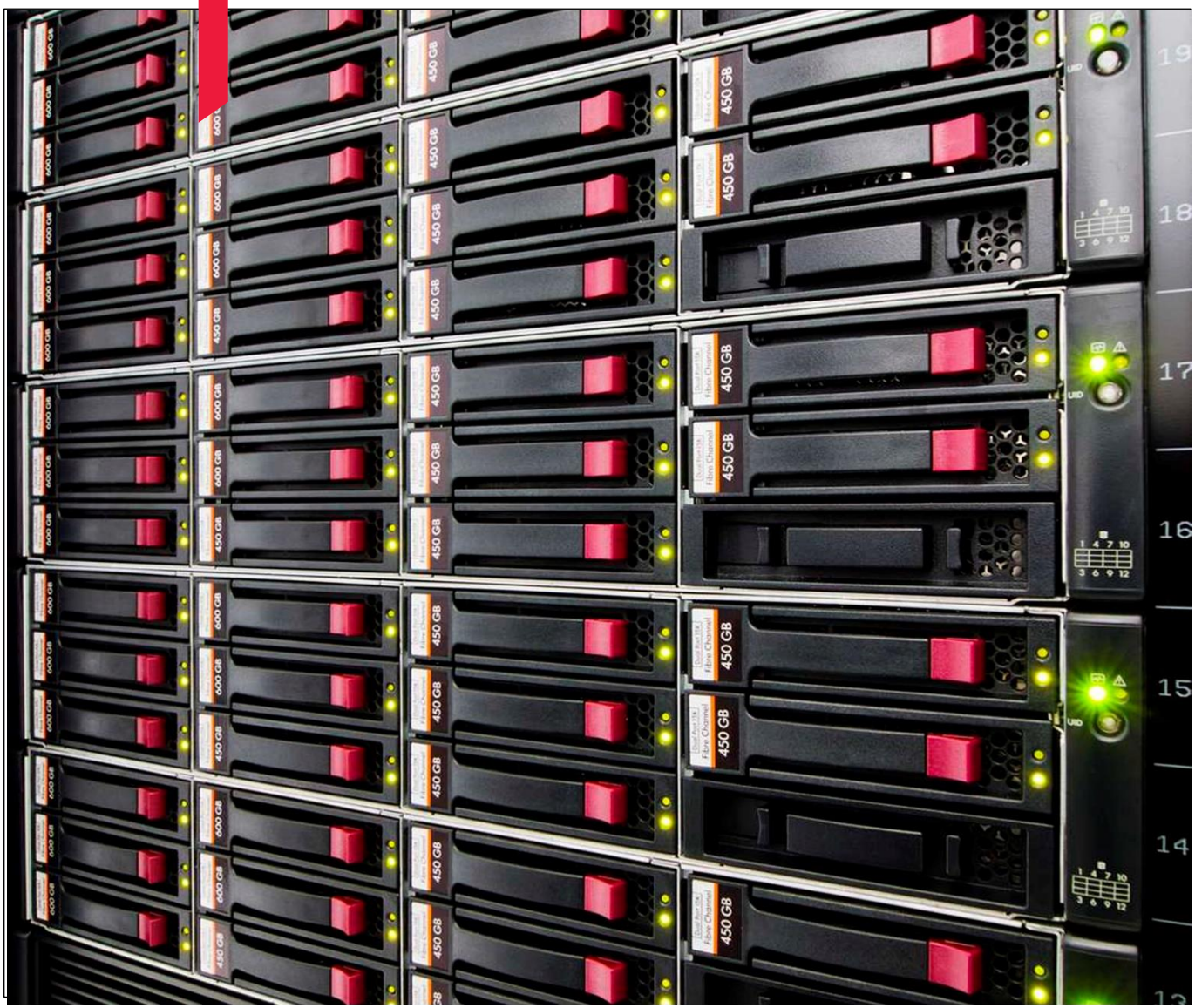

.LEGAL A/S

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. SEPTEMBER 2020 TIL 31. AUGUST 2021 OM BESKRIVELSEN AF PACTIUS OG DPA SERVICE OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. AUGUST 2020 TIL 31. AUGUST 2021 OM BESKRIVELSEN AF PACTIUS OG DPA SERVICE OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

Til: Ledelsen i .legal A/S
.legal A/S kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om den af .legal A/S (serviceleverandøren) for hele perioden fra 1. september 2020 til 31. august 2021 udarbejdede beskrivelse i sektion 3 af PACTIUS og DPA Service og de tilhørende kontroller, og om udformningen og den operationelle effektivitet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandørens ansvar

Serviceleverandøren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Serviceleverandøren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom serviceleverandøren er ansvarlig for at anføre kontrolmålene samt udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i overensstemmelse med de internationale etiske regler for revisorer (IESBA's Etiske regler), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vi er underlagt den internationale standard om kvalitetsstyring ISQC 1, og vi anvender og opretholder således et omfattende kvalitetsstyringssystem, 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 serviceleverandørens beskrivelse samt om udformningen og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed kontroller hos en serviceorganisation. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

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

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

Begrænsninger i kontroller hos en serviceleverandør

Serviceleverandørens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af virksomhedens kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af PACTIUS og DPA Service, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller 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. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i serviceleverandørens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af PACTIUS og DPA Service og de tilhørende kontroller, således som de var udformet og implementeret i hele perioden fra 1. september 2020 til 31. august 2021, i alle væsentlige henseender er retvisende, og

b. at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. september 2020 til 31. august 2021, og

c. at de testede kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. september 2020 til 31. august 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt serviceleverandørens PACTIUS og DPA Service, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundens egne kontroller, ved opnåelsen af en forståelse af kundernes informationssystemer, der er relevante for regnskabsaflæggelsen.

