www.pwc.dk

itm8 A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2024 til 31. december 2024 i henhold til databehandleraftale med dataansvarlige

Februar 2025

Indholdsfortegnelse

1. Ledelsens udtalelse

itm8 A/S behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt itm8 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.

itm8 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 itm8 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.

itm8 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 2024 til 31. december 2024. 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 2024 til 31. december 2024

(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 2024 til 31. december 2024. 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 2024 til 31. december 2024.

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 3. februar 2025
itm8 A/S

Frank Bech Jensen
Head of Compliance and Security

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger for perioden fra 1. januar 2024 til 31. december 2024 i henhold til databehandleraftale med dataansvarlige

Til: itm8 A/S og itm8 A/S' kunder

Omfang

Vi har fået som opgave at afgive erklæring om itm8 A/S' beskrivelse i afsnit 3 af itm8 A/S' hosting-ydelser i henhold til databehandleraftale med dataansvarlige i hele perioden fra 1. januar 2024 til 31. december 2024 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om itm8 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 itm8 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").

itm8 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 itm8 A/S.

Enkelte af de kontrolmål, der er anført i itm8 A/S' beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos dataansvarlige er hensigtsmæssigt udformet og fungerer effektivt sammen med itm8 A/S' kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

itm8 A/S' ansvar

itm8 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 itm8 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 hensigtsmæssigheden 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

itm8 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 2024 til 31. december 2024, 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 2024 til 31. december 2024, 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 2024 til 31. december 2024.

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 itm8 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, 3. februar 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Iraj Bastar
director

3. Beskrivelse af behandling

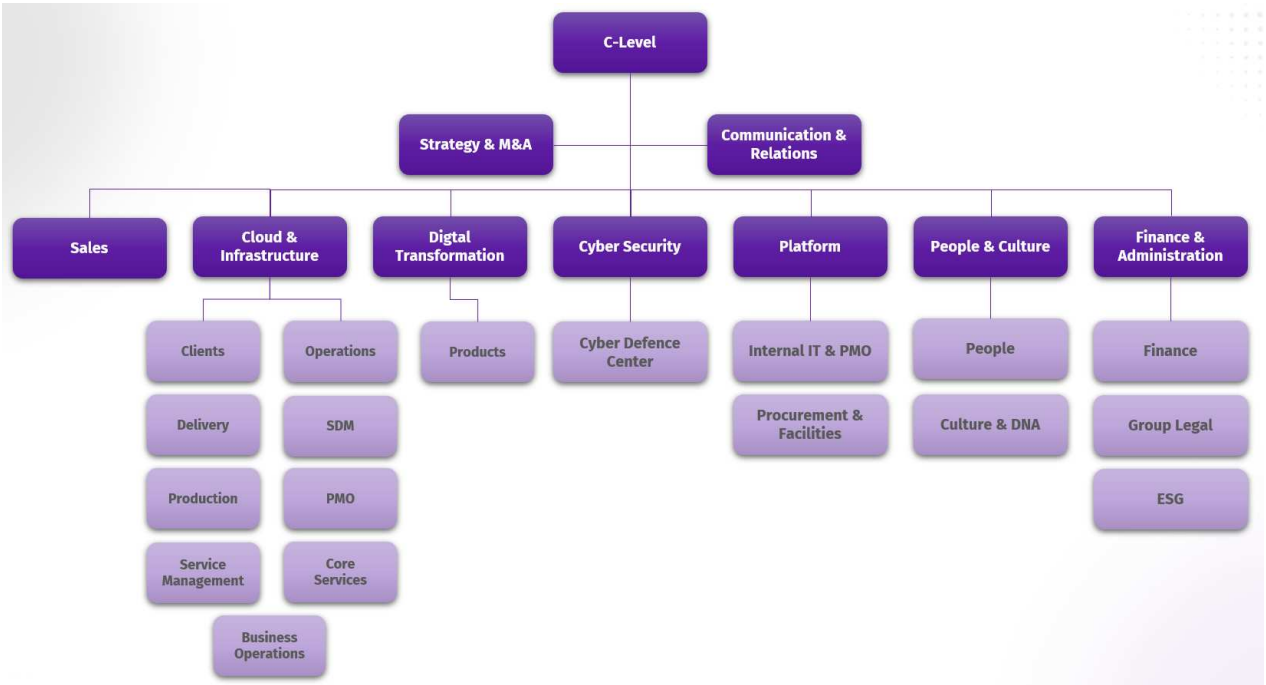
Formålet med databehandlerens aktiviteter i forbindelse med behandling af personoplysning på vegne af dataansvarlige er at levere de aftale ydelse, som er beskrevet i kontrakterne mellem den dataansvarlige og databehandleren. Disse ydelser omfatter hosting og drift, servicedesk, applikationsservices samt konsulentydelser. Instruktionerne for databehandling, som gives af den dataansvarlige, er klart defineret i databehandleraftalen mellem de respektive parter. Denne ramme sikrer, at behandlingsaktiviteterne er i overensstemmelse med de kontraktlige forpligtelser og lovgivningsmæssige krav.

