftale med dataansvarlige

Februar 2024

Indholdsfortegnelse

1. Ledelsens udtalelse

IT Relation A/S behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt IT Relation A/S' 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.

IT Relation A/S anvender B4Restore og Keepit som underdatabehandlere for backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore og Keepit varetager for IT Relation 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 hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

IT Relation A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af informationssikkerhed og foranstaltninger i relation til de hosting-ydelser, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne i hele perioden fra 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan informationssikkerhed og foranstaltninger i relation til hosting-ydelserne var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it-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 hosting-ydelsernes 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 hosting-ydelser til behandling af personoplysninger foretaget i perioden fra 1. januar 2023 til 31. december 2023

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne 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 ved 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 2023 til 31. december 2023. 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 2023 til 31. december 2023.

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.

Herning, den 8. februar 2024
IT Relation A/S

Frank Bech Jensen
Head of Compliance and Security

IT Relation A/S

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2023 til 31. december 2023 i henhold til databehandleraftale med dataansvarlige

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

Omfang

Vi har fået som opgave at afgive erklæring om IT Relation A/S' beskrivelse i afsnit 3 af IT Relation A/S' hosting-ydelser i henhold til databehandleraftale med dataansvarlige i hele perioden fra 1. januar 2023 til 31. december 2023 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

IT Relation A/S anvender B4Restore og Keepit som underdatabehandlere for backupydelser. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som B4Restore og Keepit varetager for IT Relation A/S.

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

Vores konklusion udtrykkes med høj grad af sikkerhed.

IT Relation A/S' ansvar

IT Relation 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.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om IT Relation 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 sine 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, hensigtsmæssigheden 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

IT Relation 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 hosting-ydelserne, 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 informationssikkerhed og foranstaltninger i relation til hosting-ydelserne, således som de var udformet og implementeret i hele perioden fra 1. januar 2023 til 31. december 2023, 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 2023 til 31. december 2023, 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 2023 til 31. december 2023.

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 IT Relation A/S' 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, 8. februar 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Iraj Bastar
director

3. Beskrivelse af behandling

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at levere de ydelser, der er aftalt mellem den dataansvarlige og databehandleren. Ydelserne er nærmere defineret i den enkelte kundes kontrakt(er) og ligger inden for områderne hosting og drift, servicedesk, applikationsydelser og konsulentydelser. Den dataansvarliges instruks om databehandling er fastsat i databehandleraftalen mellem partnerne.

Organisationsændringer hos IT Relation, Me'ning & itm8

Den 15. november 2023 meddeler itm8, at virksomheden igangsætter en omfattende virksomhedsfusion, der involverer alle deres selskaber. Dette indebærer konkret, at itm8 fra denne dato begynder processen med at fusionere deres 13 selskaber til en samlet enhed under navnet itm8.

Fusionsprocessen vil blive gennemført i løbet af 2024. På trods af at denne meddelelse er udsendt den 15. november 2023, forventes det ikke at påvirke leverancer, der er blevet revideret i perioden fra 1. januar 2023 til og med 31. december 2023, som er omfattet af denne revisionserklæring.

Den konsoliderede itm8-virksomhed vil på sigt levere alle sine ydelser gennem fire centrale serviceområder:

- Cloud & Infrastructure
- IT Security
- Digital Transformation
- Application Services.

Ved at samle alle aktiviteter under ét fælles itm8 har vi ambitionen om at skabe en ekstraordinær og attraktiv arbejdsplads for de mest kompetente it-specialister. Dette initiativ sigter mod at styrke vores leverancer og service, hvilket vores kunder vil opleve positivt.

Eftersom den reviderede leverance ikke ændres inden for revisionsperioden, vil virksomhederne IT Relation A/S, Me'ning og itm8 fortsat være benævnt i erklæringen, som de plejer.

Yderligere information om itm8's virksomhedsfusion kan findes ved at følge dette link: itm8 unites 13 companies in a major merger

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige vedrører primært:

Hosting og drift

Databehandleren leverer hosting og drift af den dataansvarliges it-systemer og applikationsydelser. Det primære formål med behandlingen af personoplysninger er således hosting, herunder opbevaring af den dataansvarliges personoplysninger, samt daglig drift, herunder overvågning, backup og vedligeholdelse af den dataansvarliges it-systemer, der indeholder personoplysninger.

