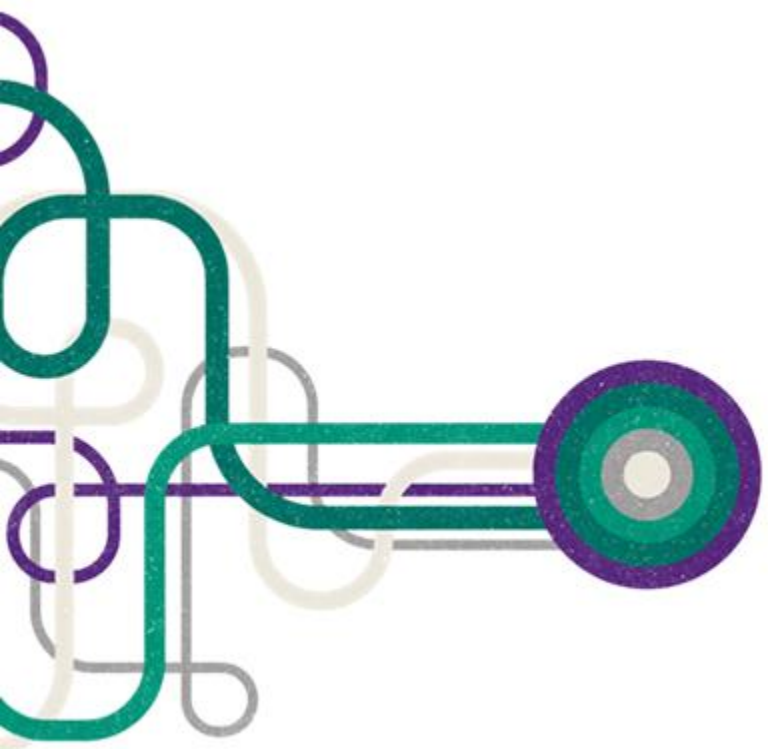
Grant Thornton

An instinct for growth™



Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med perioden 1. marts 2019 til 29. februar 2020

ISAE 3402-II

# IDQ A/S

CVR-nr.: 34 04 62 20

Maj 2020

# Indholdsfortegnelse



**Symbol**

- ● Vores gennemgang har ikke ført til bemærkninger.
- ● Der er konstateret enkelte svagheder.
- ● Der er fundet væsentlige svagheder eller mangler.

# 1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt IDQ A/S' ydelser relateret til behandling og berigelse af data i perioden, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber.

IDQ A/S bekræfter, at:

a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af IDQ A/S' ydelser relateret til behandling og berigelse af data i perioden til kunder i hele perioden fra 1. marts 2019 til 29. februar 2020. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

i. redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:
   - de typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant
   - de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
   - de tilhørende regnskabsregistreringer, underliggende information og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan informationen er overført til de rapporter, der er udarbejdet til kunder
   - hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
   - processen, der blev anvendt til at udarbejde rapporter til kunder
   - relevante kontrolmål og kontroller udformet til at nå disse mål
   - kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomhederne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
   - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner

ii. Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. marts 2019 til 29. februar 2020

iii. ikke udelader eller forvansker information, der er relevant for omfanget af det beskrevne system, under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i hele perioden fra 1. marts 2019 til 29. februar 2020. Kriterierne for denne udtalelse var, at:

i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificerede, og

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

iii. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. marts 2019 til 29. februar 2020.

København, 1. maj 2020
IDQ A/S

Henrik Saustrup

Direktør

# 2. Systembeskrivelse

### 1. Kontrolmiljø

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 håndtering, har en udførende ansvarshavende, og i visse tilfælde også en ansvarshavende godkender. Med mindre andet er anført er den udførende ansvarshavende IDQs CTO og den ansvarshavende godkender IDQs CEO.

Vores kontroller er rettet mod dels konkrete arbejdshandlinger og dels processer for en række arbejdshandlinger, som igen kan have yderligere konkrete kontroller tilknyttet. Tidsangivelse for en given kontrol opgives altid inden for en given periode. Kontrollerne tilsigtes at blive udført inden for denne periode, men driftsmæssige omstændigheder og/eller ventetid i forbindelse med leverandører eller kunder kan betyde at den praktiske kontrol udføres senere. Oversigten over kontrollerne findes i IDQs årshjul.

### 2. Vores kerneydelser

IDQ A/S er en data- og softwarevirksomhed, som udvikler og markedsfører software til forøgelse af datakvalitet. Omdrejningspunktet er de tre produkter iDQ Search, iDQ Alert og iDQ Services.

iDQ Searchs formål er at tilbyde brugerne samlet adgang til søgning, opslag og overførsel af relevante markedsdata gennem et brugervenligt userinterface.

iDQ Search giver adgang til egne kundedata samt gratis datakilder og betalingstjenester. Af primære kilder kan nævnes CPR-registret, CVR-registret, OIS/BBR, Statstidende, Tinglysningen, teledata samt kreditoplysninger fra RKI og Bisnode. iDQ Search anvendes især i forbindelse med kundeoprettelse af såvel private forbrugere som virksomheder, men anvendes desuden som søgeværktøj i relation til returpost, inkassosager, kreditforespørgsler osv.

iDQ Alerts formål er at tilbyde brugerne løbende opdatering af kunde-stamdata – fx flytninger, dødsfald, navneskift og virksomhedslukninger. Desuden er formålet at give notifikationer omkring vigtige begivenheder i kundedatabasen – begivenheder som kan betyde ændringer i risikoscenariet, fx betalingsstandsninger, udlæg, tvangsauktioner osv.

iDQ Services giver adgang til en lang række webservices (også kaldet api'er), som benytter sig af de samme kilder, som anvendes i forbindelse med iDQ Search. Disse services anvendes af kunderne til at integrere data direkte i kundens egne applikationer.

### 3. Informationssikkerhedsrelaterede kontroller

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, jf. årshjulet. Når vi har ændret ting i it-sikkerhedspolitikken, og minimum efter den årlige gennemgang, fremlægges ændringerne internt ved førstkommende månedsmøde for personalet. Ligeledes bliver eksterne leverandører inddraget og orienteret, hvis det har relevans.

Det er virksomhedens CTO, som er ansvarlig for virksomhedens informationssikkerhed.

# 2. Systembeskrivelse

### 4. Risikostyring

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

Risikovurdering foretages periodisk, minimum én gang årligt, samt når der foretages ændringer eller implementeres nye systemer, som vi vurderer at have relevans i forhold til vores generelle risikovurdering.

### 5. HR- og medarbejderrelaterede kontroller

Forud for ansættelse af medarbejdere følges en ansættelsesprocedure udarbejdet af selskabets HR-funktion. Det er den ansættende direktør, som er ansvarlig for de HR-relaterede kontroller.

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

Det er virksomhedens direktør, som er ansvarlig for at alle HR-processer og procedurer overholdes, og virksomhedens størrelse taget i betragtning varetages disse opgaver typisk af ham selv.

Den tekniske oprettelse af medarbejdere, såvel som konsulenter, foretages i henhold til relevante procedurer. Vi har desuden en proces for 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 som sidemandsoplæringer, ved kontormøder o. lign.