Beskrivelse af serviceorganisationen

itm8 A/S har gennemgået en markant udvikling og er blevet en struktureret organisation, der leverer specialiserede it-tjenester og løsninger. Organisationen er opdelt i flere divisioner, hvor kundeorienterede afdelinger driver serviceleverancer, mens forretningsdivisioner sikrer nødvendig administrativ og operationel støtte. Denne opbygning gør itm8 i stand til at levere integrerede og pålidelige tjenester, der lever op til høje krav inden for kvalitet og compliance til en bred vifte af kunder.

Denne uafhængige revisionserklæring fokuserer på itm8 | Cloud & Infrastructure, som er en central del af erklæringens omfang. Divisionen tilbyder cloud-løsninger og it-infrastrukturtjenester, der lever op til itm8's standarder for sikker og kvalitetsorienteret servicelevering. Rapporten omfatter desuden udvalgte elementer fra itm8 | Cybersecurity, herunder Cyber Defence Center, der spiller en afgørende rolle med 24/7-overvågning, SIEM-loghåndtering og hændelseshåndtering, som alle er kritiske for infrastruktursikkerheden.

Derudover inddrages komponenter fra itm8 | Digital Transformation, særligt Team Products-gruppen, der udvikler skræddersyede løsninger som Send Secure (SEPO) og Tandlægejournal-systemet (TK2). Disse specialiserede løsninger understøtter itm8's forpligtelse til at levere sikre og tilpassede tjenester, der imødekommer kundernes unikke behov.



Omfang af itm8 | Cloud & Infrastructure uafhængig revisorerklæring

Kundedivisioner

De kundeorienterede divisioner udgør itm8's primære serviceområder, hvor hver division er dedikeret til specifikke ekspertiseområder:

- **itm8 | Cloud & Infrastructure**
  Med fokus på cloud-løsninger og it-infrastruktur hjælper denne division kunder med at implementere robuste hosting- og driftsstrategier. Divisionen omsætter kundernes forretningsstrategier til skalerbare cloud- og infrastrukturløsninger gennem platformsevalueringer, design af sikkerhedspolitikker, migrationer, modernisering og 24/7-support.

- **itm8 | Cybersecurity**
  itm8 | Cybersecurity tilbyder omfattende sikkerhedstjenester, der spænder fra penetrationstests og red teaming til rådgivning om cyberrisici. Divisionen inkluderer et Cyber Defence Center, som leverer løbende SIEM-loghåndtering, sårbarhedsvurderinger og realtids-hændelseshåndtering.

- **itm8 | Digital Transformation**
  Denne division driver digital innovation for kunderne og tilbyder ERP-integration, SharePoint og Microsoft-løsninger samt unikke produkter udviklet af Team Products, såsom Send Secure-platformen og Tandlægejournal-systemet (TK2), for at optimere forretningsprocesser.

- **itm8 | Application Services**
  itm8's Application Services-division accelererer udvikling og vedligeholdelse af applikationer med fokus på sikkerhed og kvalitet. Tjenesterne inkluderer applikationsstyring, databaseadministration, overvågning, performanceoptimering og teknisk support.

Forretningsdivisioner

Som støtte til disse kerneområder leverer itm8's forretningsdivisioner—såsom HR, Marketing, Jura, Intern IT og Compliance & Security—en solid base for effektiv servicelevering. Disse divisioner er afgørende for itm8's driftsmæssige integritet og sikrer, at alle kundeorienterede aktiviteter er i overensstemmelse med itm8's standarder og lovgivningsmæssige krav.

