Lector ApS

Ordrupvej 101
2920 Charlottenlund
CVR.NR. 10 02 16 18

ISAE 3000, type 2

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger for perioden 1. juni 2023 – 31. maj 2024

Indhold

S.nr. 326624

JR/SO

1. Ledelsens udtalelse

Lector 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 Lector ApS' softwareløsninger, 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.

Lector ApS bekræfter, at:

a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Lector ApS' ydelse, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden 1. juni 2023 - 31. maj 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Lector 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 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 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 ydelsen til behandling af personoplysninger foretaget i perioden 1. juni 2023 – 31. maj 2024.

   (iii) 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 fungerede effektivt i hele perioden 1. juni 2023 til 31. maj 2024. Kriterierne anvendt for at give denne udtalelse var, at:

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

(ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. juni 2023 til 31. maj 2024.

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Charlottenlund, den 26. juli 2024
Lector ApS

Tue Villum Sørensen
Adm. direktør

2. Beskrivelse af behandling

Lector har etableret kontroller i relation til databeskyttelse og behandling af persondata med afsæt i den gældende persondatalov. De tekniske og organisatoriske kontroller har været gældende i hele perioden. Der er løbende implementeret opdaterede procedurer frem mod den udførte revision på de områder, hvor databeskyttelsesforordningen introducerede nye og/eller skærpede krav.

Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer i Lector.

Intro om Lector

Lector er en innovativ IT-konsulent-, projekt- og produktvirksomhed, som transformerer viden om Software og domæner til kundeværdi.

Vores medarbejdere tager ansvar for kundens forretningsmæssige mål og for deres kolleger via økonomisk bæredygtige løsninger.

Vi udfordrer "status quo" ved løbende at stille spørgsmål - hos vores kunder og hos os selv.

Beskrivelse af ydelser

Lector bygger på tre forretningsområder

- Sags- og Dokumenthåndtering, med produkterne TeamShare og ESS
- Toldhåndtering med produktet Logistics Trading Services, LTS
- Konsulentarbejde, hvor Lector leverer færdige software projekter eller ressourcer til kunder. Vi leverer her IT konsulenter på tekniske platforme som .NET, Java, Oracle, SQL Server og tilhørende IT-arkitektur, og organisatoriske konsulenter inden for projektledelse og Scrum/SAFe.

På produkterne TeamShare, ESS og LTS leverer Lector produktudvikling, support af produkterne, konsulentydelser ved implementering/til integrationer og kan levere hosting af de leverede installationer. Hvor TeamShare og ESS kan leveres som on-premise løsning eller som enten private eller public cloud SaaS løsninger, leveres LTS udelukkende som SaaS.

Når Lector leverer cloud SaaS udgaver af TeamShare og ESS, håndteres dette via servere og services i Microsoft Azure West-Europe, og ved at bruge kundernes egne Office 365 SharePoint Online platform, i det datacenter de har valg. Microsoft Azure leverer servere, netværk, hypervisor og storage. Azure revideres og leverer rapportering i form af årlig opdateret SOC II rapport.

Private cloud SaaS udgaver af produkterne TeamShare og ESS kan som option leveres fra et dansk hostingcenter, i samarbejde med vores underleverandør Kimo Consulting ApS. Kimo Consulting ApS er ansvarlig for den fysiske sikkerhed, hardware, netværk, backup, hypervisor og storage. Kimo Consulting ApS revideres og leverer rapportering årligt ift. ISAE 3000 og ISAE 3402.

Lector varetager alt drift af vores LTS SaaS produkt for alle kunder. Dette drives på servere i Amazon AWS. AWS står her for servere, netværk, hypervisor og storage. AWS revideres og leverer rapportering i form af årlig opdateret SOC II rapport.

Karakteren af behandlingen og praktiske tiltag

Arbejdet omkring GDPR er delt i to fokusområder – det interne, som vedrører alle interne processer, hvor vi som virksomhed har med persondata at gøre (f.eks. HR, IT, og økonomi) og det kunderettede, som vedrører alle de områder hvor vi interagerer med vores kunder og potentielt kunne komme i berøring med persondata, herunder vores cloud SaaS løsninger.

Der indgås skriftlige databehandleraftaler både med kunder og underleverandører. Aftalerne implementeres i afdelingens retningslinjer og procedurer. Lector behandler ikke persondata uden indgået databehandleraftale med den dataansvarlige (kunden).