#### 5.1 Afhængighed af nøglemedarbejdere

Via vores dokumentation og beskrivelser sikrer vi os mod personafhængighed. Vi arbejder således med dobbeltroller på de vigtigste af vores funktioner. Der afholdes månedlige one2one samtaler med nøglemedarbejdere i it-udvikling. Møderne har til formål at sikre en høj trivsel og følge op på medarbejderens ansvarsområder og på den måde minimere risikoen for og ved jobskifte.

### 6. Kunde-relaterede kontroller

Implementering af, og leverancer til, nye kunder foretages i henhold til fastlagte kontraktuelle procedurer og andre relevante procedurer. Repræsentant fra vores Salg og Ledelse skal godkende kundeopsætningen, hvorfor der sikres overensstemmelse med kontrakt, teknik og forretningskrav. Hver kundekontrakt indeholder desuden specifikation af hvem hos kunden, der har rettigheder til at fremsende og/eller godkende it-ændringsønsker på vegne af den pågældende virksomhed til IDQ, så der aldrig opstår tvivl om hvem der er ansvarlig for en udført handling.

### 7 Driftsrelaterede kontroller

#### 7.1 Fysisk sikkerhed

Al vores udstyr er placeret hos vores datacenter leverandør. Vi har ikke fysisk adgang til datacenteret, men inspicerer dette årligt. Vores datacenter leverandør har revisorerklæring af type ISAE 3402-II, som afgives årligt, og vi indhenter årligt revisorerklæringen.

Vores fysiske kontor er placeret i Lygten 39 i København. Vi har en proces for sikring af lokationen.

#### 7.2 Databærende medier

Alle mobiltelefoner er sikret med en MDM-løsning indeholdende en række sikkerhedspolitikker. Følsomme data må alene opbevares på serverrumsmedier eller i krypteret form på egen fildelingsløsning.

# 2. Systembeskrivelse

### 7.3 Bortskaffelse af medier

Medier destrueres som en del af vores indkøbsaftale med leverandøren. Ved tyveri af mobiltelefon, foretages en fuld sletning af telefonen. Det vil derefter ikke være muligt at tilgå vores netværk via den pågældende telefon.

### 7.4 Styring af netværk og drift

Vores dokumentation og arbejdsprocesser medvirker til at sikre en stabil, korrekt og driftssikker ydelse, hvor person-afhængighed og 'sjuskefejl' minimeres.

Vores tekniske set-up fokuserer på samme værdier, og værn mod uvedkommendes adgang til vores data er af højeste prioritet. Vi har desuden antivirus-systemer, e-mail skanning, og systemer til overvågning og sikring af netværk og internetbrug. Al godkendt netværkstrafik (indgående) kommer igennem vores firewall. Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv.

Adgang til netværksydelser via mobile enheder sikres via en MDM-løsning.

Adgang fra hjemmearbejdspladser sker via en krypteret VPN-forbindelse.

Standardændringer har, i videst muligt omfang, en dedikeret SOP. Alle væsentlige ændringer drøftes, prioriteres og godkendes af ledelsen.

Ekstern datakommunikation foregår, afhængig af type, via e-mails.

### 7.5 Teknisk ændringsstyring - patching

Operativsystem patchning foretages månedligt i et fastlagt servicevindue. Servicevinduet fremgår af virksomhedens generelle forretningsbetingelser, og skal ikke varsles separat. For kritiske systemopdateringer, eksempelvis Windows security updates, varsles kunderne i så god tid som muligt.

### 7.6 Overvågning og logning

Vi foretager daglig overvågning af vores systemer via automatiserede systemer til måling af grænseværdier. Alarmering, såfremt en kritisk hændelse konstateres, tilgår vores tekniske medarbejdere. Hændelser relateret til vores fælles platform, infrastruktur og serverrumsydelser håndteres af vores it-leverandør, som uden for kontortid har driftsvagt. Hændelser for login og log-out på vores platforme logføres, og vi benytter alene personhenførbare brugerkonti, hvorfor det er muligt at identificere, hvilke personer der har været logget på.

### 7.7 Adgangsstyring

Vores kunders brugere oprettes, ændres og nedtages alene på baggrund af krav fra vores kunder. Interne brugere oprettes alene på baggrund af skriftligt ønske fra ledelsen. Alle brugere er personhenførbare. For servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentligt log-on deaktiveret.

Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode. Interne brugere og deres adgangsniveau gennemgås periodisk af ledelsen.

### 7.8 Backup og sikkerhedskopiering

Vores kunders data er lige så vigtige som vores egne data, og vi har en procedure for at sikre samme. Vi tager dagligt backup, og vi har, ved vores leverandør, en procedure for kontrol af backup, herunder hvordan der skal ageres ved fejl.

### 7.9 Kapacitetsstyring

Tilgængelighed er en af vores kerneværdier, og vi sætter en ære i altid at levere den forventede kvalitet i ydelser til vores kunder. Et af de væsentlige parametre IDQ måles på af kunderne er svartider på søgninger gennem IDQ-systemet. Derfor overvåger vi konstant vores kapacitet, både disk, cpu og trafik, og vi kan løbende, og uden gene for kunderne, udvide vores kapacitet.

# 2. Systembeskrivelse

## 8. Håndtering af sikkerhedshændelser

Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af hændelser. Vi har en række tiltag for at forhindre at sikkerhedshændelser opstår, og vi har driftsvagtordning med vores infrastrukturleverandør således, at der reageres straks en hændelse måtte opstå. Vi holder os tillige fagligt opdaterede vha. producenternes hjemmesider, debatfora mv.

### 8.1 Opfølgning på sikkerhedshændelser

Alle sikkerhedsbrud dokumenteres til internt brug, og hændelsen gennemgås med alle relevante medarbejdere ved førstkommende lejlighed. Afhængig af hændelsens karakter udarbejdes nye processer og procedurer, så vi undgår at hændelsen indtræffer igen.

Sikkerhedsrelaterede emner, generelle såvel som aktuelle emner, gennemgås desuden ved interne møder.

Ved kriminelle forhold sker en politimæssig efterforskning, hvor vores logføring og øvrige overvågning kan benyttes til opklaring og evaluering af sikkerhedshændelsen.

## 9. Beredskabsstyring

Skulle en nødsituation opstå har IDQ udarbejdet en beredskabsplan. Beredskabsplanen er udarbejdet i henhold til vores it-sikkerhedspolitik og risikoanalyse, og den vedligeholdes minimum årligt. Planen testes, og plan og procedurer er forankret i vores driftsdokumentation- og procedurer. Vores beredskabsplanlægning tager højde for at vi kan levere vores ydelser rettidigt – næsten uanset hvad der sker.

## 10. Leverandørforhold

### 10.1 Sikkerhed i leverandøraftaler og kontrol af serviceydelser fra tredjepart

Alle vores leverandør og partneraftaler skal indeholde regulering af fortrolighed.

Der indhentes tillige revisorerklæring fra vores kritiske leverandører.

## 11. Komplementerende kontroller

Med mindre andet er aftalt, er vores kunder selv ansvarlige for at etablere forbindelse til vores servere.

Desuden er vores kunder selv ansvarlige for, med mindre 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, og vi) Anmodning om adgang til kundens servermiljø for kundens tredjepartsleverandører, vii) Kundens anmeldelse til Datatilsynet, for hvem dette måtte være relevant.

