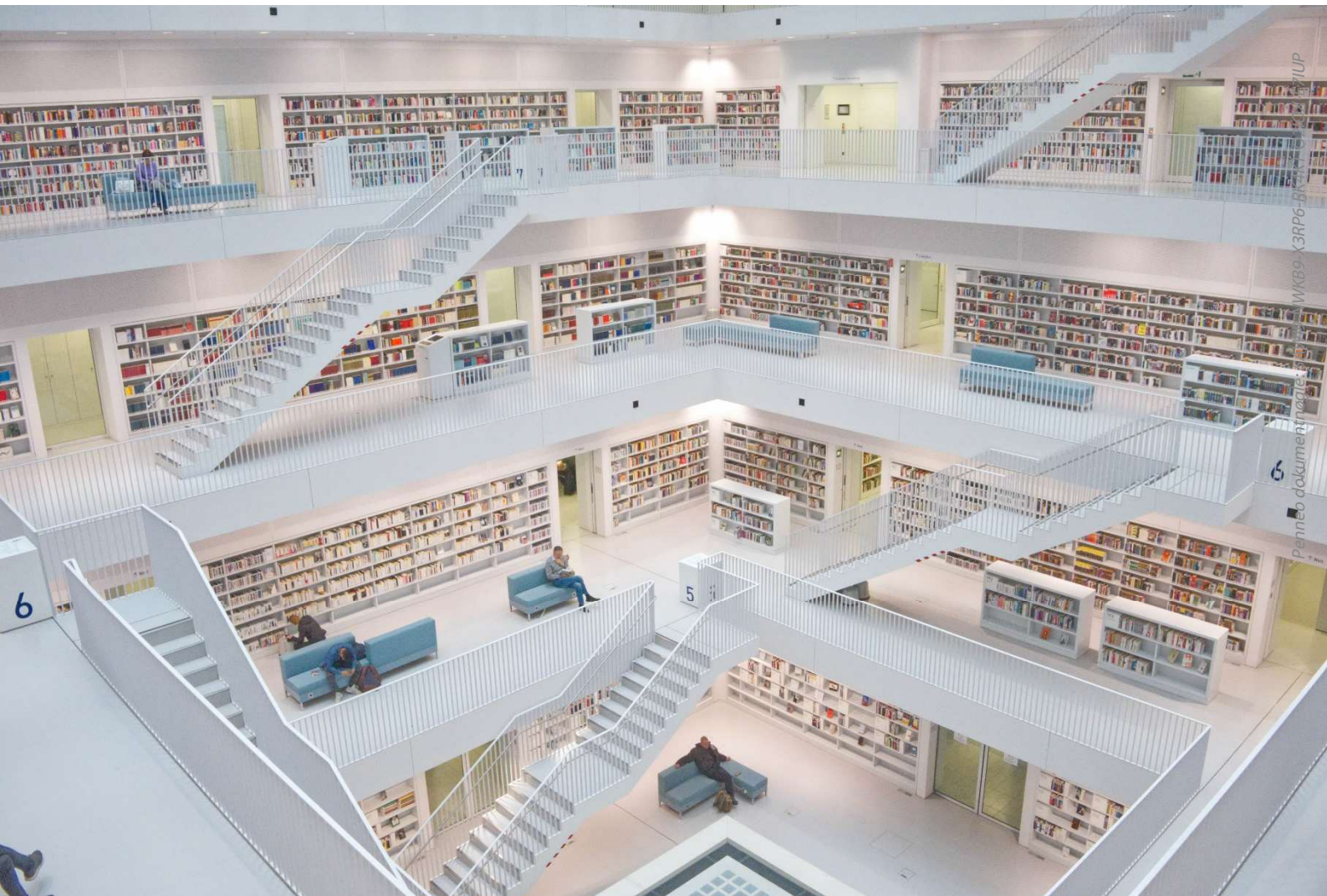


ISAE 3000, type 1

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger pr. 26. maj 2026



COMPENT

Indhold

1. Ledelsens udtalelse	1
2. Beskrivelse af behandling	3
3. Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger	6
4. Kontrolmål, kontrolaktiviteter, test og resultat heraf	8

