Revisorerklæring

JO Informatik ApS

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder pr. 20. december 2022

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Marts 2023

Indholdsfortegnelse

Afsnit 1: JO Informatik ApS' beskrivelse af behandlingsaktivitet for leverancen af FilArkiv og Insight Tools

1 Indledning

Denne kontrolbeskrivelse er del af den overordnede ramme for sikkerhedsstyring, fokuseret på dokumenteret vedligehold, drift, support og hosting af vores produkter FilArkiv og Insight Tools.

JO Informatik anser et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, og som et kvalitetselement for at kunne tilbyde en sikker service overfor kunder, samarbejdspartnere, og myndigheder. Informationssikkerhed er derfor en nøgleværdi hos JO Informatik og er en naturlig del af vores aktiviteter.

Ledelsen foretager løbende overvågning af Informationssikkerhed og risikobilledet for vores virksomhed, og vi evaluerer kontrolbeskrivelsen mindst én gang årligt.

Andre produkter og ydelser som JO Informatik leverer, er ikke omfattet af dette dokument.

2 Vores kontrolmål

Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om at levere et stabilt og sikkert produkt til vores kunder. For at kunne gøre det, er det nødvendigt, at vi har aktive politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

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

Beskrivelse af behandling

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

- **FilArkiv:** Ifølge hovedaftalen stiller JO Informatik et filarkivsystem til rådighed for kunden til opbevaring, strukturering og publicering af byggesager.
- **Insight Tools:** Ifølge hovedaftalen leverer JO Informatik en webbaseret løsning, der bl.a. kan anvendes til dokumentrensning i forbindelse med aktindsigtssager. Dokumentrensning, også kaldet "redact", omhandler redigering af PDF-filer inklusive screeninger og "redact" af personoplysninger og følsomme oplysninger.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om:

- **FilArkiv:** Opbevaring og publicering
- **Insight Tools:** Fjerne følsomme oplysninger inden publicering/aktindsigt

Personoplysninger

- **Almindelige personoplysninger**, herunder identifikationsoplysninger som navn og adresse
- **Særlige kategorier af personoplysninger** Der kan være tilfælde, hvor handicapadgang kan være nævnt
- Andre personlige oplysninger, herunder oplysninger om cpr-numre.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Borgere
- Virksomheder
- Ansatte

Tredjelandsoverførsler

Vi overfører ikke til tredjelande.

3 Vores implementerede kontroller

Vi har i virksomheden implementeret en række kontroller med henblik på at kvalitetssikre og dokumentere kvaliteten i vores ydelser. Alle kontroller, hvad enten de relaterer sig til en processuel eller teknisk handling, har en udførende ansvarshavende, og i visse tilfælde også en ansvarshavende godkender.

Vores kontroller er rettet mod dels konkrete arbejdshandlinger, dels processer for en række arbejdshandlinger, hvilket kan have konkrete kontroller tilknyttet yderligere. Konkrete arbejdshandlinger er beskrevet i vores Standard Operating Procedure (SOP) dokumenter.

Tidsangivelse for en given kontrol opgives altid over en periode, også selvom en given kontrol oftest måtte blive praktisk udført i en bestemt måned år efter år.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002 (Regelsæt for styring af Informationssikkerhed), og er dermed helt overordnet inddelt i følgende kontrolområder:

4. Risikovurdering og -håndtering
5. Informationssikkerhedspolitikker
6. Organisering af Informationssikkerhed
7. Medarbejdersikkerhed
8. Styring af aktiver
9. Adgangsstyring
10. Kryptografi
11. Fysisk sikring og miljøsikring
12. Driftssikkerhed
13. Kommunikationssikkerhed
14. Anskaffelse, udvikling og vedligeholdelse af systemer
15. Leverandørforhold
16. Styring af sikkerhedsbrud
17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetablering
18. Overensstemmelse

Det følgende beskriver vores kontrolmiljø nærmere for hvert enkelt område:

4 Risikostyring

Alle trusler vurderes systematisk og ensartet. For at tilsikre transparens, overskuelighed og dokumentation benyttes en fastlagt klassifikationsmetode. Identifikation, analyse og vurdering af risici med betydning for vores forretning kan tage afsæt i både udefra kommende trusler og interne forhold.