## 12. Overensstemmelse med lovbestemte og kontraktlige krav

Vi er underlagt Persondataloven i forhold til vores ydelser. Gennem softwareløsninger og databehandlingsservices optræder IDQ som databehandler underlagt GDPR (Persondataforordningen). Vores kunder kan dog være underlagt særlig lovgivning, og hvor det måtte være tilfældet, er vores understøttelse heraf aftalt særskilt.

Vi lader os årlige revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelsen af kontrollerne nævnt i denne beskrivelse. Vi følger rammerne inden for ISO 27002, hvilket føromtalte revisor attesterer i en ISAE3402-erklæring.

# 3. Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet

**Til: ledelsen hos IDQ A/S, IDQ A/S' kunder og deres revisorer.**

## Omfang

Vi har fået til opgave at afgive erklæring om IDQ A/S' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af IDQ A/S' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens drift af ydelser relateret til behandling og berigelse af data i perioden 1. marts 2019 til 29. februar 2020 samt udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

## IDQ A/S' ansvar

IDQ A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. IDQ A/S er herudover ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmål, og for udformningen, implementeringen og effektiviteten af fungerende kontroller for at nå de anførte kontrolmål.

## Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Firmaet anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

## Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om IDQ A/S' beskrivelse (afsnit 2) og om udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede og fungerer effektivt.

Opgaven med afgivelse af en erklæring med sikkerhed om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleveran-dørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformede eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

# 3. Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet

### Begrænsninger i kontroller hos en serviceleverandør

IDQ A/S' beskrivelse i afsnit 2 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

### Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i IDQ A/S' beskrivelse i afsnit 2, og det er på den baggrund vores vurdering,

a) at beskrivelsen af kontroller, således som de var udformede og implementerede i hele perioden 1. marts 2019 til 29. februar 2020., i alle væsentlige henseender er retvisende.

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformede i hele perioden fra 1. marts 2019 til 29. februar 2020.

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. marts 2019 til 29. februar 2020.

### Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i det efterfølgende hovedafsnit (afsnit 4).

### Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt IDQ A/S' drift af ydelser relateret til behandling og berigelse af data, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller. Denne information tjener til opnåelse af en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

København, 1. maj 2020

**Grant Thornton**

Statsautoriserede revisionspartnerselskab

CVR-nr: 34 20 99 36

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Anders Grønning-Kjærgaard
Director, Head of IT Audit & Advisory

# 4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som IDQ A/S har implementeret. 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 kontrolmål har været opnået i perioden 1. marts 2019 til 29. februar 2020.

Vi har således ikke nødvendigvis testet alle de kontroller, som IDQ A/S har nævnt i sin beskrivelse i afsnit 2.

Kontroller, udført hos IDQ A/S kunder, er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Beskrivelse og resultat af vores tests ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Vi har udført vores tests af kontroller hos IDQ A/S via følgende handlinger:

| Metode | Overordnet beskrivelse |
|---|---|
| Forespørgsel | Interview af udvalgte medarbejdere angående kontroller |
| Observation | Observation af hvordan kontroller udførelse (Design) |
| Inspektion | Gennemgang af politikker, procedurer og dokumentation af kontrollernes udførelse (Implementering) |
| Test af kontrol | Gennemførelse af kontrolhandlinger, som vi selv har udført eller som har observeret gennemført af ansvarlige medarbejdere (Udførelse) |

# 4.4 Risikovurdering og -håndtering

**Kontrolmål:**

Formål: At sikre, at virksomheden periodisk foretager en analyse og vurdering af it-risikobilledet.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 4.1 | 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.<br><br>Risikovurdering foretages periodisk, minimum én gang årligt, samt når der foretages ændringer eller implementeres nye systemer, som vi vurderer at have relevans til i forhold til en revurdering af vores generelle risikovurdering. | Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse.<br><br>Vi har forespurgt til periodisk evaluering af risikoanalysen indenfor perioden, og vi har inspiceret dokumentation for, at denne er gennemgået og godkendt af ledelsen i revisionsperioden. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.5 Informationssikkerhedspolitikker

**Kontrolmål:**

Formål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 5.1 | 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.<br><br>Virksomhedens it-sikkerhedspolitik opdateres såfremt der foretages ændringer eller implementeres nye forretningsområder, og politikken gennemgås i sin helhed minimum én gang årligt, jf. årshjulet. | Vi har forespurgt til udarbejdelsen af en informationssikkerhedspolitik, og vi har inspiceret dokumentet.<br><br>Vi har forespurgt til ledelsesgodkendelse af informationssikkerhedspolitikken, og vi har inspiceret dokumentation for ledelsesgodkendelse.<br><br>Vi har forespurgt til periodisk kontrol for gennemgang af informationssikkerhedspolitikken, og vi har inspiceret kontrol for gennemgang. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.6 Organisering af informationssikkerhed

**Kontrolmål:**

Formål: At sikre, at der etableres et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 6.1 | Det er virksomhedens CTO, som er ansvarlig for virksomhedens informationssikkerhed.<br><br>Via vores dokumentation og beskrivelser sikrer vi os mod personafhængighed, ligesom vi arbejder med dobbeltroller på alle funktioner. Der opereres på tværs af Direct Gruppen med "Organisational Review", som har til formål at minimere risici ved at beskrive nøglemedarbejdere og lægge en detaljeret plan for dels hvordan medarbejderen kan fastholdes og udvikles, dels hvordan de kan erstattes i tilfælde af jobskifte.<br><br>Vi holder os tillige fagligt opdaterede vha. producenternes hjemmesider, debatfora mv. | Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen og vedligeholdelsen af ansvarsbeskrivelser.<br><br>Vi har forespurgt til adskillelse af adgang i forhold til funktion, og vi har inspiceret dokumentation for differentieret adgang.<br><br>Vi har forespurgt til retningslinjer for kontakt med myndigheder, og vi har inspiceret retningslinjerne.<br><br>Vi har forespurgt til kontakt med interessegrupper, og vi har inspiceret dokumentation for kontakt.<br><br>Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter. Vi har desuden stikprøvevis inspiceret projektforløb og verificeret, at der tages hensyn til informationssikkerhed. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.6 Organisering af informationssikkerhed

**Kontrolmål:**

Formål: At sikre fjernarbejdspladser og brugen af mobilt udstyr

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 6.2 | Vi har i virksomheden krav om, at alle mobile enheder, skal sikres med pinkode og automatisk låsning efter inaktivitet. Vi har mulighed for, at foretage remote wipe på alle enheder, der tilsluttes virksomhedens netværk. For mobile enheder som mobiltelefoner og tablets, tilbyder vi adgang til mail og kalenderfunktioner.<br><br>Vi tillader ikke lagring af virksomhedsdata på privatejede enheder.<br><br>Alle mobiltelefoner er sikret med en MDM-løsning indeholdende en række sikkerhedspolitikker.<br><br>Ved tyveri af mobiltelefon, foretages en fuld sletning af telefonen. Det vil derefter ikke være muligt at tilgå vores netværk via den pågældende telefon.<br><br>Adgang fra hjemmearbejdspladser sker via en krypteret VPN-forbindelse. | Vi har forespurgt til styring af mobile enheder, og vi har inspiceret løsningen.<br><br>Vi har forespurgt til sikring af fjernarbejdspladser, og vi har inspiceret løsningen. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende kontroller for styring af mobile enheder. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.7 Medarbejdersikkerhed

