ROESGAARD
En del af Cedra

IntraNote A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandlingsaftaler med databehandlere, der bruger DocuNote og WorkSpace-løsningen.

Indholdsfortegnelse

1. Ledelsens udtalelse

IntraNote A/S behandler personoplysninger på vegne af kunderne i henhold til databehandleraftale elektronisk dokumenthåndtering I DocuNote og WorkSpace. IntraNote A/S anvender hos udvalgte kunder Atea, som underdatabehandler til hosting af DocuNote og WorkSpace. Denne erklæring indeholder kun kontrolmål og foranstaltninger hvor IntraNote A/S er ansvarlig. Kontrolmål og foranstaltninger relateret til Atea er beskrevet i beskrivelsen samt i de forsikringsprocedurer og test, der udføres af den uafhængige revisor.

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

IntraNote A/S bekræfter følgende:

1. Den medfølgende beskrivelse, sektion 3 og 4, giver en retvisende beskrivelse af elektronisk dokumenthåndtering i DocuNote og WorkSpace, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen den 14. april 2026. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan elektronisk dokumenthåndtering 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 registrerede
- 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 med henvisning til elektronisk dokumenthåndterings afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) indeholder relevante oplysninger om ændringer ved databehandlerens behandling af personoplysninger foretaget den 14. april 2026.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne elektronisk dokumenthåndtering 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 elektronisk dokumenthåndtering, 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 fungerede effektivt den 14. april 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, og

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse den 14. april 2026.

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.

VLRS GRP A/S

CVR.nr. 25797620
Papirfabrikken 20A
8600 Silkeborg
Danmark

Direktion

Søren Rust Nielsen
Adm. Direktør

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med IntraNote A/S.

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

Omfang

Vi har fået til opgave at afgive erklæring om IntraNote A/S' beskrivelse i sektion 3 på vegne af dataansvarlige omfattet af EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") 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 "databeskyttelsesloven") den 14. april 2026 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

IntraNote A/S' ansvar

IntraNote A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 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 FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og nødvendige omhu, fortrolighed og professionel adfærd.

Roesgaard Godkendt Revisionsaktieselskab, CVR.nr. 37543128 anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om IntraNote A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på, at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin softwareløsning DocuNote og WorkSpace samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 4.

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

IntraNote 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 DocuNote og WorkSpace, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Desuden 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 elektronisk dokumenthåndtering, således som denne var udformet og implementeret den 14. april 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 den 14. april 2026 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 den 14. april 2026.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt IntraNote A/S' DocuNote og WorkSpace, 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.

Horsens, den 21. april 2026

Roesgaard

Statsautoriseret Revisionsaktieselskab
CVR-nr. 37 54 31 28

Michael Mortensen
statsautoriseret revisor
MNE-nr. mne34108

3. Beskrivelse af behandling

Formålet med IntraNotes behandling af personoplysninger på vegne af den dataansvarlige er:

- Udvikle og implementere løsninger inden for Enterprise Content Management. Vores løsninger er fleksible standardløsninger, der er skræddersyet til dine behov, så du får en hurtig og effektiv implementering.
- Vi har leveret løsninger til det offentlige og private organisationer siden 2001 med fokus på optimering af procedurer, organisationens videndeling og elektronisk dokumenthåndtering.

IntraNotes arbejde for kunder foretages i overensstemmelse med rammeaftalen og de dertilhørende bilag, herunder databehandleraftalen, der samtidig regulerer rammerne for instruksens indhold og behandlingssikkerhed.

Denne beskrivelse og revisionsrapport dækker design og implementering af kontroller den 14. april 2026 til DocuNote og WorkSpace og er beregnet til dataansvarlige, der bruger DocuNote og WorkSpace.

Beskrivelsen og erklæringen dækker vores elektroniske dokumenthåndtering i DocuNote og WorkSpace til kunder enten på deres egen it-infrastruktur eller på IntraNotes cloud-løsning på Atea i Ballerup, Danmark.