Risikovurdering er en fast del af alle arbejds- og udviklingsprocesser, både til sikring af vores produktkvalitet, forventningsafstemning med Kunder, og ikke mindst integriteten af vores forretningsplatform.

Risikovurdering foretages således både periodisk (på øverste ledelsesniveau minimum én gang årligt), samt på daglig basis når der indgår ønsker fra kunder, foretages ændringer eller implementeres nye systemer.

5 Informationssikkerhedspolitikker

I vores it-sikkerhedspolitik har vi beskrevet, hvordan vi tilsikrer informationssikkerhed i vores forretning. Vores it-sikkerhedspolitik kan ikke fraviges, hverken for kunder, ansatte eller leverandører, og det er virksomhedens ledelse, der godkender retningslinjer og foretager de nødvendige opdateringer af samme.

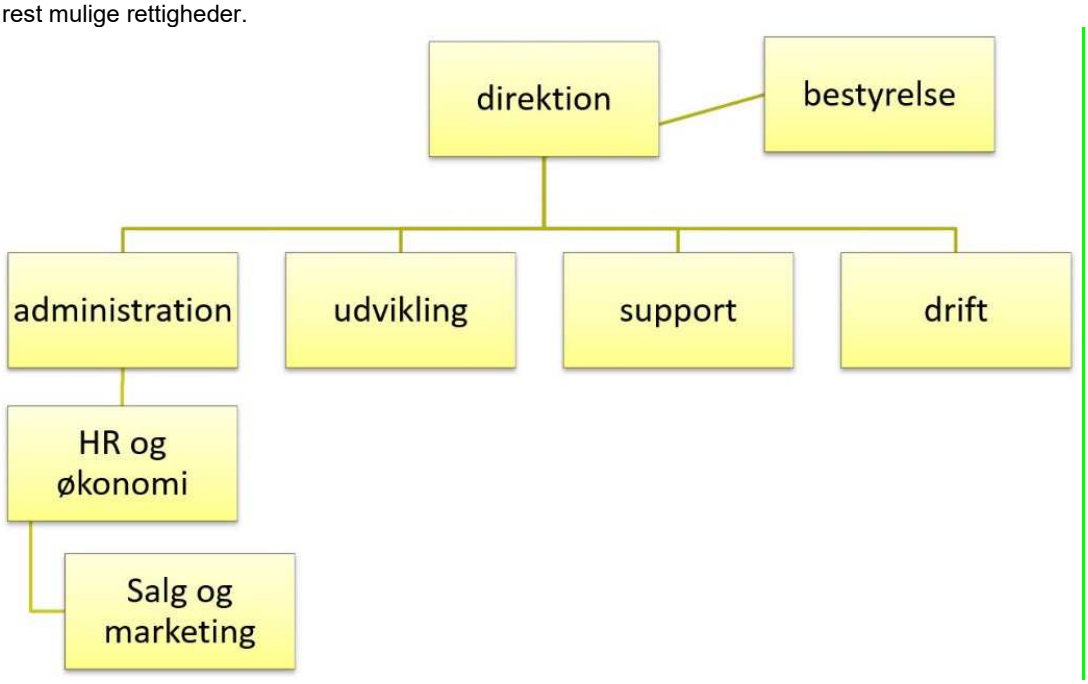
Virksomhedens it-sikkerhedspolitik opdateres såfremt, der foretages ændringer eller implementeres nye forretningsområder, og politikken gennemgås i sin helhed minimum én gang årligt. Når vi har ændret ting i it-sikkerhedspolitikken, og minimum efter den årlige gennemgang, fremlægges ændringerne internt ved førstkommende firmamøde for personalet. Ligeledes bliver eksterne leverandører mf. inddraget og orienteret, såfremt det har relevans.

Det er virksomhedens administrerende direktør, som er ansvarlig for virksomhedens informationssikkerhed, og som godkender denne.