**Kontrolmål:**

Formål: At sikre, at medarbejder og kontrahenter forstår deres ansvar og er egnede til de roller, de er betragtning til.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 7.1 | Forud for ansættelse af medarbejdere følges en ansættelsesprocedure udarbejdet af moderselskabets (Direct Gruppen) HR-funktion.<br><br>Det er den ansættende direktør, som er ansvarlig for de HR-relaterede kontroller.<br><br>For konsulenter, som skal have adgang til (dele af) vores netværk, udarbejdes altid opgavespecifik kontrakt, dedikeret fortrolighedserklæring, og anden relevant dokumentation indhentes. | Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren.<br><br>Vi har endvidere stikprøvevis inspiceret dokumentation for, at proceduren er fulgt.<br><br>Vi har forespurgt til formaliseringen af ansættelsesforhold, og vi har stikprøvevis inspiceret indholdet af kontrakter. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.7 Medarbejdersikkerhed

**Kontrolmål:**

Formål: At sikre, at medarbejdere og kontrahenter er bevidste og lever op til deres informationssikkerhedsansvar.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 7.2 | Det er virksomhedens direktør, som er ansvarlig for at alle HR-processer og procedurer overholdes, og virksomhedens størrelse taget i betragtning varetages disse opgaver typisk af ham selv.<br><br>Den tekniske oprettelse af medarbejdere- såvel som konsulenter, foretages i henhold til relevante procedurer. Vi har desuden en proces for 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 som side-mandsoplæringer, ved kontormøder o. lign.<br><br>Når vi har ændret ting i it-sikkerhedspolitikken, og minimum efter den årlige gennemgang, fremlægges ændringerne internt ved førstkommende månedsmøde for personalet. Ligeledes bliver eksterne leverandører inddraget og orienteret hvis det har relevans. | Vi har forespurgt til ledelsens ansvar for videreformidling af politikker og procedurer, og vi har inspiceret dokumentation for tildeling af ansvar.<br><br>Vi har forespurgt til videreuddannelse af personale, og vi har stikprøvevis inspiceret dokumentation for videreuddannelse.<br><br>Vi har forespurgt til retningslinjer for sanktionering, og vi har inspiceret retningslinjerne. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.7 Medarbejdersikkerhed

**Kontrolmål:**

Formål: At beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 7.3 | Det er virksomhedens direktør, som er ansvarlig for at alle HR-processer og procedurer overholdes, og virksomhedens størrelse taget i betragtning varetages disse opgaver typisk af ham selv.<br><br>Via vores dokumentation og beskrivelser sikrer vi os mod personafhængighed. Vi arbejder således med dobbeltroller på de vigtigste af vores funktioner. Der afholdes månedlige one2one samtaler med nøglemedarbejdere i it-udvikling. Møderne har til formål at sikre en høj trivsel og følge op på medarbejderens ansvarsområder og på den måde minimere risikoen for og ved jobskifte. | Vi har forespurgt til medarbejderes forpligtelse til opretholdelse af informationssikkerhed i forbindelse med ophør af ansættelse, og vi har inspiceret dokumentation for medarbejdernes forpligtelser. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.8 Styring af aktiver

**Kontrolmål:**

Formål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 8.1 | Alle aktiver ejes helt og fuldstændigt af IDQ A/S. Undtaget herfra er server- og netværksudstyr, som for visse deles vedkommende er leaset af vores infrastrukturleverandør, Sentia.<br><br>Registrering af virksomhedens aktiver varetages af Sentia og kontrolleres af IDQ's IT-ansvarlige. Sentia registrerer al ejet hardware og egne softwarelicenser. Småanskaffelser som mus, tastaturer, og docking stationer registreres ikke. Servere og infrastrukturrelateret hardware konfigurationer og tekniske forbindelser er dokumenteret i netværkstegninger, systemdokumentation mv., hvor langt størstedelen er hjemhørende hos Sentia. Dokumentejerskab forvaltes af Sentia, med henblik på at kunne genskabe en eller flere af virksomhedens services.<br><br>Hver systemejer er ansvarlig for de systemer der understøtter deres applikation, samt de processer der har til formål at sikre stabil drift af samme. Organisationens størrelse og applikationernes indbyrdes afhængigheder gør at det i daglig praksis er et uformelt samarbejde, men det er hver systemejers ansvar at holde systemdokumentationen opdateret o. lign.<br><br>*(forsættes)* | Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver.<br><br>Vi har forespurgt til oversigt over ejerskab af aktiver, og vi har inspiceret oversigten.<br><br>Vi har forespurgt til retningslinjer for brugen af aktiver, og vi har inspiceret retningslinjerne.<br><br>Vi har forespurgt til procedure til sikring af tilbagelevering af udleverede aktiver, og vi har inspiceret proceduren. Endvidere har vi stikprøvevis sikret, at proceduren for tilbagelevering af aktiver er fulgt.<br><br>Vi har forespurgt til revisorerklæring fra underleverandører med henblik på at konstatere, hvorvidt der er blevet observeret afgivelser fsva. ansvaret for og håndteringen af aktiver. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.8 Styring af aktiver

**Kontrolmål:**

Formål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 8.1 | *(fortsat)*<br><br>Virksomheden har opskrevet faste regler for brugen af aktiver, samt behandling af informationer. Disse regler er integreret i ansættelseskontrakterne, samt i personalehåndbogen. Alle medarbejdere er forpligtet til at læse personalehåndbogen, når de bliver ansat, og der er yderligere opfølgning ved ændringer der er relevant for de enkelte medarbejdere.<br><br>Virksomheden har faste procedurer til inddrivelse af IT-aktiver ved ophør af medarbejdere. Medmindre andet aftales, inddrives alle IT-aktiver, herunder også bærbare medier samt adgange, af autoriseret personale på sidste arbejdsdag. Alle udleverede IT-aktiver registreres i et centralt register. Dermed kan vi tilse, at alle aktiver inddrives igen, efter endt ansættelse. | | |

# 4.8 Styring af aktiver

**Kontrolmål:**

Formål: At sikre passende beskyttelse af informationer, der står i forhold til informationens betydning for organisationen.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 8.2 | Kundedata er adskilt i separate dataområder, således at data fra specifikke kunder kan identificeres og slettes eller porteres på anfordring.<br><br>Det bemærkes, at personfølsomme data, eksempelvis cpr-informationer i kombination med anden data, ydes særlig beskyttelse i virksomheden, og må således ikke forefindes på private enheder eller sendes ukrypteret. Alle medarbejdere, der har en arbejdsmæssig grund til at databehandle personfølsomme data bliver autoriseret til dette, og opnår derved de nødvendige adgangstilladelser.<br><br>Vi har interne regler for opbevaring af særlige datatyper, eksempelvis kundedata, hr/personaledata, salgs-data osv. Personalet gøres bekendt med dette via den medarbejdervendte IT-sikkerhedspolitik og personlig introduktion i forbindelse med jobstart. | Vi har forespurgt til politik for klassificering af data, og vi har inspiceret politikken.<br><br>Vi har forespurgt til mærkning af data, og vi har inspiceret dokumentation for mærkning af data.<br><br>Vi har forespurgt til retningslinjer for håndtering af aktiver, og vi har inspiceret retningslinjerne. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.8 Styring af aktiver