S.nr. 302452

RLS/JR

Penneo dokumentnøgle: 5AWI9-NWKB9-X3RP6-RK4K1-O2IOX-E7IUP

1. Ledelsens udtalelse

Compent ApS varetager behandling af personoplysninger på vegne af vores kunder, der er dataansvarlige i henhold til indgåede databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Compent ApS' generelle driftsydelser, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter kaldet "databeskyttelsesforordningen") er overholdt.

Compent ApS bekræfter, at:

- a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Compent ApS' generelle driftsydelser, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 26. maj 2026. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
 - (i) Redegør for, hvordan Compent ApS' systemer var udformet og implementeret, herunder redegør for:
 - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
 - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
 - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
 - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
 - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
 - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrede
 - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger 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 har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
 - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

- (ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne ydelse 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 ydelsen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.
- b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 26. maj 2026. 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.
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

København, den 26. maj 2026
Compent ApS

Jeppe Basse
Administrerende direktør

2. Beskrivelse af behandling

Kort intro om Compent

Compent er et dansk it-konsulenthus med speciale i udvikling, integration og vedligeholdelse af komplekse webløsninger og digitale platforme. Virksomheden fungerer som en teknisk samarbejdspartner, der hjælper organisationer med at omsætte forretningsbehov til stabile og skalerbare it-systemer. Compents kernekompetencer omfatter softwareudvikling, systemarkitektur og løbende teknisk support, hvor der lægges vægt på høj kodekvalitet og tæt dialog med kunden.

Beskrivelse af ydelser

Formålet med Compents (databehandlerens) behandling af personoplysninger på vegne af den dataansvarlige er:

- **Systemudvikling og konfiguration:** Udvikling af ny funktionalitet eller ændringer i eksisterende systemopsætning efter anmodning fra den dataansvarlige.
- **Vedligeholdelse og teknisk support:** Fejlfinding, optimering og løbende teknisk vedligeholdelse af den dataansvarliges it-løsninger, hvor adgang til persondata kan være nødvendig for at løse specifikke opgaver. Ved adgang til persondata foretages dette af en medarbejder med fysisk placering inden for EU.
- **Ad hoc-fejlretning:** Midlertidig adgang til applikationsdata i forbindelse med diagnosticering og udbedring af driftsforstyrrelser efter instruks.

Beskrivelse af aftaleforhold mellem parterne:

Compent yder teknisk bistand og it-konsulentytelser under gældende konsulent- og databehandleraftaler. Det præciseres, at Compent ikke agerer hosting- eller storage-leverandør for løsninger med følsomme personoplysninger. Al persondata opbevares på servere, som administreres af kunden eller en tredjepart inden for EU. Compents behandling af data er afgrænset til den tekniske adgang, der kræves for fejlfinding og service, med det formål at understøtte stabil drift og løbende udvikling.

Karakteren af behandlingen

Al persondata anonymiseres ved udvikling i både udviklings-, test- og staging-miljøer. Persondata tilgås kun i følgende sammenhænge:

- Fremsendelse af eksempler og data fra kunde til Compent uden forudgående anonymisering.
- Almindelige persondata som navn, efternavn, e-mail og telefonnummer, som udveksles via e-mail i forbindelse med opgaver eller fejlsøgning.
- Fejlsøgning i livemiljø.
- Præsentation i livemiljø hos kunden.

Praktiske tiltag

Compent har placeret ansvaret og organiseringen af informationssikkerheden hos de øverste sikkerhedsansvarlige, som er Compents CTO og CEO. Det er dermed de øverste sikkerhedsansvarliges opgave at udarbejde, implementere og kontrollere interne procedurer og databeskyttelsespolitikker.