København, den 27. september 2021

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Chef for Risk Assurance, CISA, CRISC

2. .LEGAL A/S UDTALELSE

.legal A/S leverer driftsydelser på systemerne PACTIUS OG DPA Service til selskabets kunder.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt PACTIUS og DPA Service, 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, når de opnår en forståelse af kunders informationssystemer, som er relevante for regnskabsaflæggelsen.

.legal A/S anvender serviceunderleverandør. Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse.

.legal A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af PACTIUS og DPA Service og de tilhørende kontroller i hele perioden fra 1. september 2020 til 31. august 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for PACTIUS og DPA Service, og hvordan de tilhørende kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser, der er leveret.
    - De processer i både it- og manuelle systemer, der er anvendt til styringen af de generelle it-kontroller.
    - 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.

2. Indeholder relevante oplysninger om ændringer i serviceleverandørens PACTIUS og DPA Service foretaget i perioden fra 1. september 2020 til 31. august 2021.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af PACTIUS og DPA Service og de tilhørende kontroller under hensyntagen til, at denne beskrivelse 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 PACTIUS og DPA Service, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

.legal A/S bekræfter, at de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. september 2020 til 31. august 2021. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

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

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra fra 1. september 2020 til 31. august 2021.

Aarhus, den 27. September 2021

.legal A/S

Brian Østberg
Managing Director

3. .LEGAL A/S´S BESKRIVELSE AF DRIFT KONTROLMILJØ PÅ PACTIUS OG DPA SERVICE

.legal produktfamilie
PACTIUS og DPA Service er 100% afkoblede systemer, men stadig en del af den samme. legal produktfamilie. Vi har valgt at lade dem kontrollere efter samme standard, da vi ønsker at alle produkter, der kommer fra .legal A/S skal leve op til en ensartet høj standard i forhold til IT-drift og sikkerhed.

PRACTIUS
PACTIUS er et kontraktstyrings- og GDPR compliancesystem der udvikles og drives af. legal A/S. PACTIUS kan anvendes til alt fra simpel opbevaring af kontrakter til opfølgning på rettigheder, forpligtelser og komplekse leverancer på store it-, entreprise- og outsourcing kontrakter.

Derudover har PACTIUS et tillægsmodul kaldet "Pactius Privacy". Pactius Privacy er et compliancevæktøj til at dokumentere og administrere organisationens behandling af personoplysninger. Formålet med Pactius Privacy er hjælpe virksomheder med at leve op persondataforordningen.

DPA Service
DPA (Data Processor Audit) Service er et system, der udvikles og drives af .legal A/S, til digital kontrol af en kundes databehandlere. Som en del af GDPR er at man som virksomhed eller myndighed forpligtet til løbende at føre kontrol med sine databehandlere. Formålet med DPA Service er at gøre denne proces nemmere, men samtidig sikre at kontrollerne lever op til Datatilsynets krav.

MS Azure udgør den overordnede IT platform for systemerne i .Legal A/S.

- Koden opbevares og styres i Azure DevOps.
- Data opbevares i Azure Storage, Azure SQL samt Azure Cosmos DB i europæiske datacentre i hhv. Amsterdam og Dublin.
- Test- og driftmiljøer til applikationerne er etableret i Azure.

I forhold til brug af 3. parts services uden for Azure udvælges disse ud fra krav om høj sikkerhedsstandard samt overholdelse af GDPR. Generelt forsøger vi at mindske behovet for 3. parts services uden for MS Azure.

.legals beskrivelse af kontrolmiljø

Generelt - retningslinjer og kontrolmål
Vi har internt defineret en række kontrolmål, der anvendes til at kontrollere og sikre at vores sikkerhedspolitikker og retningslinjer overholdes.

Kontrolmålene indeholder:

- Formål: Beskriver hvorfor kontrolmålet er etableret og sikrer, at det afspejler den overordnede retningslinje for ISO-afsnittet.
- Målepunkt: Beskriver hvordan kontrolmålet skal vurderes, således at der etableres et tilfredsstillende datagrundlag, og så målingen kan gennemføres inden for det tidsinterval, der er beskrevet, hvilket sikrer, at målet er specifikt og målbart.
- Tærskel: Viser, hvad der kræves for at kontrolmålet overholdes.

Der er defineret formål, målepunkter og tærskel på alle relevante områder med udgangspunkt i ISO 27001. Som systemunderstøttelse til opfølgning og dokumentation på de interne kontrolmål anvendes PACTIUS.

A.4 Risikovurdering
Direktionen i .legal A/S laver minimum én gang årligt en risikovurdering, der omfatter IT-installationerne og brugen heraf. Der tages udgangspunkt i det nuværende trusselbillede samt ny viden på området, der tilsammen danner grundlag for nye sikkerhedsinitiativer.