**Kontrolmål:**

Formål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 8.3 | Medier destrueres som en del af vores indkøbsaftale med leverandøren. Ved tyveri af mobiltelefon, foretages en fuld sletning af telefonen. Det vil derefter ikke være muligt at tilgå vores netværk via den pågældende telefon.<br><br>Alle mobiltelefoner er sikret med en MDM-løsning indeholdende en række sikkerhedspolitikker. Følsomme data må alene opbevares på serverrumsmedier eller i krypteret form på egen fildelingsløsning. | Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for løsningen.<br><br>Vi har forespurgt til retningslinjer for bortskaffelse af medier, og vi har inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende kontroller for sikker bortskaffelse.<br><br>Vi har forespurgt til transport af bærbare medier, og vi har inspiceret politikken.<br><br>Vi har inspiceret revisorerklæring fra underleverandører med henblik på at konstatere, hvorvidt der er blevet observeret afgivelser fsva. håndtering af medier | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.9 Adgangskontroller

**Kontrolmål:**

Formål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 9.1 | Virksomheden tillader alene personhenførbare brugere. Alle brugere med adgang til virksomhedens netværk, er personhenførbare. For systembrugere er der særlige regler, hvor 'sys admin' alene benyttes hvor det ikke kan undgås.<br><br>Alle adgange tildeles efter funktionsbehov i sammenhæng med den enkeltes jobrolle. Vi gennemfører intern kontrol af tildelte adgange to gange årligt jævnfør årshjulet, ligesom opdatering af adgange er faste kontroller i vores HR-processer for hhv. nyansættelse og fratrædelse (eller ændring) i ansættelse.<br><br>Funktionsopdelingen reflekteres i vores AD-politik og et samlet, generisk overblik over vores funktionsbaserede roller er dokumenteret. | Vi har forespurgt til politik for styring af adgange til systemer og bygninger, og vi har inspiceret politikken.<br><br>Vi har forespurgt til håndtering af adgang til netværk og netværksservices, og vi har inspiceret løsningen. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.9 Adgangskontroller

**Kontrolmål:**

Formål: At sikre adgang for autoriserede brugere og forhindre uautoriserede brugere adgang til systemer og tjenester

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 9.2 | Vores kunders brugere oprettes, ændres og nedtages alene på baggrund af krav fra vores kunder. Interne brugere oprettes alene på baggrund af skriftligt ønske fra ledelsen. Alle brugere er personhenførbare. For servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon deaktiveret.<br><br>Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode. Interne brugere og deres adgangsniveau gennemgås periodisk af ledelsen.<br><br>Vi har segmenterede netværk og vi benytter GPO'er, der begrænser adgange jf. funktionskrav. | Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere, og vi har inspiceret procedurerne.<br><br>Vi har inspiceret dokumentation for proces for oprettelse og nedlæggelse af brugere. Endvidere har vi inspiceret Sentia's revisorerklæring med henblik på at identificere betryggende tildeling af brugeradgang.<br><br>Vi har forespurgt til overvågning af anvendelsen af privilegerede adgangsrettigheder, og vi har inspiceret Sentias revisorerklæring med henblik på at identificere betryggende styring af privilegerede adgangsrettigheder.<br><br>Vi har forespurgt til opbevaring af fortrolige adgangskoder, og vi har inspiceret dokumentation for betryggende opbevaring.<br><br>Vi har forespurgt til proces for periodisk gennemgang af brugere, og påset at det er en del af virksomhedens årshjul. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.9 Adgangskontroller

**Kontrolmål:**

Formål: At gøre brugere ansvarlige for at sikre deres autentifikationsinformation

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 9.3 | Forventninger til brugernes håndtering af autentifikationsinformation er beskrevet i it-sikkerhedspolitikken. | Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

**Kontrolmål:**

Formål: At forhindre uautoriserede adgang til systemer og applikationer.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 9.4 | Alle brugere, kundebrugere som interne brugere, har restriktioner omkring adgangskode.<br><br>Interne brugere og deres adgangsniveau gennemgås periodisk af ledelsen.<br><br>Adgang fra hjemmearbejdspladser sker via en krypteret VPN-forbindelse.<br><br>For servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon deaktiveret.<br><br>Adgang til kildekoder styres via ændringsstyring. | Vi har forespurgt til begrænsning af adgang til data, og vi har inspiceret dokumentation for begrænsning.<br><br>Vi har forespurgt til procedure for sikker logon, og vi har inspiceret løsningen.<br><br>Vi har forespurgt til system til styring af adgangskoder, og vi har inspiceret løsningen og udvalgte konfigurationer.<br><br>Vi har inspiceret Sentia's revisorerklæring med henblik på håndtering af servicebrugere.<br><br>Vi har inspiceret roller og adgange til kildekoder. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.10 Kryptering

**Kontrolmål:**

Formål: At sikre korrekt og effektivt brug af kryptografi for at beskytte informations fortrolighed, autenticitet og/eller integritet .

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 10.1 | Adgang fra hjemmearbejdspladser sker via en krypteret VPN-forbindelse.<br><br>Udveksling af kundedata udvekslet over internettet sendes over SSH-protokol. Certifikatadministration varetages af vores infrastrukturleverandør. | Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende anvendelse af kryptografi. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.11 Fysisk sikring og miljøsikring

**Kontrolmål:**

Formål: At forhindre uautoriserede fysisk adgang til samt beskadigelse og forstyrrelse af organisationens informations- og informationsbehandlingsfaciliteter.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 11.1 | Adgang til netværk og netværksservices som switche, routere og firewalls varetages af vores IT-leverandør, Sentia. Sentia har revisorerklæring af typen ISAE 3402-II, som er afgivet uden forbehold eller væsentlige forhold med hensyn til tildeling af adgange. Fysisk er udstyret placeret i vores lokale teknikrum i Enigheden på Lygten 39, København N. Bygningen af konstant aflåst, og hver medarbejder har en nøglebrik. Desuden er selve teknik-rummet aflåst yderligere med en cylinderlås på selve døren. Nøgle hertil har virksomhedens ejerkreds, og det personale, som har funktionsbehov knyttet hertil. Sentia, virksomhedens totalleverandør, kan melde enheder såvel som brugere ind i domænet. | Vi har forespurgt til revisorerklæring fra Sentia, og vi har inspiceret erklæringen for betryggende fysisk sikring.<br><br>Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandør, og vi har stikprøvevis inspiceret dokumentation for tildeling af adgang til driftsfaciliteter.<br><br>Vi har inspiceret de fysiske forhold hos virksomhedens kontorer med henblik på at kontrollere den fysiske sikring. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.11 Fysisk sikring og miljøsikring