3.1. Underdatabehandler

IntraNote har løbende møder med Atea og modtager en ISAE3402 assurance rapport én gang om året.

Bearbejdningens art

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

- Assistance vedrørende DocuNote og WorkSpace
- Produktsupport og fejlhåndtering i DocuNote og WorkSpace
- Udvikling, implementering og tilpasning af DocuNote og WorkSpace
- Hosting af DocuNote og WorkSpace, hvis hosting er en del af aftalen

3.2. Personoplysninger

Følgende typer af personoplysninger behandles i DocuNote og WorkSpace iht. databehandleraftalen:

- Generelle personoplysninger, herunder identifikationsdata såsom navn og adresse eller data om økonomi, skatter, gæld, væsentlige sociale problemer, andre private forhold, sygedage, jobrelaterede forhold, familieforhold, bolig, motorkøretøj, ansøgninger, CV, ansættelsesdato og stilling.

- Særlige kategorier af personoplysninger kan undtagelsesvist forekomme, herunder race og etnisk oprindelse, politisk holdning, religion eller tro, fagforeningsmedlemskab, genetiske data, biometriske data til entydig identifikation af en fysisk person, data vedrørende sundhed eller sexliv eller seksuel orientering.
- Andre personoplysninger, herunder data om strafbare handlinger kan undtagelsesvist forekomme.

Kategorier af registrerede, der falder ind under databehandleraftalen:

- Medarbejdere
- Kunder
- Leverandører og andre eksterne partnere
- Børn

Typer af personoplysninger og datasubjekter varierer afhængigt af den dataansvarliges brug af DocuNote og WorkSpace.

IntraNote har først adgang til de personhenførbare data, efter at den dataansvarlige har givet en midlertidig adgang.

Den dataansvarlige er også ansvarlig for at give brugere fra Creative Quarter adgang til deres produktionsmiljø af DocuNote og WorkSpace og personoplysninger heri. Creative Quarter brugere anvender kun hardware udstedt og kontrolleret af IntraNote til at få adgang til IntraNote-systemer.

3.3. Risikovurdering

IntraNote styrer og kontrollerer DocuNote og WorkSpace baseret på en risikostyringsproces. Risikostyring omfatter følgende:

- Identifikation af potentielle risici, der kan påvirke DocuNote og WorkSpace, både fra en teknisk og forretningsmæssig synsvinkel og risikoen for de registreredes rettigheder og friheder
    - Vurdering af de identificerede potentielle risici, betydning, sandsynlighed og konsekvenser i DocuNote og WorkSpace
    - Foranstaltninger til at reducere sandsynligheden for, at risici opstår på en omkostningseffektiv måde.

En gang årligt foretages en risikovurdering, samt ved større organisatoriske og/eller tekniske ændringer. Dette bidrager til at sikre, at IntraNote overholder høje standarder, bedste praksis, kollaborativ risikovurdering og gennemgang af serviceniveauaftaler, med særligt fokus på at sikre at DocuNote og WorkSpace understøtter høj fortrolighed, integritet og tilgængelighed.

På baggrund af de identificerede risici er der udarbejdet og implementeret en informationssikkerhedspolitik med de tilhørende procedurer og retningslinjer for informationssikkerhed.

Regelmæssig vurdering eller implementering af risikobegrænsende aktiviteter eller foranstaltninger udføres.

Disse problemer rapporteres løbende til den administrerende direktør. Bestyrelsen modtager årligt en rapport om risikostyring og informationssikkerhed samt aktiviteter og initiativer.