For at sikre, at Compent lever op til IT-sikkerhedspolitikken samt de krav, der stilles i Compents databehandleraftaler, har Compent implementeret en onboarding-proces, som sikrer, at alle medarbejdere har læst og forstået politikkerne. I sammenhæng med dette skal alle medarbejdere hvert år gennemføre en række kurser under vores awareness-program, som udbydes af vores samarbejdspartner ComplyCloud.

Der arbejdes målrettet på at sikre fortrolighed, integritet og tilgængelighed i vores løsninger, og vi arbejder kontinuerligt for at sikre et passende sikkerhedsniveau, således at kvaliteten i vores produkter lever op til både Compents, vores kunders og de registreredes krav og behov.

Nedenstående tiltag er implementeret med henblik på at sikre et passende sikkerhedsniveau, men er ikke begrænset hertil:

- Informationssikkerhedspolitik
- Privatlivspolitik
- NDA og fortrolighedserklæring underskrevet ved ansættelse
- IT-sikkerhedshåndbog
- IT-sikkerhedsretningslinjer
- Change Management
- Incident-rapportering
- Awareness-træning

Compents medarbejdere er løbende informeret om ovenstående tiltag og ændringer til politikker og bliver testet årligt gennem awareness-træning, som bliver registreret centralt.

Vi har en centraliseret og differentieret adgangs- og rettighedsstruktur til at styre adgang til kildekode i alle miljøer, som er styret centralt via Microsoft-rettighedstildeling i Office 365 Entra ID. Udviklet software sættes i drift maskinelt via en CI (Continuous Integration)-pipeline, som sikrer, at vejen fra udvikling til test, staging og produktion følger en ensartet og sikker måde, der ikke kræver menneskelig involvering omkring data og minimerer fejl.

Compent har en informationssikkerhedspolitik, der beskriver medarbejdernes forpligtelser relateret til at levere vores konsulentytelser. Denne beskriver initiativerne og retningslinjerne for sikker behandling af personoplysninger samt generel sikker behandling af IT. Som led i den løbende indsats for at styrke anvendelsen er der udarbejdet politikker, vejledninger og retningslinjer for håndtering af blandt andet IT, persondata, hardware, services og anvendelse af AI.

Compents retningslinjer omfatter blandt andet:

- Krav om kryptering af fortrolige oplysninger.
- Krav om anvendelse af antivirus/anti-malware.
- Kun sporbar adgang til data og kode via personlig konto.
- Anvendelse af MFA autentificering, hvor muligt.

Informationssikkerhedspolitikken opdateres jævnligt og fremsendes til Compents medarbejdere ved væsentlige ændringer og opdateringer.

Herudover er alle systemer risikovurderet administrativt – og teknisk er der foretaget tiltag med henblik på, at der er en passende grad af sikkerhed i forhold til det enkelte systems risikoprofil.

Der udføres jævnligt kontrol af medarbejdernes rettigheder for dermed at sikre, at medarbejdere kun har adgang til relevante systemer.

Ved ansættelse af nye medarbejdere vurderer Compent altid behovet for baggrundstjek fra ansættelse til ansættelse, og dette kan omfatte:

- Referencer fra tidligere ansættelser
- Eksamenspapirer
- Straffeattest

Der indhentes som udgangspunkt altid eksamenspapirer, mens referencer og straffeattest kan indhentes, hvis det vurderes, at der er et behov. Alle medarbejdere hos Compent er underlagt tavshedspligt, som medarbejdere ved fratrædelse også bekræfter er gældende skriftligt.

Risikovurdering

Compent vurderer løbende konsekvenserne for de registrerede i forhold til fortrolighed, integritet og tilgængelighed ved behandling af personoplysninger i forbindelse med levering af en konsulentydelse. Herudover evaluerer vi løbende alle de systemer, vi er ansvarlige for leverancen af, i forhold til at sikre en passende grad af sikkerhed.

