

Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af
databeskyttelsesforordningen (GDPR) og tilhørende databeskyt-
telseslov i deres rolle som databehandler pr. 19-07-2019

ISAE 3000-I

JO Informatik ApS

CVR-nr.: 15 14 40 92

juli 2019

Indholdsfortegnelse

JO Informatik ApS' udtalelse	1
Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov pr. 19-07-2019	2
Kontrolmål, udførte kontroller, test og resultater heraf	4

JO Informatik ApS' udtalelse

Denne erklæring vedrører JO Informatik ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

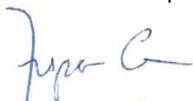
Vi bekræfter, at vi, efter vores opfattelse, i al væsentlighed har overholdt ovennævnte kriterier, pr. 19-07-2019.

Vi bekræfter herudover, at revisor har haft adgang til al information og materiale, som har været nødvendig for erklæringsafgivelsen.

På den baggrund er det vores vurdering, at vi, i al væsentlighed, har udført en hensigtsmæssig drift og administration for vores ydelser.

Helsingør, 19. juli 2019

JO Informatik ApS



Jesper Riis Olsen
Direktør

Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov pr. 19-07-2019

Til JO Informatik ApS' ledelse, selskabets kunder og disses revisorer

Vi har efter aftale undersøgt JO Informatik ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov pr. 19-07-2019.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er alene udarbejdet til brug for JO Informatik ApS' ledelse, selskabets kunder 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 revisorerets 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.

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, pr. 19-07-2019.

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 og beskrivelsen af test af kontroller på side 4-17 er udelukkende tiltænkt JO Informatik ApS' kunder i rollen som dataansvarlige, der har anvendt JO Informatik ApS' som databehandler, og deres revisorer, 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, 19. juli 2019

REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Henrik Paaske

Statsautoriseret revisor



Martin Brogaard Nielsen

It-revisor, CISA, CIPP/E, CRISC, adm. direktør

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 pr. 19-07-2019 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 test
A.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har forespurgt til skriftlige procedurer eller politikker, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks, og vi har inspiceret databehandlerens informationssikkerhedspolitik.</p> <p>Vi har forespurgt til periodisk opdaterer politikken, og vi har inspiceret dokumentation for periodisk opdatering.</p>	Ingen væsentlige afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	<p>Vi har forespurgt til politik eller procedure, hvori ledelsen foreskriver, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Vi har inspiceret informationssikkerhedspolitikken og stikprøvevis inspiceret databehandleraftaler for overensstemmelse med behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.</p>	<p>Vi har observeret, at databehandleren mangler at indhente opdaterede databehandleraftaler fra fem dataansvarlige. Dog har databehandleren indgået databehandleraftaler efter persondataloven med de dataansvarlige, og de har været i kommunikation med de dataansvarlige.</p> <p>Ingen yderligere væsentlige afvigelser konstateret i øvrigt.</p>
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 forespurgt til politik eller procedure for, at databehandleren underretter den dataansvarlige omgående, hvis en instruks strider i mod gældende ret, og 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.	Ingen væsentlige 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 test
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	Vi har forespurgt til politik eller procedure, som indeholder krav om at aftalte foranstaltninger i databehandleraftalerne skal implementeres i virksomheden, og vi har stikprøvevis inspiceret databehandleraftaler og informationssikkerhedspolitikken.	Ingen væsentlige afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har forespurgt til om databehandleren har foretaget en risikovurdering, og vi har inspiceret informationssikkerhedspolitikken og risikovurderingen.	Ingen væsentlige afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har forespurgt til hvorvidt de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus, og vi har stikprøvevis inspiceret dokumentation for anvendelse af antivirus.	Ingen væsentlige afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har forespurgt til om ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem firewall, og vi har inspiceret oversigter over firewalls, og stikprøvevis inspiceret teknisk dokumentation for implementering af firewall.	Ingen væsentlige afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har forespurgt til hvorvidt interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger, og vi har inspiceret dokumentation for, at interne netværk er segmenteret.	Ingen væsentlige afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har forespurgt til procedurer og politikker for at adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov, og vi har inspiceret proceduren for adgangstildeling og informationssikkerhedspolitik.	Ingen væsentlige afvigelser konstateret.