A.5 Informationssikkerhed
.legal arbejder efter en IT sikkerhedspolitik som dækker PACTIUS og DPA Service. IT-sikkerhedspolitikken er organiseret efter ISO 27001:2013 og danner grundlag for de involveredes omgang med PACTIUS og DPA service. IT-sikkerhedspolitikken er organiseret efter de standardiserede ISO-områder.

Opfølgningen på om kravene overholdes sker i henhold til en række retningslinjer og kontrolmål, der er beskrevet i politikken for hvert ISO-område.

IT-sikkerhedspolitikken er godkendt af ledelsen og offentliggjort i virksomheden, herunder kommunikeret til relevante ansatte og samarbejdspartnere. for at sikre at IT-sikkerhedspolitikken er passende, tilstrækkelig og effektiv, revurderes IT sikkerhedspolitikken minimum én gang årligt eller ved omfattende ændringer i organisationen, som har indflydelse på informationssikkerheden.

A.6 Organisation af informationssikkerhed
.legal har en overordnet IT sikkerhedsansvarlig med ansvar for den organisatoriske samt systemmæssige sikkerhed.

.legal arbejder med funktionsadskillelse, for at sikre, at medarbejdere alene får adgang til informationer, der er påkrævet for at udføre deres funktion. Der arbejdes med funktionerne "administration", "salg", "udvikling", "support" og "drift". Vi revurderer regelmæssigt alle medarbejderes adgange for at sikre, at adgangene fortsat stemmer overens med deres jobfunktion.

A.7 Personalesikkerhed
Alle medarbejdere/konsulenter har som en del af ansættelsen indgået tavshedspligt der sikrer at fortrolig information ikke bliver videregivet. Tavshedspligten gælder både under og efter ansættelse. Tilmed underskriver de relevante medarbejdere erklæring om overholdelse af IT Sikkerhedspolitikken, der yderligere sikrer at oplysninger om systemet og dennes sikkerhedsforhold, medarbejdere, forretningshemmeligheder og oplysninger om forretningsforbindelser forbliver fortrolige.

A.8 Styring af aktiver
Alle systemernes aktiver er identificeret, og der er udarbejdet en fortegnelse over aktiverne. Aktivfortegnelsen er dokumenteret og indeholder relevante beskrivelser af delkomponenter, fysisk og logisk placering samt ejerskab.

A.9 Adgangsstyring
Adgange til systemerne tildeles altid med udgangspunkt i "need-to-know"/ "need-to-have" og "least privilege"-principperne, så det tilsikres, at adgange er tildelt brugere med et arbejdsbetinget behov.

Systemadgang
Der er flere muligheder for systemadgang, alt efter hvilket system vi taler om. Mulighederne spænder fra single sign-on løsning via integration med kundens Microsoft Azure Active Directory til almindelig email/password-autentificering eller via .legal ID.

.legal ID er en egenudviklet login-provider baseret på sikkerhedsprotokollerne OpenID Connect / OAuth2.0 og giver mulighed for at brugeren kan benytte sit .legal ID på tværs af .legal produkter. Tilmed giver .legal ID mulighed for 2-faktor autentifikation.

Roller og rettigheder
Adgang til funktionalitet i systemerne styres via en rollebaseret model, hvor en bruger tildeles en række roller, der giver adgang til bestemte dele eller funktioner i systemet. I systemer, hvor der er behov, kan rettighederne yderligere granuleres i forhold til læse og skriveadgang.

Platformadgang
En medarbejder med behov for adgang til produktionsdata eller produktionsinfrastruktur (privilegeret adgang), skal i tillæg til et arbejdsbetinget behov, have særskilt godkendelse fra direktionen. Medarbejdere med privilegeret adgang anvender altid 2-faktor autentifikation.

A.10 Kryptografi
Systemet er en ren browserbaseret løsning. Der er i systemet udelukkende krypteret kommunikationen mellem klienten (browseren) og serveren. Systemet anvender et SHA-2 SSL-certifikat med minimum 2048bit kryptering fra en pålidelig udbyder. Data krypteres, når det bliver gemt i datacenteret, og dekrypteres automatisk, når det skal tilgås.

A.11 Fysisk sikring og miljøsikring
.legals lokaler er til enhver tid aflåst. .legal hoster ikke selv løsninger, hvilket gør at den fysiske sikring først og fremmest vedrører medarbejdernes maskiner. Alle medarbejderes maskiner er krypteret.

A.12 Driftssikkerhed

Hosting-leverandør
Microsoft Azure udgør den overordnede IT platform for systemerne i .legal A/S.

- Koden opbevares og styres i Azure DevOps.
- Data opbevares i Azure Storage, Azure SQL samt Azure Cosmos DB i europæiske datacentre i hhv. Amsterdam og Dublin.
- Test- og driftmiljøer til applikationerne er ligeledes etableret i Azure.

Systemerne hostes i Microsoft Azure – bl.a. af sikkerhedsmæssige hensyn, da den underliggende platform altid er up-to-date, samt at muligheder for datakryptering, redundans, backup og adgangsstyring generelt er gode.

I forhold til brug af 3. parts services uden for Azure udvælges disse ud fra krav om høj sikkerhedsstandard (f.eks. ISO27001 certificering) samt overholdelse af GDPR. Generelt forsøger vi at mindske behovet for 3. parts services uden for Microsoft Azure.