**Kontrolmål:**

Formål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelser i organisationen.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 11.2 | Vores teknikrum, som indeholder krydsfelt og linjeindgang, er placeret i Enigheden på Lygten 39, København N. Teknikrum har eget kølingsanlæg og temperaturovervågning, hvorfra der, i tilfælde af temperaturstigning, sendes en alarm til udvalgte medarbejdere (IT-ansvarlige).<br><br>Databærende udstyr, som ikke længere benyttes, opbevares på en reol i vores teknikrum med henblik på eventuel genanvendelse. Når udstyr skal endeligt destrueres, overdrages det til infrastrukturleverandøren Sentia til destruktion på forsvarlig vis. Det skal bemærkes, at der ikke lagres personfølsomme data uden for vores servere hos Sentia.<br><br>Det udstyr vi ejer registreres hos og af vores IT-leverandør Sentia, som opdaterer 'asset listen' ved hver ændring. | Vi har forespurgt til revisorerklæring fra Sentia, og vi har inspiceret erklæringen for betryggende fysisk sikring, og for at identificere understøttende forsyninger og sikring af regelmæssig vedligeholdelse af udstyret.<br><br>Vi har forespurgt til sikring af kabler, og vi har inspiceret revisorerklæring fra Sentia.<br><br>Vi har forespurgt til politik for bortskaffelse af databærende medier, og vi har inspiceret politikken. Endvidere har vi stikprøvevis inspiceret dokumentation for sikker bortskaffelse.<br><br>Vi har forespurgt til sikring af udstyr uden for virksomhedens lokaler.<br><br>Vi har forespurgt til periodisk eftersyn af ekstern lokation, og vi har stikprøvevis inspiceret dokumentation for eftersyn. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.12 Driftssikkerhed

**Kontrolmål:**

Formål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 12.1 | Vores dokumentation og arbejdsprocesser medvirker til at sikre en stabil, korrekt og driftssikker ydelse, hvor personafhængighed og 'sjuske-fejl' minimeres.<br><br>Vores tekniske set-up fokuserer på samme værdier, og værn mod uvedkommendes adgang til vores data er af højeste prioritet.<br><br>Standard ændringer har, i videst muligt omfang, en dedikeret SOP. Alle væsentlige ændringer drøftes, prioriteres og godkendes af ledelsen.<br><br>Operativsystem patchning foretages månedligt i et fastlagt servicevindue. Servicevinduet fremgår af virksomhedens generelle forretningsbetingelser, og skal ikke varsles separat. For kritiske systemopdateringer, eksempelvis Windows security updates, varsles kunderne i så god tid som muligt.<br><br>Tilgængelighed er en af vores kerne-værdier, og vi sætter en ære i altid at levere den forventede kvalitet i ydelser til vores kunder. Et af de væsentlige parametre IDQ måles på af kunderne, er svartider på søgninger gennem IDQ-systemet. Derfor overvåger vi konstant vores kapacitet, både disk, cpu og trafik, og vi kan løbende, og uden gene for kunderne, udvide vores kapacitet. | Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne.<br><br>Vi har forespurgt til ændringsstyring, og vi har stikprøvevis inspiceret dokumentation for håndtering af ændringer i perioden. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende styring af ændringer.<br><br>Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevis inspiceret dokumentation for overvågning af kapacitet. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende overvågning af kapacitet.<br><br>Vi har forespurgt til anvendelsen af testmiljø, og vi har inspiceret dokumentation for eksistensen af testmiljø. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.12 Driftssikkerhed

**Kontrolmål:**

Formål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 12.2 | Til beskyttelse mod malware anvender vi F-Secure antivirus-software på arbejdsstationer og servere. E-mail skanning varetages af vores e-mail leverandør, Sentia, som benytter Fusemail e-mail security, og servicen er en del af vores samlede infrastrukturleverancer. | Vi har forespurgt til foranstaltninger mod malware.<br>Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende kontroller mod malware. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

**Kontrolmål:**

Formål: At beskytte mod tab af data

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 12.3 | Vores kunders data er lige så vigtige som vores egne data, og vi har en procedure for at sikre samme. Vi tager dagligt backup, og vi har, ved vores leverandør, en procedure for kontrol af backup, herunder hvordan der skal ageres ved fejl. | Vi har forespurgt til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for opsætningen.<br>Vi har forespurgt til opbevaring af backup, og vi har inspiceret revisorerklæring fra Sentia med henblik på at se, at backup opbevares forsvarligt.<br>Vi har inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende genoprettelse af backupfiler. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.12 Driftssikkerhed

**Kontrolmål:**

Formål: At registrere hændelser og tilvejebringe bevis.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 12.4 | Vi foretager daglig overvågning af vores systemer via automatiserede systemer til måling af grænseværdier. Alarmering, såfremt en kritisk hændelse konstateres, tilgår vores tekniske medarbejdere. Hændelser relateret til vores fælles platform, infrastruktur og serverrumsydelser håndteres af vores it-leverandør, som uden for kontortid har drifts-vagt. Hændelser for login og logout på vores platforme logføres, og vi benytter alene personhenførbare brugerkonti, hvorfor det er muligt at identificere hvilke personer der har været logget på. | Vi har forespurgt til logning af bruger-aktivitet. Vi har stikprøvevis inspiceret logningskonfigurationerne. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende logningsaktivitet.<br><br>Vi har forespurgt til sikring af logoplysninger, og vi har inspiceret løsningen. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende sikring af logoplysninger.<br><br>Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret revisorerklæring fra Athena med henblik på at identificere betryggende synkronisering op imod en tidsserver. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

**Kontrolmål:**

Formål: At sikre integriteten af driftssystemer

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 12.5 | Patch management foretages af Sentia i fastlagte servicevinduer på månedsbasis. Der installeres alene opdateringer af typen 'Security' og 'Critical'. | Vi har forespurgt til retningslinjer for installation af software på driftssystemer, og vi har inspiceret retningslinjerne.<br><br>Vi har forespurgt til rettidig opdatering af driftssystemer, og vi har inspiceret revisorerklæring fra Sentia med henblik på at identificere kontroller mod rettidig og betryggende opdateringer af driftssystemerne. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.12 Driftssikkerhed

**Kontrolmål:**

Formål: At forhindre, at tekniske sårbarheder udnyttes.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 12.6 | Windows update af arbejdsstationer foregår automatisk. Sikkerhedsopdatering af 3-parts applikationsprogrammel anvendt i egenudviklede systemer er for nuværende op til hver enkelt systemejer.<br><br>Der benyttes GPO'er til at styre rettighederne i domænet. Brugere har pt. "local admin rights" på egen pc, men dette er under udfasning og forventes tilendebragt i løbet af 2019. | Vi har forespurgt til styring af tekniske sårbarheder, og vi har inspiceret dokumentation for styringen.<br><br>Vi har forespurgt til retningslinjer for begrænsning på softwareinstallation, og vi har inspiceret kontroller for begrænsningen. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

**Kontrolmål:**

Formål: At forhindre, at audit forstyrrer den daglige drift.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 12.7 | Virksomheden har årlig ekstern IT-revision. Denne planlægges i samarbejde med revisor, med henblik på at tilsikre mindst mulig afbrydelse af produktion i perioden. | Vi har forespurgt til planlægningen af audit af informationssystemerne mhp. mindst mulig forstyrrelse af den daglige drift. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.13 Kommunikationssikkerhed