B.7	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter:</p> <ul style="list-style-type: none"> • Usikker datatransmission • Kapacitetsafvigelser • Server response time • Afvigelser i forbindelse med brugeradfærd 	<p>Vi har forespurgt til hvorvidt databehandleren har etableret overvågning af systemer og databaser, og vi har stikprøvevis inspiceret overvågning omfattende:</p> <ul style="list-style-type: none"> • Usikker datatransmission • Kapacitetsafvigelser • Server response time • Afvigelser i forbindelse med brugeradfærd 	<p>Ingen væsentlige afvigelser konstateret.</p>
B.8	<p>Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.</p>	<p>Vi har forespurgt til hvorvidt databehandleren, ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail, anvender effektiv kryptering, og vi har stikprøvevis inspiceret dokumentation for sikker mail og effektiv kryptering af transmission over nettet.</p>	<p>Ingen væsentlige afvigelser konstateret.</p>
B.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> ○ Ændringer i logopsætninger, herunder deaktivering af logning ○ Ændringer i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk • Logoplysninger er beskyttet mod manipulation. 	<p>Vi har forespurgt til hvorvidt databehandleren har etableret logning i systemer, databaser og netværk, og vi har stikprøvevis inspiceret dokumentation for følgende forhold:</p> <ul style="list-style-type: none"> • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> ○ Ændringer i logopsætninger, herunder deaktivering af logning ○ Ændringer i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk • Logoplysninger er beskyttet mod manipulation. 	<p>Ingen væsentlige afvigelser konstateret.</p>

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af test
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 forespurgt til, om personoplysninger bliver anvendt i udvikling, og vi har inspiceret proceduren for udvikling. Vi har stikprøvevis inspiceret udviklingsopgaver for at påse om produktionsdata er pseudonymiseret eller tilsvarende.	Ingen væsentlige 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 forespurgt til procedure for ændringer til systemer, databaser og netværk følger en fastlagt procedure, og vi har inspiceret proceduren for udvikling. Yderligere har vi stikprøvevis inspiceret dokumentation for ændringer, herunder tickets og opdateringerne til software.	Ingen væsentlige afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har forespurgt til procedure for adgangstildeling og afbrydelse af brugeradgange til personoplysninger følger en styret proces, og vi har inspiceret proceduren for adgangstildeling. Yderligere har vi stikprøvevis inspiceret oprettelse/lukning af brugere. Vi har inspiceret oversigt over adgange for udviklere. Vi har inspiceret dokumentation for, at brugere kan logge på fra fjernarbejdspladser. Vi har forespurgt til, om brugerens adgange og rettigheder løbende bliver gennemgået, og vi har inspiceret dokumentation for periodisk kontrol.	Ingen væsentlige 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 forespurgt til hvorvidt adgange til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af tofaktor autentifikation, og vi har stikprøvevis inspiceret at adgang til system og databaser sker gennem tofaktor. Yderligere har vi forespurgt til løbende kontrol af forsøg på adgang fra fjernarbejdspladser, og vi har inspiceret dokumentation for periodisk kontrol.	Ingen væsentlige afvigelser konstateret.