I særlige situationer kan behandlingen omfatte organisering, strukturering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, hentning, konsultation, brug, sammenstilling, kombination, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med databehandlerens levering af ydelser til den dataansvarlige, eller hvis det er nødvendigt for at efterkomme en konkret anmodning fra den dataansvarlige.

Databehandleren yder it-support til databehandlerens medarbejdere mv. Ethvert arbejde, der udføres af databehandleren som led i denne support, og som omfatter behandling af personoplysninger på vegne af den dataansvarlige, sker på baggrund af en specifik anmodning fra den dataansvarlige.

Servicedesk

Databehandleren yder support til den dataansvarlige i forhold til den dataansvarliges daglige drift af den dataansvarliges it-systemer. På den dataansvarliges anmodning kan databehandleren overtage den dataansvarliges styring af den dataansvarliges it-system på arbejdspladsen eller på servere via TeamViewer eller Remote Desktop i forbindelse med en konkret opgave. Derudover kan databehandleren få adgang til systemer med det formål at udføre fejlfinding og driftsopgaver.

I tilfælde af softwarefejl eller fejl i den dataansvarliges it-system generelt kan databehandleren få databasen fra den dataansvarlige med det formål at udføre fejlfinding, rettelser mv. Dette vil altid ske efter forudgående aftale.

I særlige situationer kan behandlingen omfatte organisering, strukturering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, hentning, konsultation, brug, sammenstilling, kombination, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med levering af de aftalte ydelser, eller hvis det er nødvendigt for at efterkomme en anmodning fra den dataansvarlige.

Applikationsydelser, der leveres af Me'ning

Support, drift, backup og applikationsvedligeholdelse. Følgende applikationer er to af de vigtigste:

- Sepo - Sikker mail leveret af Me'ning. Ydelsen omfatter specifikt:
    - Kryptering/dekryptering/signering/videresendelse af e-mails (og eventuelt digital post (Digital Post)/beskeder i e-postkasser (e-Boks)) til og fra den dataansvarlige
    - Opbevaring af den dataansvarliges kryptografiske nøgle(r).
- TK2 EPJ leveret af Me'ning.

Databehandleren sørger for vedligeholdelse og support af it-systemet TK2 EPJ til den dataansvarlige. Ethvert arbejde, der udføres af databehandleren, og som omfatter behandling af personoplysninger på vegne af den dataansvarlige, sker på baggrund af en specifik anmodning fra den dataansvarlige.

Databehandleren yder support til den dataansvarlige i TeamViewer. På den dataansvarliges anmodning kan databehandleren overtage den dataansvarliges styring af systemet via TeamViewer i forbindelse med en konkret opgave.

I tilfælde af produktfejl kan databehandleren få TK2 SQL-databasen fra den dataansvarlige med det formål at udføre fejlfinding, rettelser mv.

I særlige situationer kan behandlingen omfatte organisering, strukturering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, hentning, konsultation, brug, sammenstilling, kombination, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med levering af de aftalte ydelser, eller hvis det er nødvendigt for at efterkomme en anmodning fra den dataansvarlige.

Konsulentydelser

Databehandleren udfører specifikke og afgrænsede opgaver. Konsulentydelser udføres i den dataansvarliges systemer og på den dataansvarliges data, og behandlingen fastlægges for den enkelte opgave.

Den dataansvarlige anmoder om og fastlægger opgaverne, og databehandleren bistår, i det omfang det er nødvendigt for at sikre en korrekt fastlæggelse af opgaverne.

Personoplysninger

De personoplysninger, som IT Relation behandler på vegne af den dataansvarlige, er forskellige fra kunde til kunde.

Ved indgåelse af en databehandleraftale skal den dataansvarlige sikre, at de korrekte typer af personoplysninger og kategorier af registrerede er defineret i databehandleraftalen.

Praktiske foranstaltninger

Sikkerhedsniveauet skal afspejle et generelt højt sikkerhedsniveau, der afspejler de typer oplysninger, der behandles. Tekniske og organisatoriske foranstaltninger implementeres i henhold til ISO 27001-sikkerhedsstandarden. Alle kontroller fra ISO 27001 er implementeret og overholdt.

Derudover skal sikkerhedsniveauet afspejle de konkret aftalte ydelser i parternes aftale om databehandlerens levering af ydelser til den dataansvarlige.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger der skal træffes for at etablere det aftalte sikkerhedsniveau.