6 Organisering af informationssikkerhed

6.1 Intern organisering

Ansvaret for informationssikkerhed er dokumenteret og forankret på alle niveauer i organisationen – se også figur med organisationsdiagram. Vores dokumentation og definerede processer sikrer generelt, at vi minimerer nøglepersonsafhængighed. Vi tildeler rettigheder på baggrund af funktion/rolle, og der tildeles altid efter princip om færrest mulige rettigheder.



6.2 Mobilt udstyr og fjernarbejdspladser

Vi har udarbejdet en politik, som redegør for retningslinjer for brugen af mobile enheder (lap- tops, mobiltelefoner etc.), så alle medarbejdere er bekendt med reglerne før tilslutning til virksomhedens netværk eller mail system. Reglerne er del af ansættelsesforholdet.

Alle mobiltelefoner er sikret med en række sikkerhedspolitikker via Exchange, herunder er der opsat regler for enhedsgodkendelse, hvorefter det bliver muligt at synkronisere e-mail og kalender data ned på enheden.

Følsomme data og persondata må alene opbevares på serverrumsmedier, eller som midlertidige arbejdskopier på udstyr, der ikke forlader kontoret og som bortskaffes på sikker og forsvarlig vis.

7 HR- og medarbejder relaterede kontroller

Vi har faste procedurer for de aktiviteter og kontroller, der relaterer sig til før-, under- og efter ansættelse af medarbejdere. Det er vores HR-ansvarlige, som er praktisk ansvarlig for de HR-relaterede kontroller.

For konsulenter, som skal have adgang til (dele af) vores netværk, udarbejdes altid en opgavespecifik kontrakt, herunder en dedikeret fortrolighedserklæring, og anden relevant dokumentation indhentes.

Det er virksomhedens direktør, som er ansvarlig for, at alle HR-processer og procedurer overholdes. Den tekniske oprettelse af medarbejdere såvel som konsulenter, foretages i henhold til føromtalte processer, som hver har tilknyttet et antal relevante SOP'er. Vi har desuden en proces for løbende kontrol af alle brugere med rettigheder til virksomhedens netværk.

Medarbejdere, og eksterne parter når relevant, bliver uddannet og trænet i vores retningslinjer for IT-sikkerhed og de deraf afledte opgaver. Dette foregår igennem strukturerede introduktioner mv.

8 Styring af aktiver

8.1 Ansvar for aktiver

Alle aktiver ejes helt og fuldstændigt af JO Informatik. Registrering af virksomhedens aktiver varetages af virksomhedens interne IT-ansvarlige, som registrerer al ejet hardware og egne softwarelicenser. Småanskaffelser som mus, tastaturer, og dockingstations registreres ikke.

Virksomheden har faste regler for brugen af aktiver, samt behandling af informationer på disse. Reglerne er integreret i ansættelseskontrakterne, samt i personalehåndbogen og IT-Sikkerhedspolitikken. Alle medarbejdere er forpligtet til at læse personalehåndbogen ved ansættelsens begyndelse, samt opfølgning ved ændringer, der er relevant for de enkelte medarbejdere.

Virksomheden har faste procedurer til inddrivelse af IT-aktiver ved ophør af et medarbejderforhold.

8.2 Klassifikation af information

Vi har interne regler for opbevaring af særlige datatyper, f.eks. kundedata, hr/personaledata, salgsoplysninger osv. Personalet gøres bekendt med disse regler via den medarbejdervendte IT- sikkerhedspolitik, samt personlig introduktion i forbindelse med jobstart.

8.3 Mediehåndtering

Alle data lagret på flytbare medier (serverrumsmedier undtaget), skal opbevares krypteret, og USB-medier og eksterne harddiske tillades i udgangspunktet ikke. I tilfælde af, at sådanne medier til særlige sager skal benyttes, skal disses data krypteres.

Bortskaffelse og reparation af serverrumsmedier og infrastrukturkomponenter varetages af JO Informatik. Medier uden for serverrummet, som ikke længere kan/skal repareres, bliver opbevaret hos os selv, indtil de bliver destrueret. Fysiske diske, som ikke skal genbruges, destrueres med hammer.