B.15	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 forespurgt til hvorvidt databehandleren har etableret tilstrækkelig fysisk sikkerhed i forhold til adgang til lokaler og datacentre, og vi har inspiceret virksomhedens lokaler, herunder stikprøvevis inspiceret dokumentation for styring af nøgler. Yderligere har vi forespurgt til den fysiske sikkerhed hos housing leverandør, og vi har inspiceret seneste 3402-erklæringen fra leverandøren.	Ingen væsentlige 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 test
C.1	<p>Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.</p>	<p>Vi har forespurgt til hvorvidt databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, og vi har inspiceret it-sikkerhedspolitik og at den er godkendt af ledelsen.</p> <p>Vi har forespurgt til om informationssikkerhedspolitikken bliver periodisk opdateret, og har inspiceret dokumentation for løbende periodisk opdatering.</p> <p>Vi har stikprøvevis inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til databehandlerens medarbejdere, herunder periodisk kontrol af, at medarbejdere er blevet gjort bekendt med den seneste udgave af politikken.</p>	Ingen væsentlige afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har forespurgt til hvorvidt databehandleren har sikret, at databehandleraftaler ikke er i modstrid med informationssikkerhedspolitik, og vi har inspiceret databehandlerens informationssikkerhedspolitik og stikprøvevis inspiceret databehandleraftaler for, at informationssikkerhedspolitikken ikke er i modstrid med aftalerne.	Ingen væsentlige afvigelser konstateret.
C.3	<p>Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang:</p> <ul style="list-style-type: none"> • Referencer fra tidligere ansættelser • Eksamensbeviser, certificeringer og godkendelser. 	Vi har forespurgt til skriftlige procedurer til efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse, og vi har inspiceret proceduren for indhentelse af reference og eksamensbeviser i forbindelse med ansættelse.	Ingen væsentlige afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	<p>Vi har forespurgt til hvorvidt medarbejdere i forbindelse med ansættelse underskriver en fortrolighedsaftale, og vi har stikprøvevis inspiceret fortrolighedsaftale i kontrakt.</p> <p>Vi har forespurgt til, om medarbejdere løbende bliver gjort bekendt med informationssikkerhedspolitikken, herunder i forbindelse med ansættelse, og vi har stikprøvevis inspiceret dokumentation for, at de pågældende medarbejder er blevet introduceret til informationssikkerhedspolitikken, herunder procedurer vedrørende databehandling, samt anden relevant information.</p>	Ingen væsentlige afvigelser konstateret.