3.4. Informationssikkerhedsramme og ledelsessystem

IntraNote har valgt at anvende principperne i ISO/IEC 27001:2013 (herefter ISO27001) og principperne i ISO/IEC 27002:2013 (herefter ISO27002) som informationssikkerhedsramme. IntraNote anvender et sikkerhedsstyringssystem (ISMS) i henhold til ISO 27001. IntraNote bruger ISO27002 som referenceramme for Statement of Applicability (SOA) i operationalisering af ISMS. Således i SOA af ISO27002, implementering af relevante sikkerhedsmekanismer og foranstaltninger for følgende områder er besluttet:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Sikkerhed for menneskelige ressourcer
- Asset Management
- Adgangskontrol
- Fysisk og miljømæssig sikkerhed
- Driftssikkerhed
- Kommunikationssikkerhed
- Systemanskaffelse, udvikling og vedligeholdelse
- Leverandørforhold
- Håndtering af hændelser vedrørende informationssikkerhed
- Business Continuity Management
- Overholdelse

Områderne er udvalgt ud fra den service og opgaver, som IntraNote har ansvaret for den enkelte kunde, som beskrevet i hovedaftalen og databehandleraftalen med tilhørende bilag, samt i informationssikkerhedspolitikken, procedurer og vejledninger.

En mere detaljeret beskrivelse af implementerede tiltag fremgår af IntraNotes kontrolmål og kontroller den 14. april 2026.

IntraNote har gennem de sidste år arbejdet på at forbedre og formalisere informationssikkerheden og databeskyttelse hos IntraNote. Som et resultat af dette arbejde har IntraNote foretaget forbedringer og ændringer i procedurer og aktiviteter for at være i overensstemmelse med principperne i ISO27001/ISO27002. Desuden modtager alle medarbejdere og konsulenter hos IntraNote bevidsthedstræning og er blevet informeret om arbejdet med ISO27001 og databeskyttelse.

IntraNote vil arbejde med løbende forbedring af Information Security Management System og med databeskyttelse.

Organisering af informationssikkerhed

Topledelsen hos IntraNote A/S har forpligtet sig til at bakke op om og understøtte informationssikkerheden ved at underskrive den generelle informationssikkerhedspolitik.

Virksomheden har en de-facto "no-blame"-politik, der tilskynder medarbejderne til at være åbne om brud på informationssikkerheden, hvilket reducerer behovet for adskillelse af opgaver.

IntraNote A/S har arbejdet omfattende med databeskyttelse i sine løsninger, herunder support fra en ekstern rådgiver.

Sikkerhed for menneskelige ressourcer

Da virksomheden er en værdidrevet virksomhed baseret på tillid til sine medarbejdere frem for kontrol, er virksomheden ekstremt afhængig af medarbejdernes kompetencer og deres vilje til at handle i virksomhedens interesse. For at opfylde informationssikkerhedsmålene i et sådant miljø er konstant fokus, træning og information afgørende.

Asset management

Aktiver forbundet med IntraNote-løsningerne identificeres. Alle aktiver vedligeholdes, så aktivbeholdningen er nøjagtig, opdateret, konsistent og afstemt med andre beholdninger.

Ejerskab af hvert aktiv tildeles, og klassifikationer af aktivet identificeres og dokumenteres.

Ejeren af aktivet sikrer, at aktiverne er opført, klassificeret korrekt og beskyttet og sikrer korrekt håndtering, når aktiver transporteres, slettes eller destrueres.

Medarbejdere eller eksterne parter returnerer alle aktiver tilhørende IntraNote ved opsigelse af deres ansættelse, kontrakt eller aftale.

Adgangskontrol

En politik for adgangskontrol er etableret, dokumenteret og revideret baseret på forretnings- og sikkerhedskrav.

Adgangskontrol er både fysisk og logisk, som betragtes under ét.

Brugere får kun adgang til netværks- og netværkstjenester, som brugerne specifikt er autoriseret til at bruge.

Politikken tager højde for følgende:

- Sikkerhedskrav
- Need-to-know-princippet
- Adskillelse af adgangskontrol
- Fjernelse af adgangsret ved ansættelsesforholdets ophør eller korrigeret ved ansættelsesskifte.

Der eksisterer en formel brugerregistrerings- og afregistreringsproces til administration af adgangsrettigheder. Tildeling og brug af privilegerede adgangsrettigheder er begrænset, kontrolleret og overvåget.