Sammen skaber disse divisioner en robust struktur, der gør itm8 i stand til at levere specialiserede højkvalitetstjenester, der understøtter kundernes strategiske mål.

Karakteren af behandlingen

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

Hosting og drift

Databehandleren leverer hosting- og driftstjenester for den dataansvarliges it-systemer og applikationstjenester. Det primære formål med behandlingen af personoplysninger er hosting, herunder lagring af den dataansvarliges personoplysninger samt den daglige drift af it-systemer, der indeholder personoplysninger. Disse aktiviteter omfatter overvågning, backup og vedligeholdelse.

I specifikke tilfælde kan behandlingsaktiviteter omfatte organisering, strukturering, facilitering, midlertidig lagring, filtrering, fejlfinding, tilpasning eller ændring, hentning, konsultation, brug, tilpasning, kombination, begrænsning eller sletning af personoplysninger. Sådanne aktiviteter udføres efter behov for at levere tjenester til den dataansvarlige eller for at imødekomme specifikke anmodninger fra den dataansvarlige.

Databehandleren leverer også it-support til den dataansvarliges medarbejdere og andre relevante parter. Eventuelle supportopgaver, der involverer behandling af personoplysninger på vegne af den dataansvarlige, udføres udelukkende efter specifik anmodning fra den dataansvarlige.

Servicedesk

Databehandleren leverer support til den dataansvarlige i forbindelse med den daglige drift af den dataansvarliges it-systemer. Efter anmodning kan databehandleren påtage sig styring af den dataansvarliges it-

systemer, enten på stedet eller via fjernadgangsværktøjer som TeamViewer eller Remote Desktop, for at udføre specifikke opgaver.

Derudover kan databehandleren få adgang til it-systemer for at udføre fejlfinding og driftsaktiviteter. I tilfælde af softwarefejl eller mere omfattende problemer med den dataansvarliges it-systemer kan databehandleren hente databasen fra den dataansvarlige til fejlfinding, korrektioner eller lignende formål – altid efter forudgående aftale.

I visse situationer kan behandlingsaktiviteter omfatte organisering, strukturering, facilitering, midlertidig lagring, filtrering, fejlfinding, tilpasning eller ændring, hentning, konsultation, brug, tilpasning, kombination, begrænsning eller sletning af personoplysninger. Disse aktiviteter udføres efter behov for at levere de aftale ydelser eller opfylde specifikke anmodninger fra den dataansvarlige.

Applikationsservices

Databehandleren leverer support-, drifts, backup- og applikationsvedligeholdelsestjenester for applikationer, som er udviklet internt. To nøgleapplikationer, der indgår i denne service, er:

SEPO – Sikker Mail

SEPO er en sikker mailapplikation udviklet af databehandleren. Tjenesten omfatter:

- Kryptering, dekryptering, signering og videresendelse af e-mails samt digital post (Digital Post) eller elektroniske postkassemeddelelser (e-Boks) til og fra den dataansvarlige.

- Sikker opbevaring af den dataansvarliges kryptografiske nøgle(r).

TK2 EPJ

TK2 EPJ er et it-system, der ligeledes er udviklet af databehandleren, og som vedligeholdes og understøttes som en del af denne service. Enhver behandling af personoplysninger udføres kun efter specifik anmodning fra den dataansvarlige.

Support leveres via fjernadgangsværktøjer som TeamViewer. Efter anmodning kan databehandleren midlertidigt overtage styringen af systemet via TeamViewer for at løse specifikke opgaver. I tilfælde af produktfejl kan databehandleren indhente TK2 SQL-databasen fra den dataansvarlige til fejlfinding, korrektioner eller lignende formål.

I visse tilfælde kan behandlingsaktiviteter omfatte organisering, strukturering, facilitering, midlertidig lagring, filtrering, fejlfinding, tilpasning eller ændring, hentning, konsultation, brug, tilpasning, kombination, begrænsning eller sletning af personoplysninger. Disse handlinger udføres efter behov for at levere de aftalte tjenester eller opfylde specifikke anmodninger fra den dataansvarlige.