Compent arbejder kontinuerligt med IT-sikkerhed og holder sig orienteret om potentielle trusler. Compents primære sikkerhedsprincipper baserer sig på OWASP Top 10, som vi altid følger, samt Zero Trust-modellen ved implementering af systemer.

Compent foretager indledningsvis og løbende risikovurderinger af sine underdatabehandlere og indhenter så vidt muligt en erklæring fra disse for at opretholde en høj grad af sikkerhed for de registrerede.

Ved leverancer af konsulentytelser er Compent databehandler, og kunden er dataansvarlig. Compent understøtter den dataansvarliges forpligtelser til håndtering af de registreredes rettigheder – herunder f.eks. besvarelse af anmodning om indsigt eller rettet mod at blive glemt.

Kontrolforanstaltninger

Compent vurderer løbende, hvilke praktiske sikkerhedstiltag der skal indgå i de løsninger, vi udvikler. Vi forholder os til aktuelle trusler og mulige afværgende tiltag, ligesom vi løbende vurderer nye typer af sikkerhedsforanstaltninger for at sikre, at vi kontinuerligt tilpasser vores arbejde med sikring af data.

Der er implementeret en change- og release-log på alle vores releases for at registrere og dokumentere alle ændringer foretaget på de systemer, vi har ansvar for, samt for at kunne lokalisere fejl og identificere eventuelle sikkerhedsbrister.

Der er etableret en automatisk proces, som scanner Compents løsninger for kendte sikkerhedshuller og automatisk notificerer den ansvarlige for hurtig patching/udbedring. Vi anvender, hvor det er nødvendigt, kryptering og har firewall, antivirussystemer og logging på vores miljøer.

Adgang til Compents interne systemer er i videst muligt omfang beskyttet med MFA autentificering eller IP-restriktion og centraliseret med løbende overvågning for angreb. I vores test-, udviklings- og staging-miljøer har vi en automatiseret proces til anonymisering af persondata.

Compent har implementeret kontroller (via ComplyCloud) til indhentelse af erklæringer fra underdatabehandlere i forhold til overholdelse af persondatalovgivningen. Kontrollerne sikrer, at alle erklæringer vurderes ud fra et sikkerhedsperspektiv.

Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige er selv ansvarlig for at anvende Compents ydelser på en måde, der er i overensstemmelse med lovgivningens krav.

Dette omfatter blandt andet, at kunden, som er dataansvarlig, er ansvarlig for:

- At den fornødne hjemmel til behandlingen, jf. art. 6, er til stede.
- At sikre fornøden oplysning til de registrerede omkring udøvelsen af deres rettigheder og kontrollere identiteten af de registrerede, der ønsker at udøve deres rettigheder.
- At behørigt orientere den registrerede i henhold til art. 13.
- At kontrollere identiteten på den, der anmoder om berigtigelse eller sletning.
- At sikre, at instruksen til Compent er lovlige i forhold til den til enhver tid gældende databeskyttelsesretlige regulering.
- At sikre, at instruksen er hensigtsmæssig i forhold til denne databehandleraftale og hovedydelsen.
- At sikre, at udøvelsen af den registreredes rettigheder sker rettidigt, herunder besvarelse af den registreredes anmodninger.

At eventuelle integrationer til andre systemer overholder den gældende lovgivning.

3. Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger

Til ledelsen hos Compent ApS og deres kunder

Omfang

Vi har fået som opgave at afgive erklæring om Compent ApS' beskrivelse i afsnit 2 af generelle driftsydelser til behandling af personoplysninger i henhold til databehandleraftaler med dataansvarlige, pr. 26. maj 2026 (beskrivelsen) og om udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Compent ApS' ansvar

Compent ApS 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, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisors etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Inforevision 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 Compent ApS' beskrivelse samt om udformningen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, *Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger* og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin ydelse samt for kontrollerens udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i afsnit 1.