Redundans
Produktionsmiljøets primære datalokation til dokumenter er Amsterdam (Western Europe). På denne lokation gemmes data i 3 forskellige kopier. I tilfælde af nedbrud skiftes der i Azure platformens opsætning automatisk over på en af de redundante kopier. Systemet anvender Geo Redundant Storage (GRS).

Backup
PACTIUS foretager natlig backup af data i produktionsmiljøet som lagres i 7 dage. Dertil kommer en månedlig backup, der lagres i 3 måneder. Backup replikeres 3 gange indenfor samme datacenter som databasen kører i (Amsterdam, Wester Europe).
DPA Service kører der continuos backup, der muliggør restore af data til et bestemt tidspunkt. Der kan maksimalt restores 30 dage tilbage i tid. Backup replikeres 3 gange indenfor samme datacenter som databasen kører i (Amsterdam, Wester Europe).

Logning, Monitorering og Alerts
Systemhændelser logges til en centralt systemlog, således er det muligt at spore eventuelle fejl på tværs af komponenter i det samlede system. Det samlede system bliver monitoreret via Dashboards, hvor vi kan følge ressourceforbrug, brugen samt fejl i et samlet overblik. På baggrund af den centraliserede log er der defineret en række alarmer, der håndteres af udviklingsteamet.

A.13 Kommunikationssikkerhed
Kommunikation mellem browseren og resten af systemet foregår via HTTPS (SHA-2 SSL-certifikat med minimum 2048bit kryptering). Udveksling af data mellem kunderne og systemet foregår enten via SFTP eller indbygget funktionalitet til import og eksport af data, som igen er beskyttet med HTTPS.

Alle medarbejdere og eventuelle underleverandører er underlagt fortrolighedsaftaler, som gælder både under og efter man har arbejdet med systemerne.

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

Udviklingsproces
Omdrejningspunktet for vores daglige arbejde er vores fælles udviklingsproces, der baserer sig på moderne men velafprøvede metoder som SCRUM og Kanban. Hvert produkt har egen produktejer med ansvar for planlægning og prioritering samt et fast udviklingsteam med ansvar for udvikling og kvalitetssikring. Dertil kommer support, der taler direkte med produktejeren, udviklingsteamet og kunderne.

Udviklingsprocessen sikrer at vi sparer mundtlig på daglig basis, vender eventuelle udfordringer og hjælper hinanden til effektive løsninger. Vi har flere øjne på de ændringer, vi foretager os, og gør aktivt en indsats for hele tiden at dygtiggøre os og forbedre de systemer, vi arbejder med.

Alle udviklingsteams har erfarne folk om bord for at sikre et højt niveau - også når det gælder sikkerhed.

Kvalitetssikring
Kvalitetssikrende elementer fra den fælles .legal udviklingsproces:

- Struktureret proces - Alt arbejde, uanset karakter, visualiseres som opgaver i vores opgavestyring. Alle opgaver skal igennem den samme overordnede proces med flere faser der bl.a. dækker kodereview, intern test og accept test.

- Automatiseret kvalitetssikring
    - Versionsstyret kode
    - Continuos Integration der løbende bygger koden for at sikre integritet
    - Automatiserede tests der løbende kører for at minimere regressionsfejl
    - Automatiserede deployment pipelines som gør at vi sikkert og med høj sporbarhed kan deploye ny kode til test og produktionsmiljøer.

- Udviklings-, test- og produktionsmiljø

Dedikerede udviklings, test og produktionsmiljøer for at kunne kvalitetssikre på flere niveauer før ny kode når produktionsmiljøet.

- Overvågning og alarmering

Vores miljøer er monitoreret således at vi kan sikre høj oppetid og får alarmer om eventuelle fejl eller sårbarheder så hurtigt som muligt.

A.15 Leverandørforhold
.legal har fastsat procedure for indgåelse af aftaler med leverandører. Fokuspunkter i den forbindelse er følgende:

- Der indgås leverandøraftaler med alle kunder der benytter sig systemerne.
- Eventuelle underleverandører skal leve op til samme sikkerhedsstandard og efterleve samme sikkerhedspolitikker som .legal A/S.
- .legal foretager årligt en sikkerhedskontrol

A.16 Styring af informationssikkerhedsbrud
Alle sikkerhedsmæssige hændelser eller observerede svagheder rapporteres til direktionen eller den sikkerhedsansvarlige. Så snart der er rapporteret en sikkerhedshændelse eller svaghed sættes følgende aktiviteter i gang:

1. Sikkerhedshændelsen registreres i virksomhedens opgavestyring.
2. I opgavens beskrivelse noteres sikkerhedshændelsen/svagheden i så mange detaljer som muligt, herunder som minimum:
   -Hvornår hændelsen fandt sted
   -Hvad hændelsen konkret gik ud på
   -Hvem der har indrapporteret hændelsen
3. Hændelsen analyseres herefter med henblik på følgende:
   -Afgøre hvor omfattende hændelsen er
   -Hvilke kunder der er berørt
   -Hvad der skal gøres for at enten standse hændelsen eller imødekomme hændelsen i fremtiden f.eks. ved koderettelser
4. Kunder identificeret i punkt 3, informeres herefter omkring hændelsen og konsekvenserne af hændelsen, samt hvilke tiltag der er taget fremadrettet.
5. De tiltag der er blevet besluttet prioriteres og iværksættes
6. Når tiltagene er implementeret lukkes opgaven.
7. Efter problemet er løst beskrives forløbet som et incident i projektets incidentlog. Formålet er at undersøge om der er et underlæggende rodproblem, der kan give anledning til yderligere forbedringer eller hjælpe til udbedring af lignende fremtidige problemer.