**Kontrolmål:**

Formål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 13.1 | Vores tekniske set-up fokuserer på værdier, og værn mod uvedkommendes adgang til, at vores data er af højeste prioritet. Vi har desuden anti-virussystemer, e-mail skanning, og systemer til overvågning og sikring af netværk og internetbrug. Al godkendt netværkstrafik (indgående) kommer igennem vores firewall. Vi har en fast procedure for dokumentation af internt netværk, logisk opdeling af netværk, navngivning af enheder mv. Adgang til netværksydelser via mobile enheder sikres via en MDM-løsning. Adgang fra hjemmearbejdspladser sker via en krypteret VPN-forbindelse. | Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall og patchning af firewall.<br><br>Vi har forespurgt til sikring af netværks-tjenester, og vi har inspiceret dokumentation for betryggende sikring.<br><br>Vi har inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende beskyttelse af netværk og netværkstjenester.<br><br>Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende etablering og patching af firewall. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.13 Kommunikationssikkerhed

**Kontrolmål:**

Formål: At opretholde informationssikkerhed ved overførelse internt i organisation til en ekstern entitet.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 13.2 | Der er udarbejdet politikker og procedurer for dataoverførelser.<br><br>Dataoverførelser over Internettet sker krypteret og er styret af enten underleverandør eller IDQ selv.<br><br>Der laves fortrolighedsaftaler med medarbejdere og samarbejdspartnere. | Vi har forespurgt til politikker og procedurer for dataoverførsel, og vi har inspiceret politikken og proceduren.<br><br>Vi har forespurgt til aftaler om dataoverførsel. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende kontroller for dataoverførsel.<br><br>Vi har forespurgt til retningslinjer for afsendelse af fortrolig information, og vi har inspiceret retningslinjerne.<br><br>Vi har forespurgt til etablering af for-trolighedsaftaler, og vi har inspiceret dokumentation for etablering. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.14 Anskaffelse, udvikling og vedligeholdelse af systemer

**Kontrolmål:**

Formål: At sikre, at informationssikkerhed er en integreret del af informationssystemerne og gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 14.1 | Ved vurdering af nye projekter/produkter er sikkerhedsvurdering en fast bestanddel af vurderingsprocessen. Analyse og kravsspecifikation i forbindelse med nyudvikling og videreudvikling indeholder altid sikkerhedsvurderinger, herunder ledelses- og når relevant, kundegodkendelser.<br><br>Implementering af, og leverancer til, nye kunder foretages i henhold til fastlagte procedurer og relevante SOP'er. | Vi har forespurgt til informationssikkerhedsrelaterede krav til virksomhedens løsning, og vi har inspiceret de opstillede krav.<br><br>Vi har forespurgt til sikring af løsningen på offentlige netværk, og vi har inspiceret løsningen.<br><br>Vi har forespurgt til sikring af transmissioner, hvilket er dækket af Sentia revisorerklæring. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.14 Anskaffelse, udvikling og vedligeholdelse af systemer

**Kontrolmål:**

Formål: At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemernes udviklingscyklus

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 14.2 | Vores retningslinjer for udvikling og ændringshåndtering indeholder faste kriterier for sikkerhedsrelaterede vurderinger, herunder ledelses- og når relevant, kundegodkendelser. Vi har en formel godkendelsesproces for godkendelse af opdateringer, inkluderende test og roll-back planer, for hvert udviklingstrin/produkt.<br><br>Repræsentant fra vores Salg og Ledelse skal godkende kundeopsætningen, hvorfor der sikres overensstemmelse med kontrakt, teknik og forretningskrav. Hver kundekontrakt indeholder desuden specifikation af hvem, hos kunden, der har rettigheder til at fremsende og/eller godkende it- ændringsønsker på vegne af den pågældende virksomhed til IDQ, så der aldrig opstår tvivl om hvem der er ansvarlig for en udført handling. | Vi har forespurgt til politik for styring af udvikling, og vi har inspiceret politikken.<br><br>Vi har forespurgt til procedure for styring af systemændringer, og vi har inspiceret proceduren. Vi har stikprøvevis inspiceret dokumentation for, at proceduren er fulgt.<br><br>Vi har forespurgt til test af applikationer i forbindelse med ændringer og opdatering af driftsplatformen, og vi har inspiceret dokumentation for test.<br><br>Vi har forespurgt til begrænsning af ændringer på softwarepakker, og vi har inspiceret dokumentation for prioritering af ændringer på software.<br><br>Vi har forespurgt til principper for sikker udvikling, og vi har inspiceret udarbejdede principper.<br><br>Vi har forespurgt til sikkert udviklings-miljø, og vi har inspiceret dokumentation for adskillelse mellem udviklingsmiljø og produktionsmiljø.<br><br>Vi har forespurgt til systemsikkerheds-test, og vi har stikprøvevis inspiceret dokumentation for systemsikkerheds-test.<br><br>Vi har forespurgt til systemgodkendelsestest, og vi har stikprøvevis inspiceret dokumentation for systemaccept i forbindelse med udvikling. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.14 Anskaffelse, udvikling og vedligeholdelse af systemer

**Kontrolmål:**

Formål: At sikre beskyttelse af data, som anvendes til test.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 14.3 | Testmiljø og testdata beskyttes på samme måde som produktionsdata. | Vi har forespurgt til anvendelse af testdata, og vi har inspiceret retningslinjerne for produktion af testdata. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.15 Leverandørforhold

**Kontrolmål:**

Formål: At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 15.1 | Implementering af, og leverancer til, nye kunder foretages i henhold til fastlagte kontraktuelle procedurer og relevante procedurer. Repræsentant fra vores Salg og Ledelse skal godkende kundeopsætningen, hvorfor der sikres overensstemmelse med kontrakt, teknik og forretningskrav. Hver kundekontrakt indeholder desuden specifikation af hvem, hos kunden, der har rettigheder til at fremsende og/eller godkende it-ændringsønsker på vegne af den pågældende virksomhed til IDQ, så der aldrig opstår tvivl om hvem der er ansvarlig for en udført handling. | Vi har forespurgt til formalisering af leverandøraftale, og vi har inspiceret aftale med henblik på at efterse hensyntagen til informationssikkerhed.<br><br>Vi har inspiceret revisorerklæring fra Sentia og Ambition med henblik på at identificere, om der er væsentlige bemærkninger, og om den er dækkende i forhold til virksomhedens aftale med leverandøren. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.15 Leverandørforhold

**Kontrolmål:**

Formål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 15.2 | Alle vores leverandør og partneraftaler skal indeholde regulering af fortrolighed. Der indhentes tillige revisorerklæring fra vores kritiske leverandører.<br><br>Tilgængelighed er en af vores kerneværdier, og vi sætter en ære i altid at levere den forventede kvalitet i ydelser til vores kunder. Et af de væsentlige parametre IDQ måles på af kunderne, er svartider på søgninger gennem IDQ-systemet. Derfor overvåger vi konstant vores kapacitet, både disk, cpu og trafik, og vi kan løbende, og uden gene for kunderne, udvide vores kapacitet. | Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning.<br><br>Vi har inspiceret revisorerklæring fra Sentia med henblik på at identificere, om der er væsentlige bemærkninger, og om den er dækkende i forhold til virksomhedens aftale med leverandøren. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.16 Styring af sikkerhedsbrud