Konsulentydelser

Databehandleren leverer specifikke og afgrænsede konsulentydelser. Disse opgaver udføres inden for den dataansvarliges systemer og involverer behandling af den dataansvarliges systemer og involverer behandling af den dataansvarliges data. Omfanget og karakteren af behandlingsaktiviteterne fastlægges for hver enkelt opgave.

Konsulentopgaver initieres og defineres af den dataansvarlige, hvor databehandleren yder bistand efter behov for at sikre, at opgaverne er korrekt defineret og i overensstemmelse med den dataansvarliges krav.

Persondata

De personoplysninger, som databehandleren behandler på vegne af den dataansvarlige, varierer mellem kunder.

Ved indgåelse af en databehandleraftale er det den dataansvarliges ansvar at sikre, at de relevante typer af personoplysninger og kategorier af registrerede er korrekt defineret i aftalerne.

Praktiske foranstaltninger

Databehandlerens sikkerhedsniveau afspejler generelt en høj standard, der er tilpasset de typer data, der behandles. Tekniske og organisatoriske foranstaltninger er implementeret i overensstemmelse med ISO 27001-rammeværket, hvor alle kontroller under ISO 27001 er fuldt implementeret og overholdt.

Sikkerhedsniveauet er desuden tilpasse de specifikke tjenester, der er beskrevet i aftalen mellem parterne vedrørende databehandlerens levering af tjenester til den dataansvarlige. Databehandleren er både autoriseret og forpligtet til at fastsætte de passende tekniske og organisatoriske sikkerhedsforanstaltninger, der kræves for at opnå det aftalte niveau af datasikkerhed.

Ved aftalens ikrafttræden er det databehandlerens ansvar at implementere og opretholde de sikkerhedsforanstaltninger, der er beskrevet i dokumenterne "Organisatoriske og Tekniske Foranstaltninger" og "Fysisk og Logisk Sikkerhed". Disse dokumenter er tilgængelige via databehandlerens kundeportal og på: legal.itm8.com/compliance

Disse sikkerhedskrav udgør den dataansvarliges samlede forventninger til sikkerhed baseret på den dataansvarliges egen risikovurdering.

Risikostyring

Som en del af ISO 27001-rammeværket anvender databehandleren en struktureret tilgang til risikostyring. Dette inkluderer udførelse af risikovurderinger af implementerede kontroller, databehandlingsaktiviteter og leverandører (underdatabehandlere).

Risikovurderingerne er baseret på en sandsynligheds-/konsekvensmodel, der vurderer relevante og sandsynlige trusler. Trusler, der opnår en risikoscore, som overstiger databehandlerens maksimalt acceptable risikoniveau, håndteres gennem en risikobehandlingsplan med det formål at minimere eller eliminere den tilknyttede risiko.

For leverandører anvendes en ekstra vurderingsdimension i risikovurderingerne. Databehandleren inddrager erfaringer med leverandørens sikkerhed, herunder en evaluering af tidligere sikkerhedsbrud og en gennemgang af leverandørens revisionserklæring. Hvis leverandøren ikke leverer en standardiseret revisionserklæring, eller hvis der identificeres væsentlige fund, foretages opfølgning via en kontrolvurdering og, om nødvendigt, gennem tilsyn.

Risikovurderingerne gemmes og opdateres regelmæssigt, mindst én gang om året.

Der har ikke været væsentlige ændringer til procedurer og kontroller i perioden fra 1. januar 2024 til 31. december 2024.

Kontrolforanstaltninger

itm8 A/S har implementeret de følgende kontrolforanstaltninger:

Databehandleraftaler

Databehandleren indgår skriftlige databehandleraftaler med både kunder og underleverandører. Aftaler med kunder er baseret på databehandlerens standardaftale, som er udarbejdet med udgangspunkt i Datatilsynets standardaftaleskabelon.

Når der indgås en databehandleraftale med en kunde, arkiveres den i databehandlerens aftalestyringssystem. Eventuelle afvigelser fra standardaftalen dokumenteres i dette system, og implementeringen af aftalen sikres. Nye kunder skal underskrive en databehandleraftale, før databehandleren påbegynder behandling af deres data.

Årlig gennemgang af procedurer

Databehandleren foretager en årlig gennemgang af gældende standarder og etablerede databehandleraftaler, eller når der sker væsentlige ændringer. Denne gennemgang vurderer opdatering til retningslinjer og procedurer med input fra databehandlerens juridiske samarbejdspartner.