Lector har etableret en række politikker og procedurer, som medarbejdere har modtaget løbende og gennemgår awareness om efterlevelse af, bl.a. bestående af:

- It-sikkerhedspolitikker
- Persondatapolitikker
- Procedurer (SOP)

It-sikkerhedspolitikken etablerer processer og kontroller hos Lector og omfatter alle systemer og services, der tilbydes til kunderne, såvel som interne systemer der indeholder persondata, fx HR og Økonomi.

Lector's it-sikkerhedspolitik er udarbejdet med afsæt i ISO 27001 standarden. Lector foretager løbende, minimum en gang årligt, en vurdering af denne it-sikkerhedspolitik samt de tilknyttede retningslinjer – herunder at disse lever op til de eksterne forpligtelser, udtrykt i lovgivning og kontrakter/aftaler. Procedurer dækker bl.a. sikkerhed i supporten af kunder, kontrol af underleverandører, kontrol af databehandleraftaler, håndtering af persondata anmodninger, mv. Der udføres løbende risikovurdering af alle relevante områder. Sikkerhedshændelser inkl. brud på persondatasikkerhed rapporteres til Lectors it–sikkerhedsansvarlige, som registrerer disse, og varetager videre kommunikation med evt. berørte parter.

Når politikker og procedurer/SOP (standard operating procedures) opdateres, kommunikeres dette til medarbejdere. For den helt centrale IT Sikkerhedspolitik, underskriver medarbejderen at denne er læst, forstået og følges. Politikker og proceduren er tilgængelige i vores egen interne instans af vores eget TeamShare produkt, hvor medarbejderne altid kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til den it-sikkerhedsansvarlige, der sørger for relevante rettelser.

Der bliver løbende foretaget risikoanalyse med henblik på integritet, fortrolighed og tilgængelighed samt beskyttelse af persondata set i forhold til den registreredes rettigheder. Denne risikoanalyse gennemgås kvartalsvist mellem den GDPR-ansvarlige og den administrerende direktør, samt mindst en gang om året, eller ved større ændringer, af hele ledelsesgruppen. I den aktuelle risikoanalyse forefindes der ikke risici kategoriseret som kritiske.

Kun autoriserede brugere har adgang til personoplysninger, og de tildelte brugeradgange er i overensstemmelse med arbejdsmæssigt betingede behov. Ved ændrede behov, ændres/slettes disse adgange i henhold til indarbejdede procedurer.

Lector har ingen DPO, fordi vi ikke har omfattende behandling af persondata som vores hovedaktivitet. Ifølge GDPR artikel 37 er en DPO kun påkrævet, når behandlingen involverer regelmæssig og systematisk monitorering af personer i stort omfang eller behandling af særlige typer af data i stort omfang. Vores behandling af persondata er ikke i et sådant omfang, at det udløser dette krav. Vi har dog sikret, at vi har egnede sikkerhedsforanstaltninger for at beskytte de data, vi behandler.

Risikovurdering

Ledelsen i Lector er ansvarlig for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som Lector til enhver tid står over for, så indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

- Der gennemføres kvartalsvis en risikoanalyse for at klarlægge risici.
- Alle medarbejdere i Lector er blevet undervist i persondatasikkerhed, og ledelsen tager løbende temaer og emner op over for medarbejderne for at styrke processer og forretningsgange og for at understøtte medarbejdernes it-awareness.
- Lector har en operationel risikostyring der sikrer, at der i det daglige arbejde både er fokus på at identificere operationelle fejl og risici, og at der reageres og sættes ind på de områder, der kan minimere risici til et acceptabelt niveau.

Der foretages således løbende vurdering af, hvilke sikkerhedsniveauer der er passende i Lector og hos kunderne. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Kassation
Egne data, fx HR, Økonomi, projektdokumentation m.v., slettes efter nøje afstemte kassationsregler, der sikrer overholdelse af GDPR-reglerne. Dette er implementeret i de systemer Lector benytter til at holde data, herunder vores eget TeamShare miljø.