På tidspunktet for aftalens ikrafttrædelse indebærer databehandlerens forpligtelse til at gennemføre sikkerhedsforanstaltninger, at databehandleren skal implementere og opretholde det sikkerhedsniveau, der er beskrevet i dokumenterne "Organisatoriske og tekniske foranstaltninger" og "Fysisk og logisk sikkerhed". Dokumenterne er tilgængelige i databehandlerens kundeportal og på www.itrelation.dk/gdpr-dokumenter. Disse sikkerhedskrav udgør den dataansvarliges samlede krav til sikkerhedsforhold hos databehandleren på baggrund af den dataansvarliges egen risikovurdering.

Risikovurdering

IT Relation arbejder struktureret med risikostyring som en del af ISO 27001-sikkerhedsstandarden. Dette sker gennem risikovurderinger af de implementerede kontroller, databehandling og leverandører (underdatabehandlere).

Risikovurderinger foretages på baggrund af en sandsynligheds-/konsekvensmodel, og relevante og sandsynlige trusler benyttes i vurderingen. På baggrund af vurderingen vil der være trusler, der får en score, der ligger over IT Relations maksimale accept af risiko, og disse trusler vil efterfølgende blive behandlet i en risikoplan for at minimere eller eliminere risikoen.

For leverandører anvendes der en anden vinkel i risikovurderingen. IT Relations erfaring med leverandørens sikkerhed indgår i vurderingen. Denne omfatter en gennemgang af sikkerhedsbrud hos leverandøren samt indhentning og gennemgang af leverandørens revisionserklæring. Hvis leverandøren ikke fremlægger en standardrevisionserklæring, eller hvis der har været alvorlige observationer i erklæringen, sker der opfølgning med tilsyn på baggrund af et kontrolvurderingsskema.

Risikovurderingerne ajourføres regelmæssigt og mindst en gang om året.

Kontrolforanstaltninger

IT Relation har indført følgende kontrolforanstaltninger:

Databehandleraftaler

Der indgås skriftlige databehandleraftaler med både kunder og underleverandører. Aftalen med kunderne bygger på IT Relations standarddatabehandleraftale, som igen bygger på Datatilsynets standardskabelon.

Ved indgåelse af en databehandleraftale med en kunde arkiveres aftalen i IT Relations databehandleraftalesystem. Her registreres også eventuelle afvigelser fra standardaftalen, og det sikres, at aftalen implementeres. Nye kunder skal indgå en databehandleraftale, før IT Relation kan påbegynde behandlingen af kundens data.

Årlig gennemgang af procedurer

En gang om året eller i tilfælde af større ændringer gennemgår IT Relation den gældende standard og indgåede databehandleraftaler for at se, om der er ændringer i fx retningslinjer og procedurer. IT Relation inddrager sin juridiske samarbejdspartner i dette arbejde.

En gang om året bliver leverandørerne undersøgt, gennemgået og risikovurderet. I dette arbejde indhentes revisionserklæringer fra underleverandørerne, og disse skal bygge på gældende standarder. For de leverandører, der ikke har en revisionserklæring, foretages et udvidet tilsyn.

Når IT Relation modtager en GDPR-henvendelse, behandles den ud fra en fast procedure. Det sikres, at den dataansvarlige eller den registrerede får effektiv feedback, og henvendelser behandles inden for 30 dage. GDPR-henvendelsen gemmes i ITSM-systemet.