9 Adgangsstyring

9.1 Forretningsmæssige krav til adgangsstyring

Vi har en dokumenteret proces for tildeling af adgange. Dette er ligeledes en del af vores IT- sikkerhedspolitik.

9.2 Administration af brugeradgang

Vores kunders brugere oprettes, ændres og nedtages alene på baggrund af krav fra vores kunder. Interne brugere, herunder brugere med privilegerede rettigheder, oprettes alene på baggrund af skriftligt ønske dokumenteret i vores HR-proces. Alle brugere er personhenførbare. For servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig log ind deaktiveret. Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode. Interne brugere og deres adgangsniveau gennemgås periodisk.

9.3 Brugernes ansvar

Hver medarbejder er ansvarlig for at sikre egne logininformationer, og retningslinjer for samme oplyses i Medarbejderhåndbogen.

9.4 Styring af system- og applikationsadgang

Vores kunders brugeradgange til deres systemer og data er bestemt af dem selv. Adgange for vores medarbejdere er altid funktionsbestemt. Vi arbejder i segmenterede netværk, med GPO'er og alene med identificerbare brugere.

10 Kryptografi

Udveksling af kundedata udvekslet over internettet sendes over krypteret protokol. Certifikat-administration varetages af en ekstern leverandør.

11 Fysisk sikring og miljøsikring

11.1 Sikre områder

Vi har en skalsikring med vagtordning, der sikrer mod, at uautoriserede personer får adgang til virksomhedens område. Gæster til huset må ikke gå uledsaget rundt. Vores kontor og serverrum er beliggende på 2. sal i bygningen. Bygningen er aflåst, vores virksomhed er aflåst og serverrummet er yderligere aflåst, hvor kun autoriseret teknisk personale har adgang. Serverrummet har egen alarmzone, temperaturovervågning, og køling.

Selve bygningen er fredet, og er tilknyttet Helsingør Kommunes Beredskab, som holder løbende, proaktivt tilsyn med bygningen. Et beredskab aktiveres, såfremt alarm(er) aktiveres.

Vores driftsservere er fysisk placeret hos Global Connect. I den forbindelse indhenter vi årligt en ISAE3402- II erklæring fra dem, og vi foretager et fysisk inspektionsbesøg hos Global Connect, ligeledes årligt.

11.2 Udstyr

Vores teknik rum, som indeholder krydsfelt, backup, testmiljø og linjeindgang, har eget kølingsanlæg og temperaturovervågning med tilknyttet fast beredskab. Når udstyr skal destrueres, overdrages det til sikkerhedsgodkendt leverandør, til destruktion på forsvarlig vis.

12 Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder

Vi har dokumenterede driftsprocedurer og aftaler med vores primære datacenterleverandør. Vores systemdokumentation opdateres løbende.

Vores datacenterleverandør har ansvar for al netværksovervågning og 'serverrum services', herunder strøm, køling mv. Vi håndterer selv patch management, firmware, OS sikkerhed, monitorering af kapacitet, servicetilgængelighed og backup. Desuden udføres alle applikationsspecifikke ændringer af os selv, efter en fastlagt dokumenteret proces.

Hver applikation har egen, systemspecifik overvågning. Her monitoreres eksempelvis afvikling af vigtige jobs, fejl logs mv.

12.2 Beskyttelse mod malware

Vi beskytter os blandt andet ved hjælp af antivirus software, e-mail skanning og IPS services.

12.4 Logning og overvågning

Vi har en politik for hhv. logning af netværkshandlinger og handlinger på vores virtuelle servere.

Netværkslogning (firewall og netværksenheder) gemmes i en fælles logserver for at beskytte log informationerne i fald udstyret kompromitteres.

Netværkshændelser relateret til vores infrastruktur og serverrumsydelser håndteres af vores IT- leverandør Global Connect, som uden for almindelig kontortid har driftsvagt.

Vi udfører ugentlig manuelle gennemgange og rapporteringer af loghændelser, som udsendes til ansvarlige.