Som en del af processen inspiceres, gennemgås og risikovurderes leverandører årligt. Revisionserklæringer baseret på gældende standarder indhentes fra underleverandører. For leverandører, der mangler en revisionserklæring, gennemføres der udvidet tilsyn.

Når databehandleren modtager en GDPR-forespørgsel, håndteres den i henhold til en foruddefineret procedure. Forespørgslen behandles inden for 30 dage for at sikre effektiv tilbagemelding til den dataansvarlige eller den registrerede. Disse forespørgsler dokumenteres i IT Service Management (ITSM)-systemet.

Compliance, roller og ansvar

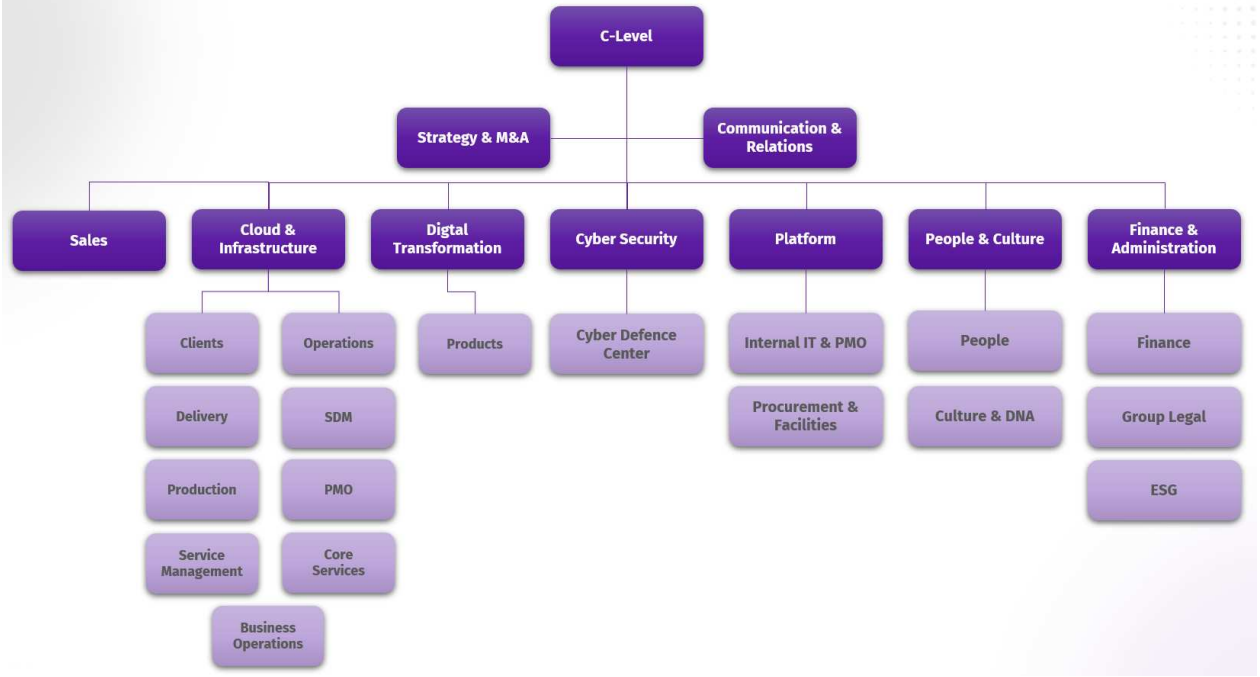
Ansvar for informationssikkerhed og compliance hos itm8 er forankret på ledelsesniveau. Topledelsen fastlægger den strategiske retning og sikrer, at den er i overensstemmelse med itm8's forpligtelser til kvalitet og lovgivningsmæssige standard. Compliance & Security-afdelingen, der arbejder under delegation fra ledelsen, har ansvaret for at overvåge implementeringen, kontrol og løbende forbedring af informationssikkerhed og compliance på tværs af organisationen.

Itm8 er organiseret i specialiserede divisioner, der omfatter både kundeorienterede og forretningsstøttende funktioner. De kundeorienterede divisioner inkluderer:

- itm8 | Cloud & Infrastructure
- itm8 | Cybersecurity
- itm8 | Digital Transformation.