Som nævnt har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Begrænsninger i kontroller hos en dataansvarlig

Compent ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved ydelsen, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

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 i afsnit 1. Det er vores opfattelse,

- (a) at beskrivelsen af generelle driftsydelser, således som denne var udformet og implementeret pr. 26. maj 2026, i alle væsentlige henseender er retvisende, og
- (b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 26. maj 2026.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests 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 Compent ApS' ydelse, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Søborg, den 26. maj 2026

inforevision

statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
statsautoriseret revisor

Simon Okkels
Partner, Lead IT-auditor (CISA)

4. Kontrolmål, kontrolaktiviteter, test og resultat heraf

4.1 Formål og omfang

Vores arbejde er udført i overensstemmelse med ISAE 3000, *Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger*.

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Compent ApS har implementeret. Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, som vi har vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål har været opnået pr. 26. maj 2026.

Denne erklæring er afgivet efter den partielle metode, og omfatter ikke kontrolmål og tilknyttede kontroller hos Compent ApS' underleverandører og underdatabehandlere.

Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Compent ApS' kunder er ikke omfattet af vores test-handlinger.

4.2 Udførte testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrolaktiviteternes funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel til passende personale hos virksomheden er udført for alle væsentlige kontrolaktiviteter. Forespørgsler er udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres. Endvidere for at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation, som indeholder information om udførelse af kontrollen. Det omfatter gennemlæsning og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Observation	Observation af kontrollens udførelse.
Genudførelse af kontrol	Den relevante kontrol er genudført med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores test af de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Kontrolmål A (Instruks)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Inspiceret, at procedurer er opdateret.</p>	Vi har ikke konstateret afvigelser.
A2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	<p>Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret via stikprøver på behandling af personoplysninger, at disse foregår i overensstemmelse med instruks.</p>	Vi har ikke konstateret afvigelser.
A3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.</p>	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Inspiceret, at procedurer er opdateret.</p> <p>Inspiceret via stikprøver på indgåede databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.</p>	Vi har ikke konstateret afvigelser.
B2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed.</p> <p>Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.</p>	Vi har ikke konstateret afvigelser.
B3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	<p>Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software.</p> <p>Inspiceret, at antivirus software er opdateret.</p>	Vi har ikke konstateret afvigelser.
B4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	<p>Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.</p> <p>Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.</p>	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Vi har ikke konstateret afvigelser.
B6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres 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 via stikprøver på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Vi har ikke konstateret afvigelser.
B7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Vi har ikke konstateret afvigelser.
B8	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 der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B9	<p>Der er etableret logning i systemer, databaser og netværk. F.eks.: aktiviteter udført af administratorer, sikkerhedshændelser som ændringer i log indstillinger, deaktivering af logning, ændringer i brugerrettigheder, fejlede loginforsøg.</p> <p>Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs.</p> <p>Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.</p> <p>Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.</p> <p>Inspiceret via stikprøver på logning, at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser.</p>	Vi har ikke konstateret afvigelser.
B10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	<p>Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form.</p> <p>Inspiceret via stikprøve på udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret.</p>	Vi har ikke konstateret afvigelser.
B11	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.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B12	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 ikke konstateret afvigelser.
B13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Bruges adgang revurderes regelmæssigt, herunder at 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 via stikprøve på medarbejders adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.	Vi har ikke konstateret afvigelser.
B14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører højrisiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Vi har ikke konstateret afvigelser.
B15	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.	Vi har ikke konstateret afvigelser.

Kontrolmål C (Organisatoriske foranstaltninger)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Vi har ikke konstateret afvigelser.
C2	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 sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret via stikprøve på indgåede databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikens krav til sikringsforanstaltninger og behandlingssikkerheden.	Vi har ikke konstateret afvigelser.
C3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvnin-gen omfatter i relevant omfang: Referencer fra tidligere ansættelser, straffeattest, eksamensbeviser m.v.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret via stikprøve på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning.	Vi har ikke konstateret afvigelser.
C4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer at nyan-satte medarbejdere underskriver en fortrolighedsaftale samt bliver introduceret til informationssikkerhedspolitikken, procedurerer vedrørende databehandling, og anden relevant information.	Vi har ikke konstateret afvigelser.
C5	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 medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages	Vi har ikke konstateret afvigelser.