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 forespurgt til dokumentation for en styret proces for fratrædelse. Vi har inspiceret procedure for fratrædelse, som beskriver, at fratrådte medarbejders rettigheder deaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Yderligere har vi stikprøvevis inspiceret nøglekvikteringer.	Ingen væsentlige afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har forespurgt til hvorvidt medarbejdere bliver orienteret om fortrolighed i forbindelse med fratrædelse, og vi har inspiceret proceduren for fratrædelse og tjekliste ved ophør af medarbejder.	Ingen væsentlige afvigelser konstateret.
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har forespurgt til hvorvidt der løbende foretages awareness træning af medarbejder, og vi har stikprøvevis inspiceret emner for awareness træning af medarbejdere.	Ingen væsentlige afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en databeskyttelsesrådgiver, og har sikret, at denne har kompetence til at udføre sin rolle.	Vi har forespurgt til hvorvidt databehandleren har vurderet behovet for en DPO, og vi har inspiceret, at der foreligger formaliseret vurdering af behovet for DPO. Vi har forespurgt til løbende opdatering af behovet for DPO, og vi har inspiceret en kontrol for løbende opdatering af vurderingen.	Ingen væsentlige 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 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 forespurgt til, hvordan databehandleren sikrer at opbevaring og sletning af personoplysninger sker i overensstemmelse med aftalen med den dataansvarlige, og vi har stikprøvevis inspiceret, at databehandleren opbevarer og sletter personoplysninger i overensstemmelse med databehandleraftalen.	Ingen væsentlige afvigelser konstateret.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: Sletning eller tilbagelevering sker efter instruks.	Vi har forespurgt til krav til databehandlerens opbevaringsperioder og sletterutiner, og vi har stikprøvevis inspiceret databehandleraftaler, hvor specifikke krav til databehandlerens opbevaringsperioder og sletterutiner er beskrevet.	Ingen væsentlige afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: <ul style="list-style-type: none"> Tilbageleveret til den dataansvarlige og/eller Slettet, hvor det ikke er i modstrid med anden lovgivning. 	Vi har forespurgt til hvorvidt databehandleren enten tilbageleverer eller sletter personoplysninger, og vi har stikprøvevis inspiceret dokumentation for tilbagelevering/sletning i forbindelse med ophør af kontrakten.	Ingen væsentlige 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 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 forespurgt til hvorvidt databehandleren opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige, og vi har stikprøvevis inspiceret dokumentation for opbevaring af personoplysninger. Yderligere har vi forespurgt til dokumentation for opbevaringsperiode og frekvens på backup, og vi har inspiceret dokumentation for dette.	Ingen væsentlige afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokalteter, lande eller landområder.	Vi har forespurgt til at opbevaring af personoplysninger udelukkende sker på lokationer som er godkendt af den dataansvarlige. Vi har stikprøvevis inspiceret databehandleraftaler, hvor lokalitet for behandling fremgår.	Ingen væsentlige 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 test
F.1	<p>Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har forespurgt til skriftlig procedure, som indeholder krav om underdatabehandleraftale og instruks om behandling, og vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Vi har forespurgt til løbende opdatering af proceduren for leverandørstyring, og vi har inspiceret dokumentation for periodisk opdatering.</p>	Ingen væsentlige afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	<p>Vi har forespurgt til hvorvidt databehandleren har generel eller specifik tilladelse fra den dataansvarlige om brug og godkendelse af underdatabehandlere.</p> <p>Yderligere, har vi stikprøvevis inspiceret databehandleraftaler for specifik eller generel godkendelse af underdatabehandlere.</p>	<p>Vi har fået oplyst, at virksomheden ikke anvender underdatabehandlere.</p> <p>Ingen væsentlige afvigelser konstateret i øvrigt.</p>
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 forespurgt til hvorvidt databehandleren underretter den dataansvarlige ved skift af underdatabehandlere, og vi har stikprøvevis inspiceret databehandleraftaler for, at ved udskiftning af underdatabehandleren, skal den dataansvarlige underrettes ved ændring i anvendelse af underdatabehandlerne.	Ingen væsentlige afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har forespurgt til hvorvidt databehandleren pålægger underdatabehandleren de samme krav, som er fastsat af dataansvarlige, der er forudsat i instruks i databehandleraftale.	<p>Vi har fået oplyst, at virksomheden ikke anvender underdatabehandlere.</p> <p>Ingen væsentlige afvigelser konstateret i øvrigt.</p>
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, om virksomheden har foretaget en risikovurdering af den enkelte underdatabehandler, og løbende følger op herpå.	<p>Vi har fået oplyst, at virksomheden ikke anvender underdatabehandlere.</p> <p>Ingen væsentlige afvigelser konstateret i øvrigt.</p>

