et trygt samfund med it og data

Revisorerklæring

CVR Nr.: 15 14 40 92

JO Informatik ApS

Erklæring fra uafhængig revisor – ISAE 3000
Erklæringsafgivelse i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov som databehandler for leverancen af driftsaktiviteter i forhold til Filarkiv for perioden 01-07-2019 til 30-06-2020

REVI-IT A/S | www.revi-it.dk
Jens Kofods Gade 1, 1268 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Juli 2020

Indholdsfortegnelse

Afsnit 1: JO Informatik ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for JO informatik ApS' kunder, som i rollen som dataansvarlige, har anvendt Filarkiv, 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 bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 2, giver en retvisende beskrivelse af Filarkiv, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 01-07-2019 til 30-06-2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Filarkiv 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 Filarkivs afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Indeholder relevante oplysninger om ændringer ved databehandlerens Filarkiv til behandling af personoplysninger foretaget i perioden fra 01-07-2019 til 30-06-2020

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne Filarkiv 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, 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 01-07-2019 til 30-06-2020. 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 01-07-2019 til 30-06-2020.

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, 30. juli 2020

JO informatik ApS

Jesper Olsen
Adm. direktør

Afsnit 2: JO informatik ApS' beskrivelse

1 Indledning

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

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.

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 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, og for at tilsikre transparens, overskuelighed og dokumentation, benyttes 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 produkt-kvalitet, 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

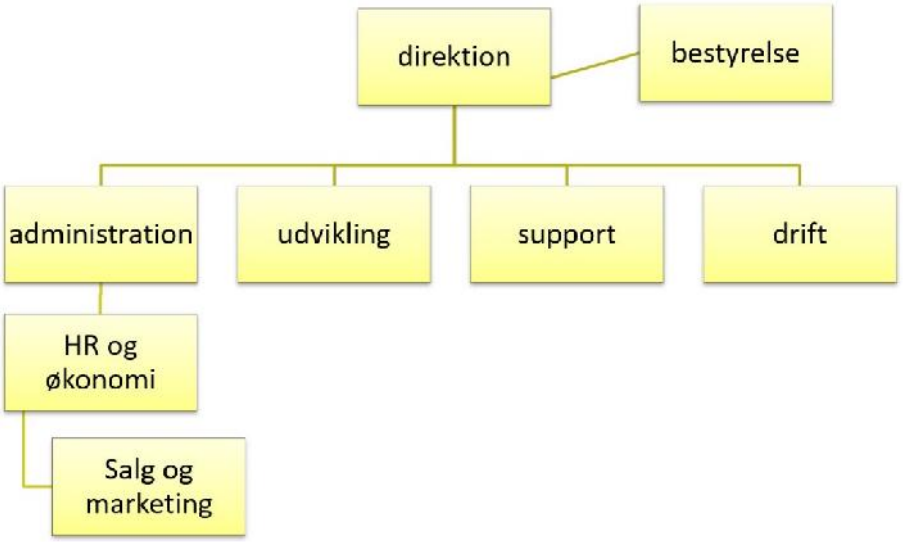
Vi har i vores it-sikkerhedspolitik beskrevet hvordan vi tilsikrer informationssikkerhed i vores forretning. Vores it-sikkerhedspolitik kan ikke fraviges, hverken for kunder, ansatte eller leverandører, og det er virksomhedens ledelse der godkender retningslinjer og foretager de nødvendige opdateringer 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. 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 (laptops, 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 medarbejderrelaterede 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 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 docking stationer registreres ikke.

Virksomheden har faste regler for brugen af aktiver, samt behandling af informationer på disse. Reglerne er integreret i ansættelseskontrakterne, samt i personalehåndbogen. 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-medie 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

Virksomheden 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, og serverrummet er yderligere aflåst, hvor kun autoriseret teknisk personale har adgang. Serverrummet har egen alarmzone, temperatur-overvågning, 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.