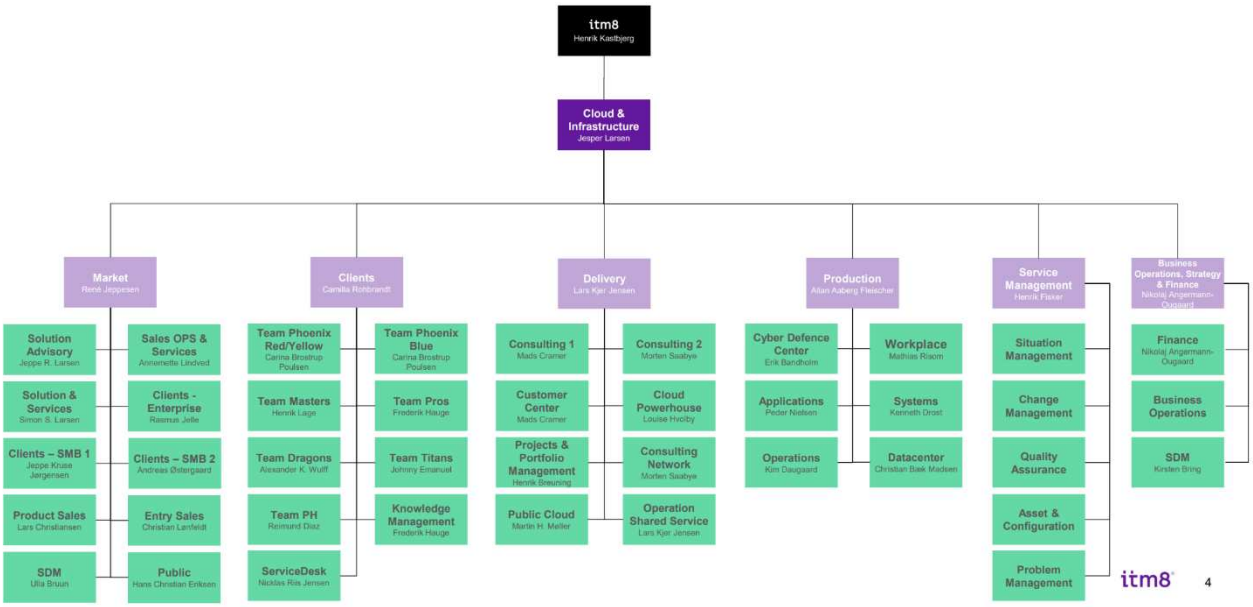
Alle medarbejdere skal have kendskab til aktuelle og relevante politikker, retningslinjer og procedurer. Dette gøres gennem awareness og uddannelse af medarbejdere.

Det sikres, at generelle politikker, retningslinjer, procedurer og sikkerhedsrammer generelt opdateres, når det er nødvendigt, og mindst en gang om året.

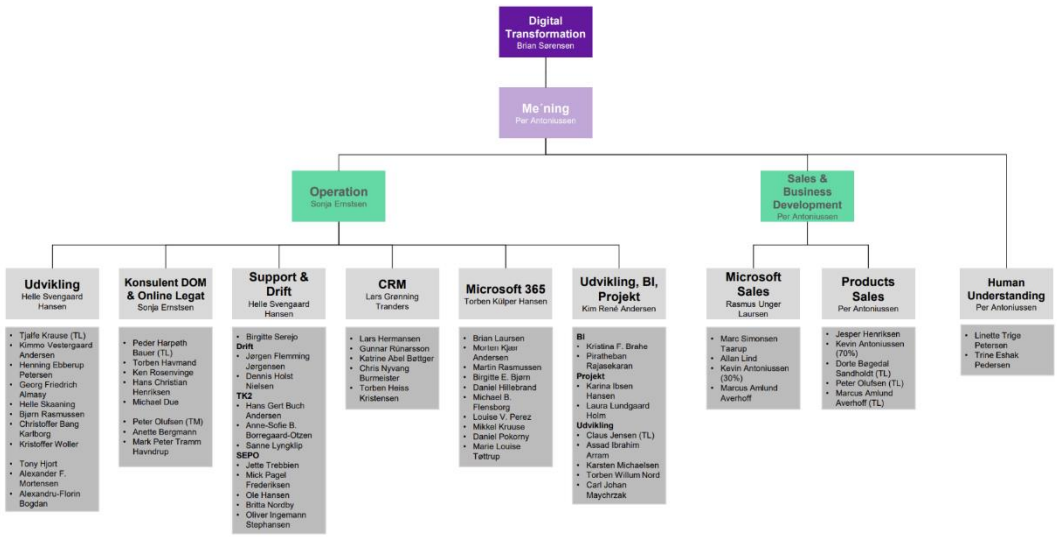
Compliance, roller og ansvar

Ansvaret for it-sikkerhed og compliance ligger hos den øverste ledelse. Den øverste ledelse har uddelegeret opgaven med at stå i spidsen for implementering, kontrol og løbende forbedringer til Group Legal-afdelingen.