A.18: Overensstemmelse
Det påhviler direktionen i .legal A/S, at lovgivningsmæssige sikkerhedskrav overholdes og at der regelmæssigt vurderes om .legal A/S er compliant.

En gang om året anmoder .legal A/S direktionen i advokatvirksomheden Bech-Bruun om at vurdere, om der er sket ændringer i lovgivningen på en måde, så der skal ændres i sikkerhedspolitikken og/eller i systemet. Resultatet af anmodning noteres på bestyrelsesmødet og eventuelle afledte ændringer implementeres.

Brugervirksomhederne egen kontroller og ansvar
Brugervirksomhederne er forpligtet til at implementere følgende komplementerende kontroller for at opnå kontrolmålene:

- Brugervirksomhederne har ansvaret for at sikre, at egne administratorers brug af PACTIUS og DPA Service sker betryggende, og i overensstemmelse med gældende aftale.
- Brugervirksomhederne styrer brugerrettighederne i PACTIUS og DPA Service, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte brugere tildeles.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed om kontroller hos en serviceorganisation.

BDO har udført handlinger for at opnå bevis for oplysningerne i .legal A/S´s beskrivelse PACTIUS og DPA Service samt for udformningen og den operationelle effektivitet af de tilhørende kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af .legal A/S, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden fra 1. september 2020 til 31. august 2021.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion, observation og genudførelse.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som MZ Azure leverer inden for hosting service, har vi modtaget en SOC 2-rapport for perioden fra 1. oktober 2019 til 30. september 2020 og tilhørende bridge letters frem til ultimo Q2 2021 vedrørende serviceunderleverandørens kontroller samt leverandørens ISO-certificering med udløb 18. juni 2023.

Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i .legal A/S´s beskrivelse af PACTIUS og DPA Service og de tilhørende kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos .legal A/S, der sikrer overvågning af serviceunderleverandørens opfyldelse af den mellem serviceunderleverandøren og .Legal A/S indgåede aftale.

Resultat af test

Resultatet af de udførte test af kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet og implementeret eller ikke har fungeret effektivt i perioden.

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed

- *At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
5.1.1 Politikker for informationssikkerhed ▶ Ledelsen skal fastlægge og godkende et sæt af politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne partner.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at ledelsen har fastlagt og godkendt et sæt af politikker for informationssikkerhed. Vi har inspiceret, at nyeste versioner af politikkerne er offentliggjort og kommunikeret ud til medarbejderne og relevante eksterne partner.	Ingen afvigelser konstateret.
5.1.2 Gennemgang af politikker for informationssikkerhed ▶ Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at informationssikkerhedspolitikkerne er opdateret og ledelsesgodkendt 16. August. 2021.	Ingen afvigelser konstateret.

A.6 Organisering af informationssikkerhed

Kontrolmål

- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.6.1.1 Roller og ansvarsområder for informationssikkerhed ▶ Alle ansvarsområder for informationssikkerhed skal defineres og fordeles	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at alle ansvarsområder for informationssikkerhed er defineret og fordelt.	Ingen afvigelser konstateret.
A.6.1.2 Funktionsadskillelse ▶ Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisations aktiver	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for funktionsadskillelse og observeret, at serviceleverandøren har defineret roller, således ansvarsområder adskilles. Vi har observeret, at alle administratoroprettelser skal godkendes af serviceleverandørens direktion. Vi har inspiceret serviceleverandørens medarbejderliste og observeret, hvilke jobfunktioner medarbejderne har. Vi har inspiceret brugerudtræk for relevante systemer og observeret, at der er funktionsadskillelse. Vi har på forespørgsel fået oplyst, at der har været to administratoroprettelser i perioden. Vi har stikprøvevist inspiceret, at der er indhentet ledelsesgodkendelse for én af administratoroprettelserne.	Ingen afvigelser konstateret.

A.7 Personalesikkerhed

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændringer eller ophør*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.7.2.1 Ledelsesansvar ▶ Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med serviceleverandørens fastlagte politikker og procedurer	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for personale- og leverandør sikkerhed. Vi har observeret, at serviceleverandørens ledelse kræver, at alle medarbejdere og kontrahenter underskriver en erklæring omkring, at organisationens fastlagte politikker og procedurer indenfor informationssikkerhed forstås. Vi har på baggrund af serviceleverandørens 19 medarbejdere stikprøvevist inspiceret tre underskrevene erklæringer.	Ingen afvigelser konstateret.
A.7.3.1 Ansættelsesforholdets ophør og ændringer ▶ Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændringer, skal defineres og kommunikeres til medarbejderen eller kontrahenten	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens ansættelseskontraktskabelon og observeret, at der her i står beskrevet medarbejdernes forpligtelser og ansvar efter ansættelsens ophør eller ændringer. Vi har på baggrund af serviceleverandørens 19 medarbejdere stikprøvevist inspiceret tre underskrevene ansættelseskontrakter fra serviceleverandørens medarbejdere.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