Kontrolmål C (Organisatoriske foranstaltninger)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C6	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, 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.	Vi har ikke konstateret afvigelser.
C7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	<p>Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.</p> <p>Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.</p>	Vi har ikke konstateret afvigelser.

Kontrolmål D (Sletning og tilbagelevering)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke konstateret afvigelser.</p>
D2	<p>Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner:</p> <p>Opbevaring og behandling sker, så længe den underliggende kommercielle aftale består, og indtil databehandlerens ydelser ophører.</p> <p>Ved ophør returneres eller slettes persondata.</p>	<p>Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.</p> <p>Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.</p>	<p>Vi er blevet oplyst om at Compent ikke opbevarer persondata for dataansvarlige.</p> <p>Vi har ikke konstateret afvigelser.</p>
D3	<p>Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: Tilbageleveret til den dataansvarlige og/eller slettet, hvor det ikke er i modstrid med anden lovgivning.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.</p>	<p>Vi har ikke konstateret afvigelser.</p>

Kontrolmål E (Opbevaring)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.</p>	<p>Vi har ikke konstateret afvigelser.</p>
E2	<p>Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.</p>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.</p> <p>Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.</p>	<p>Vi er blevet oplyst om at Compent ikke opbevarer persondata for dataansvarlige.</p> <p>Vi har ikke konstateret afvigelser.</p>

Kontrolmål F (Underdatabehandlere)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F1	<p>Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi er blevet oplyst om at Compent ikke benyttes sig at underdatabehandlere.</p> <p>Vi har ikke konstateret afvigelser.</p>

Kontrolmål G (Tredjelandsoverførsler)

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.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi er blevet oplyst om at der ikke for nogle kundeløsninger er aftaler om at virksomheden må overføre data til tredjelande.</p> <p>Vi har ikke konstateret afvigelser.</p>

Kontrolmål H (Registreredes rettigheder)

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.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for databehandlers bistand af den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke konstateret afvigelser.</p>
H2	<p>Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.</p>	<p>Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. <p>Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.</p>	<p>Vi er blevet oplyst om at Compent ikke opbevarer personoplysninger for dataansvarlige.</p> <p>Vi har ikke konstateret afvigelser.</p>

Kontrolmål I (Sikkerhedsbrud)

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

Nr.	Compent ApS's kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Inspiceret, at proceduren er opdateret.</p>	Vi har ikke konstateret afvigelser.
I2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: Awareness hos medarbejdere, overvågning af netværkstrafik, opfølgning på logning af tilgang til personoplysninger.	<p>Inspiceret, at databehandler udbyder awareness- træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p> <p>Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv.</p>	Vi har ikke konstateret afvigelser.
I3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt 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.	Vi har ikke konstateret afvigelser.
I4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p>	Vi har ikke konstateret afvigelser.

PENNEO

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.”

Jeppe Basse

Administrerende direktør

Serienummer: 9afdd2ed-0bfb-4d12-954c-66642a0b8e9f

IP: 188.120.xxx.xxx

2026-05-26 08:12:58 UTC



Simon Okkels

**inforevision statsautoriseret revisionsaktieselskab CVR:
19263096**

Partner, Lead IT-auditor (CISA)

Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a

IP: 93.165.xxx.xxx

2026-05-26 09:52:05 UTC



John Richardt Søbjerg

**inforevision statsautoriseret revisionsaktieselskab CVR:
19263096**

Statsautoriseret revisor

Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a

IP: 93.165.xxx.xxx

2026-05-26 10:05:47 UTC



Penneo dokumentnøgle: 5AWI9-NWKB9-X3RP6-RK4K1-O2IOX-E7IUP

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.