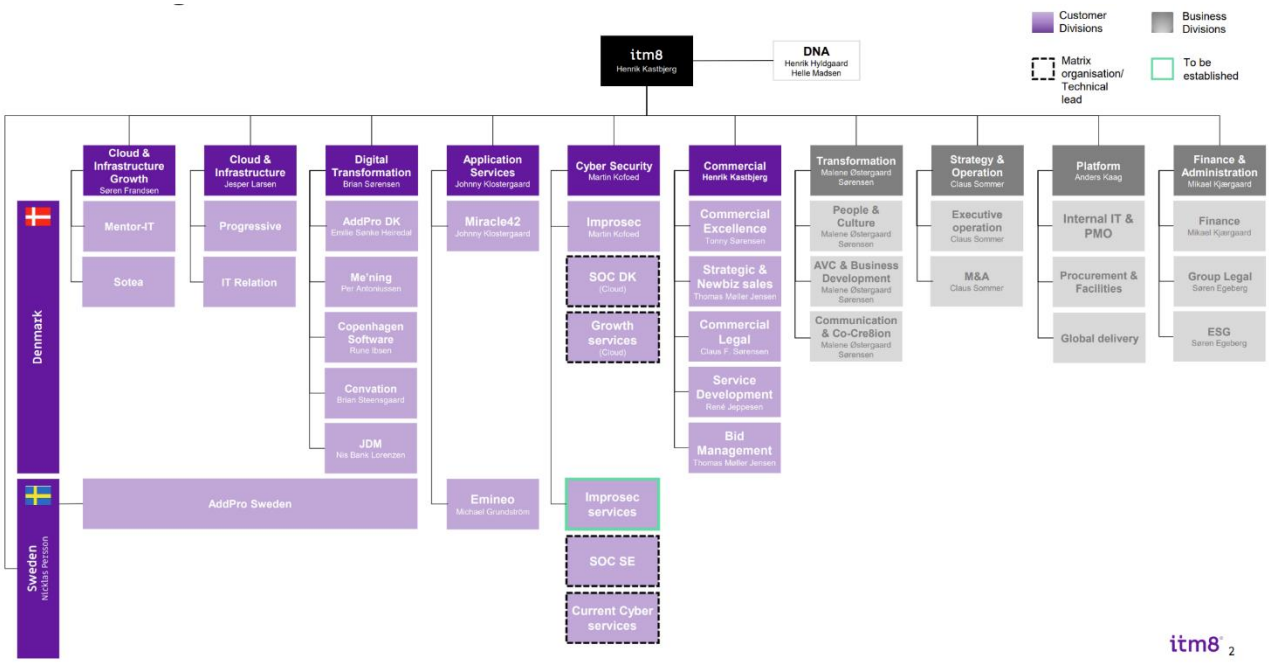
Organisationsplan for IT Relation (i figuren benævnt "Cloud & Infrastructure")



Organisationsplan for Me'ning



Organisationsplan for itm8



Itm8 varetager koncernfunktioner som datacenter, HR, Finance og Compliance and Security.

Compliance and Security informerer medarbejderne om aktuelle relevante sikkerhedstrusler og giver gode råd om bedre it-sikkerhed. Den enkelte medarbejder er ansvarlig for at overholde gældende politikker og retningslinjer, opsøge og følge gældende procedurer og generelt forholde sig proaktivt til sikkerheden. En gang om året eller i tilfælde af større ændringer udvælger sikkerhedschefen stikprøver, som skal vise, om der er kendskab til it-sikkerheden.

Medarbejder-awareness om GDPR

Op til, under og efter implementeringen af GDPR i IT Relation er det løbende blevet kommunikeret til medarbejderne, hvordan man skal håndtere persondata. Selvom det er forholdsvis få medarbejdere, der i deres dagligdag håndterer persondata, så har der været en bred awareness om persondata blandt alle IT Relations medarbejdere.

Alle medarbejdere modtager grundig oplæring i IT Relations informationssikkerhedsregler ved start hos IT Relation samt løbende opdateringer om informationssikkerhedsområdet på IT Relations intranet og nyhedssite.

Der bliver hver måned gjort opmærksom på gældende trusler imod IT Relation via både blogindlæg og opslag hos IT Relation.

Det er medarbejdernes ansvar at overholde de til enhver tid gældende politikker og retningslinjer.

Overvågning

Kun autoriserede brugere har adgang til personoplysninger, og de tildelte brugeradgange er i overensstemmelse med et arbejdsbetinget behov.