Kontrolmål

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.8.1.1 Fortegnelse over aktiver ▶ Aktiver til relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens fortegnelse over aktiver i relation til information og informationsbehandlingsfaciliteter. Vi har observeret, at den senest er opdateret i August 2021.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester*
- *At forhindre uautoriseret adgang til systemer og applikationer*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.9.1.2 Adgang til netværk og netværkstjenester ▶ Der forefindes procedure i henhold til sikring af at brugere kun har adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adgangsstyring. Vi har observeret, at proceduren indeholder krav om adgangsminimering til netværk og netværkstjenester. Vi har inspiceret, at kun et begrænset antal medarbejdere med et arbejdsbetinget behov har adgang til serviceleverandørens netværk og netværkstjenester.	Ingen afvigelser konstateret.
A.9.2.2 Tildeling af brugeradgang ▶ Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adgangsstyring og observeret, at rettigheder skal gives ud fra et arbejdsbetinget behov. Vi har på forespørgsel fået oplyst, at når en ny medarbejder ansættes vurderes det af nærmeste leder og der gives herefter rettigheder til vedkommende. Vi har observeret, at serviceleverandøren har ansat to nye medarbejdere i perioden, som henholdsvis skal arbejde med support af PACTIUS og DPA Service. Vi har inspiceret, at serviceleverandøren kun har givet medarbejdere med et arbejdsbetinget behov adgang til systemerne.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester*
- *At forhindre uautoriseret adgang til systemer og applikationer*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.9.2.3 Styring af privilegerede adgangsrettigheder ▶ Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adgangsstyring og observeret, at serviceleverandøren har beskrevet hvordan styringen af privilegerede adgangsrettigheder sker. Vi har på forespørgsel fået oplyst, at to medarbejdere har fået tildelt privilegerede adgangsrettigheder i erklæringsperioden. Vi har stikprøvevist inspiceret én af tildelingerne og observeret, at den følger proceduren for tildeling af privilegerede adgangsrettigheder.	Ingen afvigelser konstateret.
A.9.2.5 Gennemgang af brugeradgangsrettigheder ▶ Der foretages periodisk gennemgang af brugerrettigheder.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandøren har gennemført periodisk gennemgang af alle tildelte adgangsrettigheder.	Ingen afvigelser konstateret.
A.9.4.1 Begrænset adgang til informationer ▶ Der er en procedure for begrænsning af adgang til information og applikationssystemer	Vi har udført forespørgsler hos relevant personale Vi har inspiceret, at serviceleverandøren har niveauopdelt adgangsrettigheder til systemerne PACTIUS og DPA Service. Vi har inspiceret serviceleverandørens procedure for adgangsstyring og observeret, at rettigheder skal gives efter et arbejdsbetinget behov. Vi har inspiceret, at serviceleverandøren har givet medarbejdere adgange og tilhørende rettigheder efter et arbejdsbetinget behov.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester*
- *At forhindre uautoriseret adgang til systemer og applikationer*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.9.4.2 Procedurer for sikker log-on ▶ Der kræves i henhold til politikken for adgangsstyring, at adgang til systemer og applikationer styres af en procedure for sikker log-on.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at der er implementeret to-faktor login.	Ingen afvigelser konstateret.
A.9.4.3 System for administration af adgangskoder ▶ Der er implementeret en procedure for administration af systemadministrator adgangskoder	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandøren har implementeret De-vops til brug af administration af systemnøgler.	Ingen afvigelser konstateret.
A.9.4.5 Styrings af adgang til kildekoder til programmer ▶ Adgangen til kildekoder til programmer begrænset	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for kildekoder og observeret, at kildekoder opbevares i DevOps i et dedikeret projekt. Vi har inspiceret at serviceleverandøren opbevarer kildekoder i DevOps og det kun er udviklere, som har adgang til koderne.	Ingen afvigelser konstateret.