For data fra kunder, sker opbevaring af personoplysninger alene i overensstemmelse med kontrakten og databehandleraftalen med den dataansvarlige. Personoplysninger slettes og tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige. Lector kan desuden bistå den dataansvarlige i kassation af data undervejs i kontrakten, såfremt dette er ønsket.

Kontrolforanstaltninger
Lector har opstillet politikker, procedurer og procesbeskrivelser til etablering, implementering, vedligeholdelse og løbende forbedring af processer og kontroller for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen og databeskyttelsesloven. Kontrollerne er sat i system gennem udarbejdelse af et årshjul i Lector.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

Lector har desuden udarbejdet procedurer for rekruttering og fratrædelse af medarbejdere og eksterne konsulenter samt retningslinjer for kompetenceudvikling og instruktion af medarbejdere, der behandler personoplysninger og it-awareness, herunder gennemførelse af løbende oplysninger til medarbejderne.

Lector har indført politikker og procedurer, der sikrer, at personoplysninger slettes og tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Det kontrolleres årligt, at personoplysninger, som er blevet behandlet på vegne af den dataansvarlige, er blevet tilbageleveret til den dataansvarlige og slettet, efter endt samarbejde.

Support:
Der ydes support på alle produkter, der er udviklet af Lector. Personoplysninger i forbindelse med support behandles med fortrolighed og respekt for den enkelte bruger.

Henvendelser fra de dataansvarlige:
Lector har en procedure for håndtering og dokumentation af henvendelser fra dataansvarlige i relation til bistand for håndtering af de registreredes rettigheder (indsigtsret, sletning, berigtigelse mv.).

Dokumentation af henvendelser fra dataansvarlige vedr. f.eks. indsigtsret, sletning, berigtigelse mv. håndteres i vores supportsystem.

Lector bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder i henhold til Databeskyttelsesforordningen.

Der er udarbejde procedurer og kontroller indenfor for følgende hovedområder, som refererer til databeskyttelsesforordningen:

- Instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale
- Databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed
- Databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed
- Personoplysninger kan slettes eller tilbageleveres hvis der indgås aftale herom med den dataansvarlige
- Databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige
- 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
- Databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag
- Databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede
- Eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale

Komplementerende kontroller

Som led i levering af ydelserne er der kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i beskrivelsen. Dette omfatter blandt andet at den dataansvarlige

- Sikrer, at personoplysninger er ajourførte
- Sikrer, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering
- Sikrer, at instruksen er hensigtsmæssig, set i forhold til databehandleraftalen og hovedydelsen
- Sikrer, at den dataansvarliges brugere er ajourførte

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

Til ledelsen hos Lector ApS og deres kunder

Omfang
Vi har fået som opgave at afgive erklæring om Lector ApS' beskrivelse i afsnit 2 af ydelse til behandling af personoplysninger i henhold til databehandleraftaler med dataansvarlige, i hele perioden 1. juni 2023 – 31. maj 2024 (beskrivelsen) og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter kontrolmål og tilknyttede kontroller hos Lector ApS' underleverandører og underdatabehandlere. Brugen af underleverandører er nærmere oplistet i databehandleraftaler med kunderne.

Lector ApS' ansvar
Lector 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 revisorers 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 Lector 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 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 ydelse 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 afsnit 1.

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
Lector 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. 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 i afsnit 1. Det er vores opfattelse,

(a) at beskrivelsen af ydelsen, således som denne var udformet og implementeret i hele perioden fra 1. juni 2023 til 31. maj 2024, 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 i hele perioden fra 1. juni 2023 til 31. maj 2024,
(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. juni 2023 til 31. maj 2024.

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 Lector 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, 26. juli 2024

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 Lector 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 i hele perioden 1. juni 2023 til 31. maj 2024.

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

Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Lector ApS' kunder er ikke omfattet af vores testhandlinger.

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 Lector ApS 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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A1	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.	Vi har ikke konstateret afvigelser.
A2	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 via stikprøver på behandling af personoplysninger, at disse foregår i overensstemmelse med instruks.	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vi er blevet oplyst om at der ikke har været tilfælde hvor virksomheden har vurderet instruksen værende i strid med lovgivningen 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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B1	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 via stikprøver på indgåede databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	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.	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. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Vi har ikke konstateret afvigelser.
B3	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.	Vi har ikke konstateret afvigelser.
B4	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.	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.	Lector ApS 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. Inspiceret, at der via stikprøver på alarmer er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
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 teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Vi har ikke konstateret afvigelser.
B9	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. 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. 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. Inspiceret via stikprøver på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.	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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
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.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret via stikprøve på udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret. Inspiceret via stikprøve på udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	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 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.	Vi har ikke konstateret afvigelser.
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.