Standardbrugerkonti gennemgås mindst en gang om året, og for privilegerede brugere foretages revision i Brugeradministration en gang i kvartalet.

IT Relations adgang til kundesystemer logges. Loggen indeholder oplysninger om tidspunkt, bruger, rettigheder, og til hvilket system der er oprettet forbindelse. Oplysningerne opbevares i mindst seks måneder og slettes derefter.

Følgende skal logges i forbindelse med adgang til personoplysninger:

- Login på administrationsplatformen for at få adgang til kundesystemer
- Login på kundeservere
- Login på udvalgte systemer og tjenester, som IT Relation leverer.

Compliance and Security foretager revision af adgange på baggrund af stikprøver. Dette gøres mindst to gange om året.

Rapportering til ledelsen

Styringen af informationssikkerheden i hele IT Relations organisation koordineres på EMT-møderne (Executive Management Team). Information Security-afdelingen rapporterer løbende til EMT om såvel it- og informationssikkerhed som behandlingssikkerheden i relation til persondata.

EMT træffer beslutninger om IT Relations politikker i relation til sikring af data generelt og sikrer også, at der implementeres de procedurer og instrukser, der er nødvendige for at opnå målsætningen med politikken. EMT vurderer de vedtagne politikker mindst en gang om året.

Overholdelse af GDPR ses som en naturlig del af hverdagen og som en levende del af Information Security Management-systemet hos IT Relation.

Der laves løbende risikovurderinger med EMT på sager af principiel informationssikkerheds- og datasikkerhedsmæssig karakter.

Tilsyn med underdatabehandlere

IT Relation fører regelmæssigt tilsyn med godkendte underdatabehandlere. Dette gøres ved at stille krav om enten it-revisionserklæringer (ISAE 3402 og/eller ISAE 3000) udført af uvildig tredjepart eller ved et aftalt fysisk besøg og efterfølgende revision hos underdatabehandleren. IT Relation stiller krav om at modtage de omtalte ISAE-erklæringer hvert år, og hvis disse ikke modtages, så vil IT Relation ud fra en risikobaseret tilgang gennemføre fysiske besøg hos underdatabehandleren.

IT Relation A/S anvender IT Relation Philippines Inc. og ITM8 Prague s.r.o som underdatabehandlere til at levere services til kunder i tæt samarbejde med den danske organisation. Dette omfatter services indenfor drift, servicedesk, udvikling og konsulentydelser. Herunder bl.a. 24X7-overvågning og -alarmhåndtering.

IT Relation Philippines Inc. og ITM8 Prague s.r.o er 100 % integreret i og styret fra den danske organisation og arbejder derfor også ud fra samme sikkerhedsretningslinjer og instrukser.

IT Relation Philippines Inc. og ITM8 Prague s.r.o anvendes udelukkende til behandling af den dataansvarliges persondata for kunder, som har accepteret disse som underdatabehandler.

Kategorier af persondata, som indsamles, behandles og opbevares

Som databehandler (IT Relation) for den dataansvarlige (kunden) indsamler, behandler og opbevarer IT Relation kun persondata på den dataansvarliges anmodning. Dette forhold og kategorierne af persondata er nærmere aftalt i de specifikke databehandleraftaler, som IT Relation og kunden har indgået.

Det er primært i applikationer (kundesystemer), at der findes kategorier af persondata.

IT Relation har ikke og behøver ikke adgang til disse systemer i forbindelse med fejlrettelse og driftsrelaterede sager.

IT Relation har udarbejdet en liste over interne systemer, hvor persondata behandles og opbevares. Disse opdateres og slettes i takt med ændringer i medarbejderstaben samt i overensstemmelse med overholdelsen af kravene i GDPR og bogføringsloven.

Overførsel til tredjelande

Medmindre andet er aftalt i kundens specifikke databehandleraftale, bliver der ikke sendt data til tredjelande uden for Den Europæiske Union. IT Relation har tre datacentre i Danmark og gør kun brug af public cloud hosting via europæiske noder i vores leverance af public cloud.

Håndtering af sikkerhedsbrud

I tilfælde af et konkret sikkerhedsbrud på et kundesystem og/eller et internt system, hvor der behandles persondata, vil der blive oprettet en sag i IT Relations Service Management-system. Inden for den tidsramme der er aftalt med kunderne, vil IT Relation herefter informere om sikkerhedsbruddets karakter, størrelse og foreløbige omfang mht. et eventuelt brud på persondatasikkerheden hos IT Relation eller hos kunden.