Disse divisioner leverer skræddersyede it-tjenester, samtidig med at de overholder itm8's høje standarder for sikker og compliant serviceleverance. Forretningsunderstøttende divisioner som HR, Compliance & Security og Intern IT sikrer, at de grundlæggende politikker, procedurer og rammeværk er på plads for at opretholde organisatorisk integritet og sikkerhed.

Gennem denne struktur sikrer Compliance & Security-afdelingen, at itm8 opretholder en sammenhængende tilgang til risikostyring, lovgivningsmæssigt overholdelse of informationssikkerhed. Samtidig leverer afdelingen løbende vejledning og overvågning for at opfylde organisationens og kundernes krav. Medarbejdere på tværs af alle divisioner har ansvar for at overholde politikkerne og bidrage proaktivt til et sikkert miljø.



Omfang af itm8 | Cloud & Infrastructure uafhængig revisorerklæring

Awareness-træning i relation til GDPR

itm8 prioriterer at fremme medarbejdernes viden om GDPR-compliance på tværs af organisationen. Selvom kun en del af medarbejderne regelmæssigt håndterer personoplysninger, sikrer itm8, at alle ansatte er informerede om korrekt datahåndtering.

Nyansatte modtager træning i itm8's informationssikkerhedspolitikker som en del af deres onboarding-proces. Opdateringer leveres regelmæssigt via interne kommunikationskanaler, herunder intranet og nyhedsplatforme. Løbende awareness-initiativer såsom blogindlæg og plakater fremhæver aktuelle sikkerhedstrusler og styrker de bedste praksisser for databeskyttelse.

Medarbejdere har til ansvar at overholde itm8's politikker og retningslinjer og bidrage til organisationens forpligtelse til at beskytte persondata.

Overvågning

Adgang til persondata er begrænset til autoriserede brugere baseret på et arbejdsrelateret behov. Brugeradgangsrettigheder gennemgås årligt for standardkonti, mens kvartalsvise revisioner gennemføres for privilegerede konti.

Al adgang til kundesystemer fra itm8's personale logges, hvor der fanges detaljer såsom tidsstempel, bruger, privilegier og det system, der blev tilgået. Disse logge opbevares i mindst seks måneder, før de bliver slettet sikkert. Logningskravene omfatter:

- Login til administrationsplatform for adgang til kundesystemer
- Login til kundeservere
- Login til specifikke systemer og tjenester leveret af itm8.

User Management-afdelingen gennemfører flere revisioner i løbet af året for at sikre overholdelse af adgangskontrolpolitikkerne.

Rapportering til ledelsen

Executive Management Team (EMT) har ansvaret for informationssikkerhed på tværs af itm8 og sikrer, at der er overensstemmelse med organisatoriske mål og lovgivningskrav. Compliance & Security-afdelingen

leverer regelmæssigt rapporter til EMT om it-sikkerhed, informationssikkerhed og håndtering af persondata.

EMT er ansvarlig for itm8's datasikkerhedspolitikker, og Compliance & Security er ansvarlig for at sikre, at nødvendige procedurer og instruktioner implementeres for at opfylde målene i politikkerne. Disse politikker gennemgås mindst én gang årligt for at opretholde relevans og effektivitet.

Risikovurderinger af kritiske informationer og datasikkerhedsforhold gennemføres løbende i samarbejde med EMT og integrerer GDPR-compliance som en kernekomponent itm8's informationssikkerhedsstyringssystem.

Tilsyn med underdatabehandlere

itm8 sikrer, at godkendte underdatabehandlere overholder sikkerheds- og lovgivningskrav gennem regelmæssig overvågning. Dette inkluderer indhentning af årlige it-revisionserklæringer såsom ISAE 3402 eller ISAE 3000 udført af uafhængige tredjeparter. Hvis disse erklæringer ikke leveres, anvender itm8 en risikobaseret tilgang og gennemfører on-site-revisioner for at verificere overholdelse.

itm8 anvender sine datterselskaber, itm8 Phillipines INC og itm8 Prague S.R.O, som underdatabehandlere for at støtte servicelevering i samarbejde med den danske organisation. Disse enheder håndterer tjenester såsom drift, servicedesk-support, udvikling og rådgivning, herunder 24/7 overvågning og alarmhåndtering.

itm8 Philippines Inc. og itm8 Prague S.R.O er 100 % integreret og styres fra den danske organisation og følger de samme sikkerhedsguidelines og instruktioner.

itm8 Philippines Inc. og itm8 Prague S.R.O bruges udelukkende til behandling af dataansvarliges persondata for kunder, der har accepteret disse underdatabehandlere.