Kontrolmål B (Tekniske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B13	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 via stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret via stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	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 høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen yderligere afvigelser fundet.
B15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler, 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.	Lector ApS 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 informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Vi har ikke konstateret afvigelser.
C3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen 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. Inspiceret via stikprøve på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet referencer fra tidligere ansættelser, straffeattest, eksamensbeviser m.v., i relevant omfang.	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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
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 ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: informationssikkerhedspolitikken, procedurer vedrørende databehandlings, samt 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 medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Vi har ikke konstateret afvigelser.
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. Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Vi er blevet oplyst at medarbejdere kun gjort opmærksom på tavshedspligt under ansættelse og ikke ved fratrædelse 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.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Vi har ikke 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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D1	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.	Vi har ikke konstateret afvigelser.
D2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: Maksimal opbevaringsperiode ligger mellem 1- 3 mdr. afhængig af aftale.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Vi har ikke konstateret afvigelser.
D3	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 ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Vi har ikke konstateret afvigelser.

Kontrolmål E (Opbevaring)

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

Nr.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E1	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 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Vi har ikke konstateret afvigelser.
E2	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 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Vi er blevet oplyst at kundernes data ligger i deres egen Azure Tenant og for de komponenter Lector har ansvaret for er data opbevaret i Europa. Vi har ikke konstateret afvigelser.

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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F1	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.	Vi har ikke konstateret afvigelser.
F2	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 underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Vi har ikke konstateret afvigelser.
F3	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. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Vi har fået oplyst, at der ikke er skiftet underdatabehandlere i perioden, og har derfor ikke kunne teste effektiviteten af kontrollen. Vi har ikke konstateret afvigelser.
F4	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 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har ikke konstateret afvigelser.

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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F5	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.	Vi har ikke konstateret afvigelser.
F6	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.	Vi har ikke konstateret afvigelser.

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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G1	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.	Vi er blevet oplyst om at der ikke overføres persondata vedr. kunder til tredjelande. Vi har ikke konstateret afvigelser.
G2	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 dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Vi er blevet oplyst om at der ikke overføres persondata vedr. kunder til tredjelande. Vi har ikke konstateret afvigelser.
G3	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.	Vi er blevet oplyst om at der ikke overføres persondata vedr. kunder til tredjelande. Vi har ikke konstateret afvigelser.

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.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H1	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. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer. Inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.	Vi har fået oplyst, at der ikke har været udført bistand til dataansvarlig i perioden, og har derfor ikke kunne teste effektiviteten af kontrollen. Vi har ikke konstateret afvigelser.
H2	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.	Vi har ikke konstateret afvigelser.

Kontrolmål I (Sikkerhedsbrud) Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I1	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.	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.	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.	Vi har ikke konstateret afvigelser.
I3	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. 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.	Vi er blevet oplyst, at der ikke har været nogen brud på persondatasikkerheden i erklæringsperioden Vi har ikke konstateret afvigelser.

Kontrolmål I (Sikkerhedsbrud) Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Lector ApS kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet og tager højde for følgende vigtige elementer: Karakteren af bruddet, sandsynlige konsekvenser af bruddet samt foranstaltninger som er truffet eller foreslås truffet for at håndtere bruddet.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for beskrivelser af: Karakteren af bruddet, sandsynlige konsekvenser af bruddet samt foranstaltninger som er truffet eller foreslås truffet for at håndtere bruddet. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden. Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	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."

Tue Villum Sørensen
Adm. direktør
Serienummer: e558b121-cb89-4e24-9c08-212e8fef3400
IP: 94.18.xxx.xxx
2024-07-29 07:40:24 UTC

Simon Okkels
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Partner, Lead IT-auditor (CISA)
Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a
IP: 93.165.xxx.xxx
2024-07-29 07:53:12 UTC

John Richardt Søbjærg
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Statsautoriseret revisor
Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a
IP: 62.243.xxx.xxx
2024-07-29 08:04:11 UTC