I det omfang IT Relation behandler persondata på vegne af og efter instruks af den dataansvarlige, bistår IT Relation i tilfælde af sikkerhedsbrud på persondata med:

- forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt, senest 72 timer efter at den dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

- forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

- forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko pga. mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

Komplementære kontroller hos de dataansvarlige

De dataansvarlige har følgende forpligtelser:

- At sikre, at personoplysningerne er ajourført

- At sikre, at instrukserne er lovlige set i forhold til den til enhver tid gældende persondataretlige regulering

- At sikre, at instrukserne i databehandleraftalen er korrekte, og kontakte IT Relation, hvis der er behov for ændringer
- At sikre, at typerne af personoplysninger og kategorierne af registrerede er korrekte i databehandleraftalen
- At sikre, at den dataansvarliges brugere bliver gennemgået og har den korrekte adgangsprofil
- At udføre risikoanalyse på de dataansvarliges registrerede
- At foretage revision af deres databehandlere (fx IT Relation)
- Løbende at gennemgå aftalte sikkerhedsforanstaltninger og konfigurationer for kundens miljø og sikre, at de er tilstrækkelige.

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.	Ingen afvigelser noteret.
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 stikprøver på behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.

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 stikprøver på databehandleraftaler, at der er etableret de aftalte sikkerhedsforanstaltninger.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
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 stikprøver på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Vi har ved vores revision noteret, at for udvalgte brugere har proceduren for oprettelse af adgang ikke været efterlevet. Forholdet er udbedret i 2023. Ingen yderligere afvigelser noteret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Brugerlogin • Kritiske indstillinger for systemer og databaser.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret ved stikprøver på alarmer, at der er sket opfølgning og overvågning.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.

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 en stikprøve på logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser.
		Inspiceret ved stikprøver på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.
			Ingen afvigelser noteret.

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. Inspiceret ved en stikprøve på udviklings- og testdatabaser, at personoplysningerne heri er pseudonymiseret eller anonymiseret. Inspiceret ved stikprøver på udviklings- og testdatabaser, hvor personoplysningerne ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.

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 en stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve 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.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
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 stikprøver på databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser noteret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter som udgangspunkt altid straffeattest.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved stikprøver på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved stikprøver på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser.	Ingen afvigelser noteret.

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 en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved stikprøver på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information.	Ingen afvigelser noteret.
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 stikprøver på fratrådte medarbejdere i erklæringsperioden, at rettighederne er inaktiveret eller ophørt, samt at aktiverne er inddraget.	Ingen afvigelser noteret.
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 stikprøver på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Data i kundens systemer og opsætninger i firewalls osv. slettes tidligst en måned efter og senest tre måneder efter aftalens ophør. • Data om kunden i IT Relations' systemer, og hvor IT Relation er dataansvarlig, slettes i henhold til den frist, der er for sletning, i det respektive system.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved stikprøver på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysningerne er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen afvigelser noteret.
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 stikprøver på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen afvigelser noteret.

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 stikprøver på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen afvigelser noteret.
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 stikprøver på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
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 stikprøver 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.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.
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 stikprøver på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser noteret.

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 • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
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 stikprøver på dataoverførsler af personoplysninger, at overførslen sker efter instruks fra den dataansvarlige.	Ingen afvigelser noteret.
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 stikprøver på dataoverførsler af personoplysninger, at disse er vurderet og dokumenteret og der eksisterer et gyldigt overførselsgrundlag.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
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.	Ingen afvigelser noteret.

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.	Ingen afvigelser noteret.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejderne • 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.	Ingen afvigelser noteret.
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 ved vores revision noteret, at enkelte sikkerhedshændelser ikke har været behandlet rettidigt og i overensstemmelse med IT Relations procedurer herfor. Vi har noteret, at proceduren er blevet opdateret efterfølgende justeret. Ingen yderligere afvigelser noteret.

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.	Ingen afvigelser noteret.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Frank Bech Jensen
Kunde
Serienummer: 4ecdf2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c
IP: 93.165.xxx.xxx
2024-02-08 20:24:25 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 83.136.xxx.xxx
2024-02-08 20:30:17 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2024-02-08 21:01:10 UTC