Al brugeradgang gennemgås regelmæssigt, mindst én gang om året.

Fysisk og miljømæssig sikkerhed

Fysisk sikkerhed for kundesystemer, der hostes hos Atea, er Ateas ansvar og er kontraktuelt reguleret.

Fysisk sikkerhed af kundehostede systemer er kundens ansvar og fremgår af en kontrakt med kunden.

Hos IntraNote indeholder kun serverrummet vitale informationsaktiver.

Kontorborde, bærbare computere og mobile enheder kan indeholde følsomme oplysninger, men dette område er reguleret af en klar skrivebordspolitik, en låseskærm og adgangskodepolitik og gennem Bitlocker-kryptering.

Driftssikkerhed

Systemopsætning og betjeningsprocedurer er baseret på Best Practice.

Der findes formelle procedurer for ændringer af kundesystemer (hostet hos kunden eller hos Atea).

Der eksisterer ingen formel procedure for ændringer af IntraNotes egen infrastruktur. Men på grund af it-ledelsens ikke-formaliserede ansvar, er det usandsynligt, at ændringer nogensinde vil blive gennemført uden koordinering og godkendelse af IT-ledelsen.

Systemanskaffelse, udvikling og vedligeholdelse

En politik er på plads, der kun tillader kundeejede testdata i huset, når der er en aktiv servicebillet tilknyttet det. Procedurerne angiver, at testdata skal slettes, når servicebilletten lukkes.

Desuden har IntraNote databehandleraftaler med alle kunder og underleverandører i overholdelse af EU's GDPR-regler og har implementeret passende processer til at håndtere følsomme personoplysninger.

Leverandørforhold

Krav til informationssikkerhed ved håndtering af risici forbundet med leverandørers adgang aftales med Atea. Ledelsen fra IntraNote mødes løbende med Atea og modtager løbende rapportering fra Atea, og en ISAE3402-sikkerhedsrapport fra Atea modtages én gang om året.

Revisionserklæringen er en delvis erklæringserklæring.

Håndtering af informationssikkerhedshændelser og håndtering af databrud

Der findes skriftlige procedurer om, at databehandleren skal informere den dataansvarlige i tilfælde af brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurderinger af, om procedurerne skal ajourføres. Følgende kontroller er opsat for at identificere eventuelle brud på persondatasikkerheden:

- Bevidsthedstræning af medarbejdere
- Overvågning af netværkstrafik
- Opfølgning på logning af adgang til personhenførbare data.

Hvis der er sket et databrud, informerer databehandleren den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at have fået kendskab til et sådant databrud hos databehandleren eller en underdatabehandler.

Databehandleren har etableret procedurer for at bistå den dataansvarlige med at foretage indberetninger til Datatilsynet, herunder:

- Arten af databruddet;
- Sandsynlige konsekvenser ved databruddet;
- Foranstaltninger truffet eller foreslået truffet for at reagere på databruddet.

Forretningskontinuitet

Krav til informationssikkerhed i krisesituationer fastlægges. Forretningskontinuitetsplan og katastrofegenopretningsplan eksisterer. Sådanne planer testes og opdateres regelmæssigt, mindst én gang om året.

Compliance

Relevante lovmæssige og kontraktmæssige krav er identificeret. Krav er dokumenteret og opdateret.

Kontrolmål og kontrolaktiviteter

Vi henviser til afsnit 4 for en beskrivelse af kontrolmålene og de konkrete kontrolaktiviteter og revisionen heraf.

Supplerende kontrol hos de dataansvarlige

De dataansvarlige har følgende forpligtelser:

- At sikre, at personoplysninger data er ajourførte
- At sikre lovligheden af instruktioner i henhold til de til enhver tid gældende regler under privatlivets fred.

Den enkelte kunde er ansvarlig for dataoverførsel mellem kunden til IntraNotes DocuNote og WorkSpace hos Atea. Det er således den enkelte kundes ansvar at sikre kontrollerne i forbindelse hermed.