A.10 Kryptografi		
Kontrolmål ▶ *At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
A.10.1.1 Politik for anvendelse af kryptografi ▶ Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens politik for kryptering og observeret, at systemerne skal anvende et SHA-2 SSL-certifikat med minimum 2048 bit kryptering. Vi har inspiceret, at systemerne anvender et SHA-2 SSL-certifikat med minimum 2048 bit kryptering. Vi har yderligere inspiceret, at Microsoft Azure ligeledes anvender kryptering i overensstemmelse med proceduren.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.11.1.3 Sikring af kontorer, lokaler og faciliteter ▶ Der er etableret fysisk sikring af kontorer, lokaler og faciliteter	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og observeret, at der skal etableres fysisk sikring af kontoret. Vi har foretaget fysisk inspektion af serviceleverandørens kontor i Aarhus og observeret, at der er etableret lås og alarm både til kontoret og til bygningen.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter*
- *At beskytte mod tab af data*
- *At registrere hændelser og tilvejebringe bevis*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.12.1.1 Dokumenterede driftsprocedurer ▶ Driftsprocedurer skal dokumenteres og gøres tilgængelige for alle brugere, der har brug for dem	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandøren har udarbejdet en driftsprocedure, og den ligger tilgængelig på deres fælles Sharepoint.	Ingen afvigelser konstateret.
A.12.1.2 Ændringsstyring ▶ Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, skal styres	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandøren har en udviklingsprocedure og observeret, at de har en procedure for ændringsstyring. Vi har observeret, at der skal være versionering og sporbarhed i alle ændringer. Vi har inspiceret, at ændringer styres gennem versionering og sporbarhed.	Ingen afvigelser konstateret.
A.12.1.4 Adskillelse af udviklings-, test og driftsmiljøet ▶ Udviklings, test- og driftsmiljøer skal adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljø	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adskillelse. Vi har inspiceret, at der er adskillelse mellem udviklings-, test og driftsmiljøet for PACTIUS og DPA Service.	Ingen afvigelser konstateret.
A.12.3.1 Backup af information ▶ Der skal tages backupkopier af informations, software og systembilleder, og disse skal testes regelmæssigt i overensstemmelse med den aftalte backuppolitik	Vi har udført forespørgsler hos relevant personale.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter*
- *At beskytte mod tab af data*
- *At registrere hændelser og tilvejebringe bevis*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret serviceleverandørens procedure for backup og observeret, at det ligger i Microsoft Azure. Vi har observeret, at systemet skal foretage natlig backup af data i produktionsmiljøet som lagres i 7 dage. Dertil kommer en månedlig backup, der lagres i 3 måneder. Derudover har vi observeret, at der skal foretages årligt reststore test af backuppen. Vi har inspiceret, at intervallet for backup er implementeret samt at der er udført restore test i erklæringsperioden.	
A.12.4.1 Hændelseslogning ▶ Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser skal udføres, opbevares og gennemgås regelmæssigt	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for logning, monitorering og alarmering og observeret, at der skal være hændelseslogning af brugeraktivitet, undertegnelser, fejl og informationssikkerhedshændelser. Loggen skal opbevares og gennemgås regelmæssigt. Vi har inspiceret, at der er opsat hændelseslog for begge systemer. Vi har inspiceret, at der forefindes et dashbord over hændelser, som gennemgås af driftsorganisationen dagligt.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

Kontrolmål

- *At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.13.2.2 Aftaler om informationssikkerhedsoverførsel ▶ Der forefindes procedurer for sikker overførsel af forretningsinformation mellem organisationen og eksterne parter	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandøren procedure for leverandørsikkerhed og observeret, at der ved indgåelse af leverandøraftaler skal underskrives en erklæring om overholdelse af serviceleverandørens sikkerhedspolitik. Vi har inspiceret skabelonen for erklæringen. Vi har på forespørgsel fået oplyst, at der ikke er eller har været indgået aftaler med leverandører i erklæringsperioden. Vi har derfor ikke kunne teste for implementering af proceduren.	Ingen afvigelser konstateret.
A.13.2.4 Fortroligheds- og hemmeligholdelsesaftaler ▶ Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, gennemgås, regelmæssigt og dokumenteres	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for personalesikkerhed og observeret, at nye medarbejdere ved ansættelse skal underskrive erklæring om overholdelse af serviceleverandørens sikkerhedspolitik. Vi har stikprøvevist inspiceret, at medarbejdere har underskrevet erklæringen. Vi har yderligere inspiceret, at serviceleverandørens skabelon for ansættelseskontrakter indeholder krav om fortrolighed. Vi har stikprøvevist inspiceret, at der indgår krav om fortrolighed i ansættelseskontrakter.	Ingen afvigelser konstateret.

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer		
Kontrolmål ▶ *At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus* ▶ *At sikre beskyttelse af data, som anvendes til test*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
A.14.2.2 Procedurer for styring af systemændringer ▶ Ændringer af systemer inden for udviklingslivscyklussen skal styres ved hjælp af formelle procedurer for ændringsstyring	Vi har udført forespørgsler hos relevant personale. VI har inspiceret serviceleverandørens procedure for udvikling og observeret, at ændringer af systemer inden for udviklingslivscyklussen skal styres ved hjælp af formelle procedurer for ændringsstyring. Vi har inspiceret, at proceduren er implementeret, således at ændringer af systemer styres gennem godkendt proces.	Ingen afvigelser konstateret.
A.14.2.3 Teknisk gennemgang af applikationer efter ændringer af driftsplatforme ▶ Ved ændring af driftsplatforme skal forretningskritiske applikationer gennemgås og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for udvikling og observeret, at alle ændringer først skal godkendes af en anden udvikler og så af den opgave ansvarlige. Vi har stikprøvevist inspiceret, at ændringer godkendes efter proceduren.	Ingen afvigelser konstateret.
A.14.2.6 Sikkert udviklingsmiljø ▶ Der er udviklet sikre udviklingsmiljøer for systemudvikling	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandøren bruger Jira cloud til systemudvikling.	Ingen afvigelser konstateret.
A.14.2.8 Systemsikkerhedstest ▶ Test af sikkerhedsfunktionalitet skal udføres ved udvikling	Vi har udført forespørgsler hos relevant personale.	Ingen afvigelser konstateret.

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

Kontrolmål

- *At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus*
- *At sikre beskyttelse af data, som anvendes til test*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret serviceleverandørens procedure for udvikling og observeret, at der ved ændringer skal foretages regresionstest med henblik på at disse ikke har negative indvirker på organisationens drift eller sikkerhed. Vi har stikprøvevist inspiceret, at der er foretaget regresionstest ved ændringer.	
A.14.3.1 Sikring af testdata - Der er implementeret en fast procedure for beskyttelse af testdata	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at serviceleverandøren benytter sig af fabrikeret testdata i testmiljøet.	Ingen afvigelser konstateret.