12.6 Sårbarhedsstyring

For infrastruktur og serverrum varetages opgaven af vores interne it-ansvarlige. For vores egne applikationer og services holder vi os opdateret via relevante faglige og tekniske fora. Vi abonnerer desuden på adviseringer fra DKCERT og CSIS.

13 Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

Vores dokumentation og arbejdsprocesser medvirker til at sikre en stabil, korrekt og driftssikker ydelse, hvor personafhængighed og utilsigtede fejl minimeres.

Vi har en opdeling af vores domæne og benytter dedikerede miljøer. Servere, placeret i et dedikeret domæne med eget AD, er derfor både fysisk og logisk isoleret fra de øvrige servere placeret i andre VLAN.

Trafik mellem de forskellige VLAN er begrænset således: Det er defineret ud fra en source IP, destinations IP samt, hvilke services der skal være åbnet for.

Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv.

13.2 Informationsoverførsel

Vi har regler for udveksling af data med kunder, og behandling af kundedata må aldrig forgå over e-mail eller andre åbne kommunikationskanaler.

Implementering af og leverancer til nye kunder foretages i henhold til fastlagte procedurer og relevante SOP'er. En repræsentant fra vores Salg og Ledelse skal godkende kundeopsætningen, hvorfor der sikres overensstemmelse med kontrakt, teknik og forretningskrav.

Vi har ligeledes regler for udveksling af kundedata via internettet. Vi benytter desuden krypteret VPN-tunnel til anvendelse af udstyr på distance, og vi anvender IP adressefiltrering på alle offentlige tilgængelige webservices for vores kunde. De borgerrettede webservices er placeret i dedikeret zone.

Vi har databehandleraftaler med alle vores kunder.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

Vi har en fast procedure for vurdering af sikkerhedskrav og risici, ved anskaffelse, udvikling og vedligeholdelse af vores systemer.

14.2 Sikkerhed i udviklings- og hjælpeprocesser

Vores retningslinjer for udvikling og ændringshåndtering indeholder faste kriterier for sikkerhedsrelaterede vurderinger, herunder ledelses- og når relevant, kundegodkendelser. Vi har dertil en formel godkendelsesproces for godkendelse af opdateringer, inkluderende test og roll-back planer, for hvert udviklingstrin/produkt.

14.3 Testdata

Vi har et separat testmiljø. Testmiljø og testdata beskyttes på samme måde som produktionsdata, og testdata slettes straks efter brug.

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

Eventuelle leverandører, der vil optræde som databehandlere, skal til enhver tid efterleve vores IT-sikkerhedspolitik, ligesom visse leverandører skal kunne dokumentere deres kvalitet ved at fremvise relevant revisorerklæring uden anmærkninger.

Kundeaftaler har tilsvarende klausuler om informationssikkerhed, særligt i forhold til hvilke forhold kunden selv er ansvarlig for (eksempelvis egen brugeroprettelse).

15.2 Styring af leverandørydelser

Vi har ingen leverandører, som har adgang til vores kundedata og/eller fortrolige eller følsomme data.

For leverandører og konsulenter, som får adgang til vores netværk, er forhold omhandlende fortrolighed og it-sikkerhed altid en del af aftalegrundlaget.

16 Styring af informationssikkerhedsbrud

Såfremt et informationssikkerhedsbrud indtræffer:

- Aktiveres vores beredskabsplan
- Hvor det er relevant, indsamles beviser
- Kunder orienteres

Vurdering af sikkerhedshændelser foretages af den IT-ansvarlige i samarbejde med virksomhedens direktør.

Efter en hændelse evalueres alle relevante retningslinjer og sikkerhedsforanstaltninger samt risikoanalysen og beredskabsplanen. Dette sker med henblik på at sikre læring af hændelsen, og at undgå at hændelse indtræder igen (hvis muligt).

Ved kriminelle forhold, hvor der sker en politimæssig efterforskning, vil vores logføring og øvrige overvågning blive videregivet til relevante myndigheder med henblik opklaring og evaluering af sikkerhedshændelsen.