Kategorier af persondata, som indsamles, behandles og opbevares

Som databehandler for kunden (den dataansvarlige) indsamler, behandler og opbevarer itm8 persondata udelukkende efter kundens anvisning. Disse forhold og de specifikke kategorier af persondata er beskrevet i de databehandleraftaler, itm8 indgår med sine kunder. De primære kategorier af persondata håndteres i kundens applikationer og systemer. itm8 kræver ikke adgang til disse systemer for fejlretning eller operationelle opgaver.

itm8 opretholder en liste over interne systemer, hvor persondata behandles og opbevares. Denne liste opdateres regelmæssigt for at afspejle ændringer i arbejdsstyrken og sikre overholdelse af kravene i GDPR og den danske Bogføringslov. Persondata slettes, så snart de ikke længere er nødvendige i overensstemmelse med disse regler.

Overførsel til tredjelande

Medmindre andet er angivet i kundens specifikke databehandleraftale, vil persondata ikke blive overført til tredjelande uden for Den Europæiske Union. itm8 benytter kun sine datacentre i Danmark til opbevaring og behandling. Til offentlige cloudtjenester anvender itm8 udelukkende europæiske noder, hvilket sikrer overholdelse af europæiske databeskyttelseskrav.

Håndtering af sikkerhedsbrud

I tilfælde af et sikkerhedsbrud, der involverer et kundesystem eller et internt system, hvor persondata behandles, vil der blive åbnet en sag i itm8's service management-system. itm8 vil underrette kunden inden for den aftale tidsramme om arten, omfanget og den foreløbige vurdering af bruddet. Hvis itm8 behandler persondata på vegne af og i henhold til instrukser fra dataansvarlige, vil itm8 bistå med at påtage sig følgende ansvar:

- At underrette Datatilsynet om et persondatabrud uden unødig forsinkelse, og hvor det er muligt, senest 72 timer efter, at bruddet er blevet opdaget, medmindre det er usandsynligt, at bruddet medfører en risiko for fysiske personers rettigheder og friheder

- At informere de registrerede uden unødig forsinkelse, hvis bruddet indebærer en høj risiko for deres rettigheder og friheder

- At konsultere Datatilsynet før behandlingen, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandling kan medføre en høj risiko på grund af de foranstaltninger, som dataansvarlige har truffet for at afbøde denne risiko.

Kontrolmål og -aktiviteter fremgår detaljeret i afsnit 4.

Komplementære kontroller hos de dataansvarlige

De dataansvarlige har følgende forpligtelser:

- Sikre, at persondata er opdateret

- Sikre lovligheden af instruktioner i overensstemmelse med gældende privatlivsreguleringer

- Gennemgå og bekræfte, at instruktionerne i databehandleraftalen er korrekte og kontakte itm8, hvis ændringer er nødvendige

- Sikre, at de persondata, der behandles, samt kategorierne af registrerede, er præcist angivet i databehandleraftalen

- Sikre, at dataansvarliges brugere regelmæssigt bliver gennemgået og har de korrekt adgangsprofiler

- Udføre risikoanalyser af de registrerede hos dataansvarlige

- Foretage revisioner af deres databehandlere, herunder itm8

- Løbende gennemgå de aftalte sikkerhedsforanstaltninger og konfigurationer for kundens miljø for at 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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.	Ingen 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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.	Vi har noteret at 2 Domain Controller ikke har været opdateret/patched jf. godkendte procedure. Vi har modtaget dokumentation efterfølgende at begge servere er opdateret med de seneste opdateringer. Ingen yderligere 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 itm8's systemer, og hvor itm8 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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 afvigelse 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.	. 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.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 afvigelse noteret.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, 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
2025-02-03 20:06:04 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-03 20:19:00 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 83.136.xxx.xxx
2025-02-03 20:20:08 UTC