12.3 Backup

Vi har en detaljeret procedure for sikkerhedskopiering og Continuity Management.

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, som uden for almindelig kontortid har driftsvagt.

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

12.5 Styring af driftssoftware

Vedligeholdelse af operativsystem og infrastrukturkomponenter foretages månedligt i et fastlagt service vindue. Vi håndterer alle applikationsspecifikke ændringer selv, efter en fastlagt dokumenteret proces.

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, og er derfor både fysisk og logisk isoleret fra de øvrige servere placeret i andre VLAN.

Trafik mellem de forskellige VLAN er begrænset, således er det 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 godkendelses-proces 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

Vores leverandører (databehandlere) skal til hver en tid efterleve vores IT-sikkerhedspolitik, ligesom visse leverandører skal kunne dokumentere deres kvalitet, ved at fremvise relevant revisorerklæring uden anmærkninger. Dette er en del af aftaleforholdet, og kontrolleres minimum en gang årligt.

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 de konsulenter vi benytter, som har privilegerede adgange, har vi databehandleraftaler med.
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 osv. Vurdering af sikkerhedshændelser foretages af den IT-ansvarlige i samarbejde med virksomhedens direktør.

Efter en hændelse, evalueres alle relevante retningslinjer og sikkerhedsforanstaltninger, risikoanalysen og beredskabsplanen, 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 på at benytte oplysningerne til opklaring og evaluering af sikkerhedshændelsen.

17 Beredskabsstyring

Katastrofer søges undgået 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 beredskabs-udløsende 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.

19 Væsentlige ændringer i perioden

Intet af relevans

20 Komplimenterende kontroller

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 3: Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov i perioden 01-07-2019 til 30-06-2020

Til JO informatik ApS' ledelse, selskabets kunder i rollen som dataansvarlige og disses revisorer

Vi har efter aftale undersøgt JO informatik ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov for perioden 01-07-2019 til 30-06-2020 i rollen som databehandler for ydelsen Filarkiv.

Erklæringen er alene udarbejdet til brug for JO informatik ApS' ledelse, selskabets kunder i rollen som dataansvarlig og disses revisorer til vurdering af de tilrettelagte forretningsgange, og kan ikke anvendes til andre formål.

Ledelsens ansvar

Ledelsen i JO informatik ApS har ansvaret for at implementere og sikre opretholdelsen af forretningsgange som krævet af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

Revisors ansvar

Det er vores ansvar, på grundlag af det udførte arbejde, at udtrykke en konklusion om, hvorvidt selskabet overholder de krav, der er nævnt i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

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 vores konklusion.

REVI-IT A/S er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vores arbejde har omfattet forespørgsler, observationer samt vurdering og stikprøvevis undersøgelse af den information, vi har modtaget.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke afdækkes af vort arbejde. Endvidere vil en anvendelse af vor konklusion på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, ændring i kravene til behandling af oplysninger eller i selskabets overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion eventuelt ikke længere vil være gældende.

Begrænsninger i kontroller hos en dataansvarlig

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, 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

Denne konklusion er udformet på grundlag af forståelsen af de kriterier, som der er redegjort for i erklæringens indledende afsnit, og som bygger på kravene i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov**.**

Det er vores opfattelse, at JO informatik ApS, i alle væsentlige henseender, lever op til ovennævnte kriterier for perioden 01-07-2019 til 30-06-2020.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt JO informatik ApS' Filarkiv i deres rolle som dataansvarlig, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov er overholdt.

København, 30. juli 2020

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Basel Rimon Obari
It-revisor, CISA, CISM, Partner

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

Den følgende oversigt er udformet for at skabe et overblik over de kontroller, som JO informatik ApS har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte artikler for perioden 01-07-2019 til 30-06-2020 er efterlevet.