17 Beredskabsstyring

Katastrofer søges undgået/begrænset gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Risikoanalyse og beredskabsplaner omfatter skadebegrænsende tiltag, etablering af temporære nødløsninger og genetablering af permanent løsning. Minimum en gang om året testes (dele af) beredskabsplanen, hvor vi foretager en simulation af et udvalgt beredskabsudløsende scenarie.

Desuden er vores infrastruktur designet med særlige hensyn til redundans, og vi arbejder på at idriftsætte et dedikeret D/R site.

18 Overensstemmelse

JO Informatik er ikke underlagt særlovgivning for nuværende. Vi har heller ikke særlige interessegrupper for nuværende. Vores kunder kan være underlagt yderligere lovgivning, og hvor det måtte være tilfældet, er vores understøttelser heraf aftalt særskilt.

Vi har en række interne kontroller for at tilsikre en til alle tidsværende overensstemmelse med interne politikker, procedurer og den faktisk drift. Disse dækker også teknisk overensstemmelse.

Vi er desuden underlagt årlig IT-revision af ekstern, uafhængig, revisor.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

Komplementerende kontroller hos de dataansvarlige

Medmindre andet er aftalt, er vores kunder selv ansvarlige for at etablere forbindelse til vores servere. Desuden er vores kunder selv ansvarlige for, medmindre andet er aftalt, at:

i) Det aftalte niveau for backup dækker kundens behov
ii) Brugeradministration, herunder anmodninger om oprettelse og nedtagning af bruger, og periodisk gennemgang, af kundens egne brugere
iii) At sporbarhed opretholdes i tredjepartssoftware, som kunden selv administrerer
iv) At kundespecifikke softwareløsninger understøtter den af os udbudte backup teknologi
v) Særaftale for backupjobs der kræver krypteringspassword, hvor kunden alene er ansvarlig for håndtering og opbevaring af krypteringspassword
vi) Anmodning om adgang til kundens servermiljø for kundens tredjepartsleverandører, og
vii) Kundens anmeldelse til Datatilsynet, for hvem dette måtte være relevant.

Afsnit 2: JO Informatik ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for JO Informatik ApS' kunder, som har indgået en databehandleraftale med JO Informatik ApS, 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.

JO Informatik ApS anvender underleverandøren Global Connect. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos JO Informatik ApS' underleverandør. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i JO Informatik ApS' beskrivelse i afsnit 1 af FilArkiv og Insight Tools, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos JO Informatik ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

JO Informatik ApS bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af, hvordan JO Informatik ApS har behandlet personoplysninger på vegne af dataansvarlige pr. 20. december 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan JO Informatik ApS' processer og kontroller relateret til databeskyttelse 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 JO Informatik ApS' 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) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne FilArkiv og Insight Tools 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 FilArkiv og Insight Tools, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 20. december 2022, hvis relevante kontroller hos underleverandører var operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af JO Informatik ApS pr. 20. december 2022. 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, og

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

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

Helsingør, den 8. marts 2023
JO Informatik ApS

Jesper Olsen
Adm. direktør

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder pr. 20. december 2022

Til JO Informatik ApS og JO Informatik ApS' kunder i rollen som dataansvarlige

Omfang

Vi har fået til opgave at afgive erklæring med høj grad af sikkerhed om JO Informatik ApS' beskrivelse i "Afsnit 1" af FilArkiv og Insight Tools i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig pr. 20. december 2022 og b) om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

JO Informatik ApS anvender underleverandøren Global Connect. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos JO Informatik ApS' underleverandør. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlernes kontroller, der forudsættes i designet af JO Informatik ApS´ kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos JO Informatik ApS.

Enkelte af de kontrolmål, der er anført i JO Informatik ApS' beskrivelse i afsnit 1 af FilArkiv og Insight Tools, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos JO Informatik ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

JO Informatik ApS' ansvar

JO Informatik ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i "Afsnit 2", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme og implementere kontroller for at opnå de anførte kontrolmål.