Al brugerstyring, herunder tildeling af adgangsrettigheder og beskyttelse af adgang gennem servere og udstyr placeret på kundesteder, er de dataansvarliges ansvar.

Yderligere er midlertidig adgang givet til brugere fra Creative Quarter eller IntraNote ansvaret for de dataansvarlige.

Anskaffelse, udvikling, tilpasning og implementering af DocuNote og WorkSpace hos kunder er kundens eget ansvar. Styring af systemudvikling, indkøb og forandringsledelse er også kundernes ansvar.

Til DocuNote og WorkSpace-sessioner, der opererer andre steder end hos IntraNotes IAAS Cloud hos Atea i Ballerup kunderne er selv ansvarlige for drift, fysisk og miljømæssig sikkerhed.

Kunden er ansvarlig for alt indhold i DocuNote og WorkSpace. Kunden er ansvarlig for al kontrol vedrørende datahåndtering, herunder sletning af personhenførbare data fra DocuNote og WorkSpace.

Kunden er som dataansvarlig ansvarlig for at have en databehandleraftale med IntraNote som databehandler.

Antivirus er ikke installeret på servere og databaser, i stedet skal der installeres antivirus beskyttelse på klienter, der har adgang til DocuNote og WorkSpace. Kunden er ansvarlig for at sikre, at klienter er beskyttet med antivirus.

Test af kontroller udført af den uafhængige revisor – formål og omfang

Vores arbejde blev udført i overensstemmelse med International Auditing and Assurance Standards.

Vores test af udformningen og implementeringen af kontrollerne har omfattet kontrolmålene og tilknyttede kontroller udvalgt af ledelsen og som vist i sektion 4. Denne rapport leveres under delmetoden og inkluderer ikke test af kontroller udført af undertjenesteudbyder Atea. Ydelser leveret af Atea A/S vedrører infrastruktur, fysisk sikkerhed og miljøsikkerhed.

Andre kontrolformål, tilhørende kontroller og kontroller hos den enkelte dataansvarlige er ikke dækket af vores forsikringsarbejde. Det forudsættes, at sidstnævnte kontroller undersøges og vurderes af den dataansvarlige.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Overordnede politikker:

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*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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 procedurer er opdateret.	Ingen væsentlige afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på 3 behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen væsentlige afvigelser konstateret.

Kontrolmål A **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.**			
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.	Der har aldrig været behov for underretning om ulovlige behandlinger Ingen væsentlige afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Inspiceret ved en stikprøve på 3 databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Ingen væsentlige afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler 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 databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.	Ingen væsentlige afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
		Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	
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 antivirus software. Inspiceret, at antivirus software er opdateret.	Ingen væsentlige afvigelser konstateret.
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 firewall er konfigureret i henhold til intern politik herfor.	Ingen væsentlige afvigelser konstateret.
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 væsentlige afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
B.6	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 ved en stikprøve på 3 brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen væsentlige afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Cacti • DocuNote og WorkSpace • Crowdstrike	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen væsentlige afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
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 der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Ingen væsentlige afvigelser konstateret.

B.9	Der er etableret logning i systemer, databaser og netværk af følende 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
	  ○ Logoplysninger 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 og opfølgning på logs.
		
		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 logs er beskyttet mod manipulation og sletning.
			Det er konstateret, at der ikke foreligger dokumentation for, at beskyttelse mod manipulation af log-oplysninger er implementeret.
			