**Kontrolmål:**

Formål: At sikre ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og –svagheder.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 16.1 | Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af hændelser. Vi har en række tiltag for at forhindre at sikkerhedshændelser opstår, og vi har driftsvagtordning med vores infrastrukturleverandør, således at der reageres straks en hændelse måtte opstå. Vi holder os tillige fagligt opdaterede vha. producenternes hjemmesider, debatfora mv.<br><br>Alle sikkerhedsbrud dokumenteres til internt brug, og hændelsen gennemgås med alle relevante medarbejdere ved førstkommende lejlighed. Afhængig af hændelsens karakter udarbejdes nye processer og procedurer, så vi undgår at hændelsen indtræffer igen.<br><br>Sikkerhedsrelaterede emner, generelle såvel som aktuelle emner, gennemgås desuden ved interne møder.<br><br>Ved kriminelle forhold sker en politimæssig efterforskning, hvor vores logføring og øvrige overvågning kan benyttes til opklaring og evaluering af sikkerhedshændelsen. | Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har desuden inspiceret procedure til håndtering af informationssikkerhedshændelser.<br><br>Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har forespurgt til retningslinjerne.<br><br>Vi har forespurgt til informationssikkerhedshændelser i perioden.<br><br>Vi har forespurgt til procedure for evaluering af informationssikkerheds-brud, og vi har inspiceret proceduren. Endvidere har vi inspiceret revisorerklæring fra Sentia med henblik på at identificere betryggende styring af informationssikkerhedshændelser. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.17 Informationssikkerhedsaspekter ved ned-, beredskabs- og reetablering

**Kontrolmål:**

Formål: at sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for beredskabs- og reetableringsstyring.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 17.1 | Skulle en nødsituation opstå har IDQ udarbejdet en beredskabsplan. Beredskabsplanen er udarbejdet i henhold til vores it-sikkerhedspolitik og risikoanalyse, og den vedligeholdes minimum årligt. Planen testes, og plan og procedurer er forankret i vores driftsdokumentation og procedurer. Vores beredskabsplanlægning tager højde for at vi kan levere vores ydelser rettidigt – næsten uanset hvad der sker. | Vi har forespurgt til udarbejdelsen af en beredskabsplan til sikring af videreførelse af driften i forbindelse med nedbrud og lignende, og vi har inspiceret planen.<br><br>Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test.<br><br>Vi har forespurgt til implementering af kompenserende tiltag i forbindelse med test af beredskabsplan, og vi har inspiceret dokumentation for implementeringen.<br><br>Vi har endvidere forespurgt til opdatering af beredskabsplanen, og vi har inspiceret dokumentation for opdatering. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

**Kontrolmål:**

Formål: At sikre tilgængelighed af informationsbehandlingsfaciliteter.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 17.2 | Vores beredskabsplanlægning tager højde for at vi kan levere vores ydelser rettidigt – næsten uanset hvad der sker. | Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret revisorerklæring fra Athena med henblik på at identificere tilgængelighed af driftssystemer. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.18 Overensstemmelse

**Kontrolmål:**

Formål: At sikre, at informationssikkerhed drives i overensstemmelse med lov- og kontraktkrav.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 18.1 | Vi er underlagt EU GDPR i forhold til vores ydelser. Gennem softwareløsninger og databehandlingsservices optræder IDQ som databehandler underlagt GDPR (Persondataforordningen). Vores kunder kan dog være underlagt særlig lovgivning, og hvor det måtte være tilfældet, er vores understøttelse heraf aftalt særskilt. Med mindre andet er aftalt, er vores kunder selv ansvarlige for at etablere forbindelse til vores servere.<br><br>Implementering af, og leverancer til, nye kunder foretages i henhold til fastlagte kontraktuelle procedurer og relevante procedurer. Repræsentant fra vores Salg og Ledelse skal godkende kundeopsætningen, hvorfor der sikres overensstemmelse med kontrakt, teknik og forretningskrav. Hver kundekontrakt indeholder desuden specifikation af hvem, hos kunden, der har rettigheder til at fremsende og/eller godkende it-ændringsønsker på vegne af den pågældende virksomhed til IDQ, så der aldrig opstår tvivl om hvem der er ansvarlig for en udført handling. | Vi har kontrolleret, at ansvar for overholdelse af lov- og kontraktkrav er placeret i organisationen.<br><br>Vi har inspiceret, at ophavsret til systemsoftware overholdes.<br><br>Vi har gennemgået udarbejdelse af ISAE 3000 erklæring som databehandler.<br><br>Vi har inspiceret, at ledelsen styrer informationssikkerheden og implementering af kontroller.<br><br>Vi har inspiceret årshjul for ledelseskontroller. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |

# 4.18 Overensstemmelse

**Kontrolmål:**

Formål: At sikre, at informationssikkerhed drives i overensstemmelse med lov- og kontraktkrav.

| Nr. | IDQ A/S kontrol | Revisors udførte test | Resultat af revisors test |
|---|---|---|---|
| 18.2 | Vi lader os årlige revidere af ekstern revisor med henblik på afgivelse af erklæring for overholdelsen af kontrollerne nævnt i denne beskrivelse. Vi følger rammerne inden for ISO 27002, hvilket føromtalte revisor attesterer i en ISAE 3402-erklæring. | Vi har forespurgt til uafhængig evaluering af informationssikkerheden.<br><br>Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerhedspolitik og procedurer, og vi har inspiceret udvalgte kontroller.<br><br>Vi har forespurgt til periodisk kontrol af teknisk overensstemmelse, og vi har inspiceret dokumentation for overvågning. | Vores gennemgang har ikke ført til væsentlige bemærkninger. |




"Grant Thornton" henviser til det brand, hvorunder Grant Thorntons medlemsfirmaer leverer tjenesteydelser indenfor revision, regnskab, skat og rådgivning til deres kunder og/eller til et eller flere medlemsfirmaer, afhængig af konteksten.

Grant Thornton Danmark er medlem af firmaet Grant Thornton International Ltd (GTIL). GTIL og medlemsvirksomhederne er ikke et globalt partnerskab. GTIL og hvert enkelt medlemsfirma udgør hver især en separat juridisk enhed. Tjenesteydelser leveres af medlemsfirmaerne. GTIL leverer ikke tjenesteydelser til kunder. GTIL og dets medlemmer repræsenterer og forpligter ikke hinanden og er heller ikke ansvarlige for hinandens handlinger og forsømmelser.

PENNEO

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

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

**Henrik Saustrup**
**Underskriver**
*Serienummer: CVR:34046220-RID:14399917*
*IP: 87.60.xxx.xxx*
*2020-05-01 08:20:28Z*
NEM ID

**Anders Grønning Kjærgaard**
**Revisor**
*Serienummer: PID:9208-2002-2-822661869402*
*IP: 213.32.xxx.xxx*
*2020-05-01 09:23:51Z*
NEM ID

**Jacob Helly Juell-Hansen**
**Statsautoriseret revisor**
*Serienummer: CVR:34209936-RID:50904197*
*IP: 62.243.xxx.xxx*
*2020-05-01 13:21:19Z*
NEM ID