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 test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til lande uden for EU/EØS eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.	Vi har forespurgt til hvorvidt databehandleren overfører personoplysninger til tredjelande.	Vi har fået oplyst, at databehandleren ikke overfører til tredjelande. Ingen væsentlige afvigelser konstateret i øvrigt.

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 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 forespurgt til procedurer, som beskriver hvordan databehandleren kan bistå den dataansvarlige med håndtering af registreres rettigheder, og vi har stikprøvevis inspiceret databehandleraftaler, hvori det er beskrevet, hvordan databehandler kan bistå den dataansvarlige med persondataanmodninger.	Ingen væsentlige 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 hvorvidt databehandleren er i stand til at efterkomme persondataanmodninger fra den dataansvarlige, og vi har stikprøvevis inspiceret dokumentation for, at databehandlere kan efterleve følgende: <ul style="list-style-type: none"> • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Indsigt i personoplysninger 	Ingen væsentlige afvigelser konstateret.

Kontrolmål I – Sikkerhedsbrud

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 test
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har forespurgt til, om databehandleren har en procedure for håndtering af sikkerhedsbrud, og en log over sikkerhedsbrud, og vi har inspiceret proceduren, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden, samt loggen over sikkerhedsbrud.</p> <p>Vi har stikprøvevis inspiceret indrapportering af sikkerhedsbrud.</p> <p>Vi har forespurgt til hvorvidt databehandleren løbende gennemgår hændelser, og vi har inspiceret dokumentation for periodisk gennemgang af hændelser.</p>	Ingen væsentlige afvigelser konstateret.
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> - Awareness hos medarbejdere - Overvågning af netværkstrafik - Opfølgning på logning af tilgang til personoplysninger 	<p>Vi har forespurgt til hvorvidt databehandleren har etableret awarenessstræning, overvågning af netværk og opfølgning af adgang til personoplysninger, og vi har stikprøvevis inspiceret dokumentation for, at databehandleren har etableret træning af medarbejdere, overvågning af netværkstrafik og opfølgning på logning af tilgang til personoplysninger.</p>	Ingen væsentlige afvigelser konstateret.
I.3	<p>Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.</p>	<p>Vi har forespurgt til hvorvidt databehandleren underretter den dataansvarlige ved eventuelle brud, og vi har stikprøvevis inspiceret eksempel på underretning af den dataansvarlige i forbindelse med persondatasikkerhedshændelser.</p>	Ingen væsentlige afvigelser konstateret.
I.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>Vi har forespurgt til hvorvidt databehandleren kan bistå den dataansvarlige ved anmeldelse til Datatilsynet, og vi har stikprøvevis inspiceret dokumentation for følgende:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	Ingen væsentlige 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 test
J.1	Der foreligger skriftlige procedurer for indhentelse af skriftligt samtykke til behandling af personoplysninger.	Vi har forespurgt til, om virksomheden indhenter eller opbevarer samtykke på vegne af de dataansvarlige.	Virksomheden oplyser, at de ikke skal indhente samtykke på vegne af den dataansvarlige. Ingen væsentlige afvigelser konstateret i øvrigt.
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 tekniske foranstaltninger, der sikrer, at det kan dokumenteres, hvilke oplysninger der er givet i forbindelse med samtykke.	Virksomheden oplyser, at de ikke indhenter eller opbevarer samtykke på vegne af den dataansvarlige. Ingen væsentlige afvigelser konstateret i øvrigt.
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 hvorvidt databehandleren kan bistå den dataansvarlige med oplysninger om behandlingen, og vi har stikprøvevis inspiceret databehandleraftaler, hvori det er beskrevet, hvordan databehandleren kan bistå den dataansvarlige.	Ingen væsentlige 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 har kontakt til de registrerede.	Vi har fået oplyst, at databehandleren ikke har kontakt til de registrerede. Ingen væsentlige afvigelser konstateret i øvrigt.

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 test
K.1	<p>Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige, som indeholder:</p> <ul style="list-style-type: none"> • Navn på og kontaktoplysninger for databehandleren for hver dataansvarlig og – hvis det er relevant – den dataansvarliges databeskyttelsesrådgiver • De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige • Overførsler af personoplysninger til et tredjeland eller en international organisation, og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier • En generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger 	Vi har forespurgt til hvorvidt databehandleren har udarbejdet en fortegnelse over behandlingsaktiviteter, og vi har inspiceret fortegnelsen.	Ingen væsentlige afvigelser konstateret.
K.2	Der foretages halvårligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	Vi har forespurgt til om databehandleren løbende vurderer fortegnelsen, og vi har inspiceret dokumentation for periodisk opdatering af fortegnelsen.	Ingen væsentlige afvigelser konstateret.
K.3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Vi har forespurgt til hvorvidt databehandlerens ledelse har godkendt fortegnelsen, og vi har inspiceret ledelsesgodkendelse af fortegnelsen.	Ingen væsentlige afvigelser konstateret.