Grant Thorntons uafhængighed og kvalitetsstyring

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

Grant Thornton anvender international standard om kvalitetsstyring, ISQC 1[1] , og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

Grant Thorntons ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om JO Informatik 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, 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af FilArkiv og Insight Tools samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke er implementeret. Vores handlinger har omfattet test af implementeringen 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 databehandler

JO Informatik 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 FilArkiv og Insight Tools, 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. Det er vores opfattelse,

(a) at beskrivelsen af FilArkiv og Insight Tools, således som denne var udformet og implementeret pr. 20. december 2022, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 20. december 2022, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandør var operationelt effektive, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af JO Informatik ApS' kontroller pr. 20. december 2022.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i det efterfølgende afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt JO Informatik ApS' FilArkiv og Insight Tools, 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.

København, den 8. marts 2023

Grant Thornton
Statsautoriseret Revisionspartnerselskab

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Christian H. Riis
Executive director, CISA

Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

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

Vores test af udformningen har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-I nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået pr. 20. december 2022.

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos JO Informatik ApS' underleverandør.

Kontroller udført hos de dataansvarlige er ikke omfattet af vores erklæring.

Vi har udført vores tests af kontroller hos JO Informatik ApS via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos JO Informatik ApS. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af 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.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Kortlægning af kontrolområder op mod GDPR-artikler, ISO 27701 og ISO 27001/2

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2.

Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Nyt område ift. ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Nyt område ift. ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har inspiceret databehandleraftale, og påset, at instruksen i denne er i overensstemmelse med informationssikkerhedspolitikken. Vi har inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har forespurgt, om databehandleren har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi er blevet informeret om, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, hvorfor vi ikke har testet implementeringen af relevante procedurer. Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er krav om overholdelse af aftalte sikringsforanstaltninger. Vi har påset, at politikken er opdateret.	Ingen 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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Vi har inspiceret, at den foretagne risikovurdering er opdateret og at den omfatter den aktuelle behandling af personoplysninger.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har stikprøvevis inspiceret opbevaring af personoplysninger, og stikprøvevis påset, at der er implementeret beskyttelse mod malware, som løbende opdateres.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Vi har inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugernes adgang til personoplysninger. Vi har inspiceret adgange, og påset, at de er baseret på et arbejdsbetinget behov.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har inspiceret, at der er opsat systemovervågning med alarmering.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevis inspiceret transmission over nettet, og stikprøvevis påset, at transmission sker med kryptering.	Ingen afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til logning. Vi har stikprøvevis inspiceret logopsætningen for servere og systemer, og stikprøvevis påset, at disse stemmer overens med politikken.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der er procedurer for håndtering af personoplysninger i forbindelse med udvikling. Vi har inspiceret anvendelse af dummy-data til udvikling.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer. Vi har inspiceret ændring, og påset, at denne følger den interne procedure.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
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.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har inspiceret dokumentation for, at en fratrådt medarbejders adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Vi har inspiceret, at der foreligger dokumentation for regelmæssig – og mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.
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.	Vi har inspiceret dokumentation for anvendelse af to-faktor i forbindelse med adgang til systemer.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til den fysiske sikkerhed. Vi har inspiceret, at databehandleren har en oversigt over relevante nøgler til kontor og datacenter.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret databehandleraftale, og påset, at instruksen i denne er i overensstemmelse med informationssikkerhedspolitikken. Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har inspiceret dokumentation for, at proceduren er blevet fulgt.	Ingen 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.	Vi har inspiceret, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale. Vi har inspiceret dokumentation for, at nyansatte medarbejder er blevet introduceret til relevante politikker og procedurer.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget fra tidligere medarbejdere.	Ingen 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.	Vi har inspiceret ansættelsesaftaler, og påset, at fortrolighed gælder efter ansættelse.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til IT-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne, omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	Vi har inspiceret dokumentation for, at databehandleren har vurderet behov for en databeskyttelsesrådgiver.	Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har forespurgt til seneste ophørte databehandleraftale.	Vi er blevet informeret om, at der ikke har været ophørte databehandlinger, hvorfor vi ikke har testet implementeringen af databehandlerens procedurer. Ingen afvigelser konstateret.
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.	Vi har forespurgt til seneste ophørte databehandleraftale.	Vi er blevet informeret om, at der ikke har været ophørte databehandlinger, hvorfor vi ikke har testet implementeringen af databehandlerens procedurer. Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der er procedurer for overholdelse af instrukser fra dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har inspiceret seneste databehandleraftale, og påset, at lokation for behandling fremgår heraf.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af 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.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har inspiceret databehandleraftaler med dataansvarlige, og påset, at der er taget stilling til underdatabehandlere. Vi har forespurgt til, om databehandleren har underdatabehandlere.	Vi er blevet informeret om, at databehandleren ikke anvender underdatabehandlere. Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af 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.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
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.	Vi har inspiceret proceduren for udskiftning af underdatabehandlere, og påset, at der er taget stilling til håndtering af leverandører. Vi har forespurgt til, om der har været udskiftninger eller ændringer af leverandører.	Vi er blevet informeret om, at der ikke er blevet udskiftet leverandører. Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har inspiceret databehandleraftaler med dataansvarlige, påset, at er taget stilling til underdatabehandlere. Vi har forespurgt til, om databehandleren har underdatabehandlere.	Vi er blevet oplyst, at JO Informatik ApS ikke har underdatabehandlere. Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret seneste indgået databehandleraftaler med dataansvarlige. Vi har forespurgt til, om databehandleren har underdatabehandlere.	Vi er blevet oplyst, at JO Informatik ApS ikke har underdatabehandlere. Ingen 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.	Vi har inspiceret dokumentation for, at databehandleren har udført tilsyn med leverandør.	Vi er blevet oplyst, at JO Informatik ApS ikke har underdatabehandlere. Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