De krav, som fremgår direkte af forordningen eller loven, kan ikke fraviges. Derimod kan der justeres på, hvordan sikkerheden implementeres, da sikkerhedskravene i forordningen på flere punkter er af mere generel og overordnet karakter, som bl.a. skal tage hensyn til formål, behandlingens karakter, kategorien af personoplysninger mv. Herudover kan der være konkrete krav i de enkelte kundekontrakter, der kan have en rækkevidde, der går ud over databeskyttelseslovens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos JO informatik ApS' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

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

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv udført – eller har observeret – en genudførelse af kontroller med henblik på at verificere, at kontrollen fungerer som forventet

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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at virksomheden alene må behandle data efter instruks fra de dataansvarlige. Vi har inspiceret informationssikkerhedspolitikken, og påset, at denne er blevet opdateret i perioden.	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har inspiceret informationssikkerhedspolitikken og stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at disse er i overensstemmelse.	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 informationssikkerhedspolitikken, og påset, at virksomheden kun behandler personoplysninger efter lovlig instruks.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er krav om overholdelse af aftale om sikringsforanstaltninger.	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 risikoanalysen, og påset, at denne tager udgangspunkt i relevante behandlingsaktiviteter. Vi har inspiceret analysen, og påset, at denne er blevet opdateret i perioden.	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 servere, og stikprøvevis påset, at antivirus er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret oversigt over firewalls, og stikprøvevis inspiceret konfigurationen af disse.	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 netværks-diagrammer, liste over servere og andre netværkskomponenter, og påset, at netværket er segmenteret.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret proceduren for adgangsstyring, og påset, at der er taget stilling til arbejdsbetinget behov for adgange. Vi har stikprøvevis inspiceret oversigt over adgange, og stikprøvevis påset, at der er et arbejdsbetinget behov.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har stikprøvevis inspiceret overvågning af systemer, backups og servere, og stikprøvevis påset, at der er etableret alarmer. Vi har stikprøvevis inspiceret overvågning af certifikater, og påset, at virksomheden fører tilsyn med certifikater.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevis inspiceret overvågning af certifikater, og stikprøvevis påset, at de bliver overvåget.	Ingen afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til logning. Vi har stikprøvevis inspiceret logopsætningen for servere og systemer, og stikprøvevis påset, at disse stemmer i 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 proceduren for udvikling, og påset, at denne er blevet opdateret i perioden. Yderligere har vi inspiceret proceduren, og påset, at der er taget stilling til personoplysninger i forbindelse med udvikling. Vi har stikprøvevis inspiceret udviklingssager, og stikprøvevis påset, at disse stemmer i overens med proceduren.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests. Vi har inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Vi har inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	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 proceduren for ændringer, og stikprøvevis påset, at ændringer i perioden følger proceduren. Vi har stikprøvevis inspiceret firmware på switches, og stikprøvevis påset, at disse er opdateret.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til person-oplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret proceduren for adgangsstyring, og påset, at der er taget stilling til tildeling og afbrydelse af brugeradgange. Vi har inspiceret liste over fratrådte medarbejdere i perioden, og stikprøvevis påset, at rettigheder er blevet inddraget.	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 tofaktor autentifikation.	Vi har inspiceret tofaktorløsningen, og påset, at denne er konfigureret i henhold til informations-sikkerhedspolitikken.	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 oversigt over nøgler, og påset, at kun medarbejdere med et arbejdsbetinget behov har adgang til personoplysninger. Vi har inspiceret erklæring fra housingleverandør, og påset, at der er etableret tilstrækkelig fysisk sikring af datacentret.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om IT-sikkerhedspolitikken skal opdateres.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at den tager udgangspunkt i behandlingssikkerhed. Vi har inspiceret ledelses-godkendelse af politikken. Vi har stikprøvevis inspiceret kommunikation til medarbejdere, og stikprøvevis påset, at de er blevet informeret omkring ændringer til politikken. Vi har inspiceret politikken, og påset, at denne er blevet opdateret i perioden.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informations-sikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret informationssikkerhedspolitikken og stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at politikken er i overensstemmelse med aftalerne.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret tjekliste for ansættelser, og påset, at der er taget stilling til efterprøvning af medarbejdere i forbindelse med ansættelse. Vi har forespurgt til, om der har været ansættelser i perioden.	Vi er blevet oplyst, at der ikke har været nye ansættelser i perioden, hvorfor vi ikke har kunne teste effektiviteten af proceduren. Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortroligheds-aftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har inspiceret proceduren for ansættelse, og påset, at der er taget stilling til fortrolighed og introduktion til politiker. Vi har forespurgt til, om der har været ansættelser i perioden.	Vi er blevet oplyst, at der ikke har været nye ansættelser i perioden, hvorfor vi ikke har kunne teste effektiviteten af proceduren. Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors 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 proceduren for fratrædelse, og påset, at der er taget stilling til inddragelse af brugerrettigheder og tilbagelevering af aktiver. Vi har stikprøvevis inspiceret nøglekvittering, og påset, at nøgler er blevet leveret tilbage i forbindelse med fratrædelse.	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 informations-sikkerhedspolitikken, og påset, at der er taget stilling til fortrolighed. Vi har stikprøvevis inspiceret kvitteringer for opsigelse, og påset, dette er sket i overensstemmelse med proceduren.	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 stikprøvevis inspiceret awarenesstræning i perioden, og stikprøvevis påset, at medarbejdere er blevet trænet i IT-sikkerhed.	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 og bliver inddraget i relevante områder.	Vi har inspiceret vurderingen af behovet for en DPO, og påset, at dette er blevet vurderet i perioden.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til at opbevaring og sletning skal ske i overensstemmelse med aftaler.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevis inspiceret nye databehandleraftaler i perioden, og stikprøvevis påset, at der er aftalt opbevaringsperioder og sletterutiner.	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 retningslinjer for sletning og tilbage, Vi har forespurgt til, om der har været ophørte kunder i perioden.	Vi er blevet oplyst, at der ikke har været ophørte kunder i perioden, hvorfor vi ikke har kunne kontrollere hvorvidt data slettes/tilbageleveres i overensstemmelse med retningslinjerne. 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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til, at opbevaring sker i overensstemmelse med aftaler.	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 stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at opbevaring af personoplysninger sker i overensstemmelse med aftalen. Vi har stikprøvevis inspiceret backupjobs og restore i perioden, og påset, at dette er i overensstemmelse med aftalerne.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandler-aftaler og instruks.	Vi har inspiceret proceduren for vurdering af nye leverandører, og påset, at der er krav om databehandleraftale.	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 proceduren for anvendelse af underdatabehandlere og leverandører og forespurgt til hvorvidt nye underdatabehandlere er blevet taget i brug.	Vi er blevet oplyst, at virksomheden ikke anvender underdatabehandlere hvorfor kontrollen vurderes ikke relevant. Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har inspiceret proceduren for anvendelse af underdatabehandlere og leverandører og vi har forespurgt til, om der har været ændringer i anvendte underdatabehandlere i perioden.	Vi er blevet oplyst, at virksomheden ikke anvender underdatabehandlere, og der har heller ikke været ændringer i perioden, hvorfor kontrollen vurderes ikke relevant. 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 proceduren for anvendelse af underdatabehandlere og forespurgt hvorvidt virksomheden anvender underdatabehandlere.	Vi er blevet oplyst, at virksomheden ikke anvender underdatabehandlere hvorfor kontrollen vurderes ikke relevant. Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdata-behandlere.	Vi har inspiceret proceduren for anvendelse af underdatabehandlere og forespurgt hvorvidt virksomheden har en oversigt over godkendte underdatabehandlere.	Vi er blevet oplyst, at virksomheden ikke anvender underdatabehandlere hvorfor kontrollen vurderes ikke relevant. Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
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 forespurgt til løbende tilsyn med Global Connect, som er virksomhedens housingleverandør, og inspiceret, at der er blevet ført tilsyn med dem i perioden.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.	Vi har forespurgt til, om virksomheden overfører til tredjelande.	Vi er blevet oplyst, at virksomheden ikke overfører til tredjelande, hvorfor kontrolmål G vurderes ikke relevant. 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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.	Vi har inspiceret informations-sikkerhedspolitikken, og påset, at der er taget stilling til at bistå de dataansvarlige ved anmodninger.	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 til, om der har været anmodninger i perioden.	Vi er blevet oplyst, at der ikke har været nogen anmodninger i perioden, hvorfor vi ikke har kunne kontrollere hvorvidt JO Informatik besvarer anmodninger fra de registrerede i overensstemmelse med indgåede databehandleraftaler. Vi har imidlertid inspiceret at JO Informatiks system har de nødvendige funktioner hertil. 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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret proceduren for sikkerhedsbrud, og påset, at de dataansvarlige.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har stikprøvevis inspiceret awareness-materiale, og stikprøvevis påset, at medarbejdere bliver trænet i sikkerhedsbrud.	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 persondata-sikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret loggen over hændelser i perioden, og vi har stikprøvevis påset, at data-ansvarlige er blevet informeret omkring hændelserne.	Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet.	Vi har inspiceret procedurerne for sikkerhedsbrud, og påset, at der er etableret bistand til de dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål J – Betingelser for samtykke og oplysningspligt