			Ingen yderligere afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
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.	Ingen væsentlige afvigelser konstateret.
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 gennemførsel af sårbarhedsscanninger og penetrationstests. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Det er konstateret at processen for håndtering af identificerede sårbarheder ikke er implementeret effektivt. Ingen yderligere afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
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.	Det er konstateret, at der anvendes en aktiv firewall, og at det ikke har været muligt at fremskaffe dokumentation for, at enheden fortsat modtager relevante sikkerhedsopdateringer. Ingen yderligere afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	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 3 medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve på 1 fratrådt medarbejder, at disses adgange til systemer og databaser er rettidigt deaktiverede eller nedlagt.	Ingen væsentlige afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	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 høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen væsentlige afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således 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.	Ingen væsentlige afvigelser konstateret.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	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 væsentlige afvigelser konstateret.
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 sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på 3 databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen væsentlige afvigelser konstateret.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på 3 databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved en stikprøve på en nyansat medarbejder, at der er dokumentation for, at efterprøvningen har omfattet: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Ingen væsentlige afvigelser konstateret.
C.4	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 ved en stikprøve på en nyansat medarbejder, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på en nyansat medarbejder, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen væsentlige afgivelser konstateret.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
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 fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på to fratrådte medarbejdere, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen væsentlige afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, 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 en stikprøve på to fratrådte medarbejdere, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen yderligere afvigelser konstateret.
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 væsentlige afvigelser konstateret.

Kontrolmål D **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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 væsentlige afvigelser konstateret.
	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Ved ophør af tjenester forpligtes Databehandleren til, efter anmodning fra den Dataansvarlige, at slette alle de personoplysninger, der er blevet behandlet på vegne af den Dataansvarlige, og formelt bekræfte over for den Dataansvarlige, at sletning har fundet sted. Alternativt kan databehandleren returnere	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på 2 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på 2 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er	Ingen væsentlige afvigelser konstateret.

	personoplysningerne til den dataansvarlige og efterfølgende slette alle eksisterende kopier af dataene, medmindre EU- eller national lovgivning kræver, at personoplysningerne opbevares	dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	

Kontrolmål D **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.**			
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret ved en stikprøve på to ophørte databehandlinger, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen væsentlige afvigelser konstateret.

Kontrolmål E **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på 3 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen væsentlige afvigelser konstateret.

Kontrolmål E **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på 3 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 væsentlige afvigelser konstateret.

Kontrolmål F **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.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen væsentlige afvigelser konstateret.
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 en stikprøve på 3 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 væsentlige afvigelser konstateret.

Kontrolmål F **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.**			
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Der har ikke været ændringer ift. brug af underdatabehandlere.	Ingen væsentlige afvigelser konstateret.
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 en stikprøve på 3 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen væsentlige afvigelser konstateret.

Kontrolmål F **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**			
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 væsentlige afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	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 væsentlige afgivelser konstateret.

Kontrolmål			**G**
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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 væsentlige afvigelser konstateret.
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 en stikprøve på 3 dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Ingen væsentlige afgivelser konstateret.

Kontrolmål G **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.**			
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 en stikprøve på 3 dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Ingen væsentlige afgivelser konstateret.

Kontrolmål H **Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen væsentlige afgivelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	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 væsentlige afgivelser konstateret.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen væsentlige afgivelser konstateret.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af tilgang til personoplysninger	Inspiceret, at databehandler udbyder awareness- træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik 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 væsentlige afvigelser konstateret.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
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. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 72 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden	Der har ikke været databrud i erklæringsperioden. Ingen væsentlige afgivelser konstateret.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af 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 væsentlige afgivelser konstateret.

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."

Søren Rust Nielsen
Underskriver 1
Serienummer: 5210fb3c-ceba-48a1-b5bc-1905c80a229e
IP: 85.184.xxx.xxx
2026-04-23 07:05:08 UTC

MitID

Casper Lundqvist Damgaard
Underskriver 2
Serienummer: 7d687d52-addf-4922-9663-ef26cda7b82c
IP: 92.246.xxx.xxx
2026-04-23 07:14:25 UTC

MitID

Michael Mortensen
Roesgaard Godkendt Revisionsaktieselskab CVR: 37543128
Underskriver 3
Serienummer: 56c78f0d-d030-41dc-a7fe-ad94bcba5a88
IP: 212.98.xxx.xxx
2026-04-23 09:31:59 UTC

MitID