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.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret proceduren for onboarding af kunder, og påset, at der skal tages stilling til tredjelandsoverførsler i databehandleraftaler. Vi har forespurgt til, om databehandleren overfører til tredjelande. Vi har inspiceret databehandleraftale, og påset, at der er taget stilling til tredjelandsoverførsler.	Vi er blevet informeret om, at databehandleren ikke overfører til tredjelande, og finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har inspiceret, at databehandleren har procedurer for håndtering af tredjelandsoverførsler. Vi har forespurgt til, om databehandleren overfører til tredjelande. Vi har inspiceret databehandleraftale, og påset, at der er taget stilling til tredjelandsoverførsler.	Vi er blevet informeret om, at databehandleren ikke overfører til tredjelande, og finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har forespurgt til, om databehandleren overfører til tredjelande. Vi har inspiceret databehandleraftale, og påset, at der er taget stilling til tredjelandsoverførsler.	Vi er blevet informeret om, at databehandleren ikke overfører til tredjelande, og finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Kontrolmål H – De 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.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser 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.	Vi har forespurgt, om databehandleren har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder.	Vi er blevet informeret om, at databehandleren ikke har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder, hvorfor vi ikke har testet implementeringen af databehandlerens procedurer. Ingen afvigelser konstateret

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	*JO Informatik ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har forespurgt, om der har været persondatassikkerhedsbrud.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet implementering af databehandlerens procedurer. Ingen afvigelser konstateret
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.	Vi har inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden. Vi har forespurgt, om der har været persondatassikkerhedsbrud.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet implementering af databehandlerens procedurer. Ingen afvigelser konstateret

PENNEO

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

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

Jesper Riis Olsen
JO INFORMATIK ApS CVR: 15144092
Underskriver 1
Serienummer: 55403ab6-a278-470e-b907-9a8e883d056a
IP: 80.63.xxx.xxx
2023-03-08 15:51:02 UTC
MitID

Christian H. Riis
Underskriver 2
Serienummer: CVR:34209936-RID:62278486
IP: 62.243.xxx.xxx
2023-03-08 15:55:06 UTC
NEM ID

Jacob Helly Juell-Hansen
Underskriver 3
Serienummer: CVR:34209936-RID:50904197
IP: 62.243.xxx.xxx
2023-03-09 14:02:19 UTC
NEM ID