Der efterleves procedurer og kontroller, som sikrer, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger, og hvori det sikres, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt anden information, der er nødvendig for opfyldelse af oplysningspligten.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
J.1	Der foreligger skriftlige procedurer for indhentelse af skriftligt samtykke til behandling af personoplysninger.	Vi har forespurgt til, om virksomheden indhenter samtykke på vegne af de dataansvarlige.	Vi har fået oplyst, at virksomheden ikke er forpligtet til at indhenter samtykke fra de registrerede i forbindelse med de revidererede ydelser, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret.
J.2	Der er implementeret tekniske foranstaltninger, der sikrer, at det kan dokumenteres, hvilke oplysninger der er givet i forbindelse med indgåelse af samtykket.	Vi har forespurgt til, om virksomheden indhenter samtykke på vegne af de dataansvarlige.	Vi har fået oplyst, at virksomheden ikke er forpligtet til at indhenter samtykke fra de registrerede i forbindelse med de revidererede ydelser, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret.
J.3	Der foreligger skriftlige procedurer, hvori det er beskrevet, hvordan det sikres, at den registrerede modtager oplysninger om formål med behandling af personoplysninger samt oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer, eller hvordan databehandler kan bistå den dataansvarlige hermed.	Vi har forespurgt til, om databehandleren står for oplysningspligten.	Vi har fået oplyst, at virksomheden ikke står for oplysningspligten. Ingen afvigelser konstateret.
J.4	Der foretages løbende – og mindst én gang årligt – kontrol af, at alle registrerede har modtaget beskrivelsen af den registreredes ret til indsigt i, berigtigelse eller sletning af personoplysninger.	Vi har forespurgt til, om databehandleren står for oplysningspligten.	Vi har fået oplyst, at virksomheden ikke står for oplysningspligten. Ingen afvigelser konstateret.

Kontrolmål K – Fortegnelse over behandlingsaktiviteter

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
K.1	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret fortegnelsen, og påset, at denne indeholder kategorier af behandlings-aktiviteter.	Ingen afvigelser konstateret.
K.2	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	Vi har inspiceret fortegnelsen, og påset, at den er blevet opdateret i perioden.	Ingen afvigelser konstateret.
K.3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlings-aktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Vi har inspiceret fortegnelsen, og påset, at denne er blevet godkendt af ledelsen.	Ingen afvigelser konstateret.