A.15 Leverandørforhold

Kontrolmål

- *At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.15.1.1 Informationssikkerhedspolitik for leverandørforhold ▶ Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørernes adgang til organisationens aktiver skal aftales med leverandøren og skal dokumenteres	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandøren procedure for leverandørsikkerhed og observeret, at der ved indgåelse af leverandøraftaler skal underskrives en erklæring om overholdelse af serviceleverandørens sikkerhedspolitik. Vi har inspiceret skabelonen for erklæringen. Vi har på forespørgsel fået oplyst, at der ikke er eller har været indgået aftaler med leverandører i erklæringsperioden. Det har derfor ikke været muligt at teste for implementering af proceduren. Vi har inspiceret, at serviceleverandøren har indhentet og gennemgået SOC 2 rapport og tilhørende bridge letters samt ISO-certificering fra Microsoft vedr. deres overholdelse af sikkerhedskravene.	Ingen afvigelser konstateret.
A.15.1.2 Håndtering af sikkerhed i leverandøraftaler ▶ Alle relevante informationssikkerhedskrav skal fastlægges og aftales sammen med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens information	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandøren procedure for leverandørsikkerhed og observeret, at der ved indgåelse af leverandøraftaler skal underskrives en erklæring om overholdelse af serviceleverandørens sikkerhedspolitik. Vi har inspiceret skabelonen for erklæringen. Vi har på forespørgsel fået oplyst, at der ikke er eller har været indgået aftaler med leverandører i erklæringsperioden. Det har derfor ikke været muligt at teste for implementering af proceduren. Vi har inspiceret, at serviceleverandøren har indhentet og gennemgået SOC 2 rapport og tilhørende bridge letters samt ISO-certificering fra Microsoft vedr. deres overholdelse af sikkerhedskravene.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud		
Kontrolmål ▶ *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
A.16.1.1 Ansvar og procedurer ▶ Ledelsesansvar og procedurer skal fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for sikkerhedsbrud og observeret, at der her er besluttet hvordan processen for et sikkerhedsbrud er samt ansvarsfordelingen.	Ingen afvigelser konstateret.
A.16.1.2 Rapportering af informationssikkerhedshændelser ▶ Informationssikkerhedshændelser bliver rapporteret til ledelsen	Vi har udført forespørgsler hos relevant personale. Vi har på forespørgsel fået oplyst, at serviceleverandøren ikke har haft sikkerhedsbrud i erklæringsperioden. Vi har derfor ikke kunne teste om informationssikkerhedshændelser bliver rapporteret til ledelsen.	Ingen afvigelser konstateret.
A.16.1.5 Håndtering af informationssikkerhedsbrud ▶ Der er dokumenterede procedurer ved nedbrud	Vi har udført forespørgsler hos relevant personale. Vi har på forespørgsel fået oplyst, at serviceleverandøren ikke har haft sikkerhedsbrud i erklæringsperioden VI har yderligere fået oplyst, at der én gang har været mistanke om sikkerhedsbrud, men det blev vurderet af ledelsen, at der ikke var tale om et sikkerhedsbrud. Vi har inspiceret, at serviceleverandøren har registeret og behandlet og vurderet hændelsen.	Ingen afvigelser konstateret.
A.16.1.6 Erfaringer for informationssikkerhedsbrud ▶ Erfaring fra tidligere informationssikkerhedsbrud anvendes til fremtidig læring	Vi har udført forespørgsler hos relevant personale. Vi har på forespørgsel fået oplyst, at serviceleverandøren ikke har haft sikkerhedsbrud i erklæringsperioden.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud		
Kontrolmål ▶ *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
A.16.1.7 Indsamling af beviser ▶ Der indsamles beviser for informationssikkerhedsbrud	Vi har udført forespørgsler hos relevant personale. Vi har på forespørgsel fået oplyst, at serviceleverandøren ikke har haft sikkerhedsbrud i erklæringsperioden.	Ingen afvigelser konstateret.

A.18 Overensstemmelse

Kontrolmål

- *At imødegå overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav*
- *At sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.18.1.1 Identifikation af gældende lovgivning og kontraktkrav ▶ Alle relevante lov-, myndigheds- og kontraktkrav samt organisationens metode til overholdelse af disse krav skal være klart identificeret, dokumenteret og opdateret for hvert informationssystem og for organisationen	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for overensstemmelse med lov- og kontraktkrav og observeret at en gang om året anmoder serviceleverandørens direktion advokatvirksomheden Bech-Bruun om at vurdere, om det er sket ændringer i ovenstående lovgivning på en måde, så der skal ændres i sikkerhedspolitikken og/eller i systemet. Vi har inspiceret, at advokatvirksomheden Bech-Bruun d. 27. august har gennemgået og bekræftet, at serviceleverandørens procedurer og politikker er i overensstemmelse med gældende lovgivning. Vi har inspiceret, at serviceleverandørens ledelse har gennemgået Bech-Bruuns gennemgang.	Ingen afvigelser konstateret.
A.18.1.4 Privatlivets fred og beskyttelse af personoplysninger ▶ Personoplysninger skal beskyttelses i overensstemmelse med relevant lovgivning og eventuelle forskrifter.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at advokatvirksomheden Bech-Bruun i august 2021 har gennemgået og bekræftet, at serviceleverandørens procedurer og politikker er i overensstemmelse med gældende lovgivning.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

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."

Mikkel Jon Larssen
Partner
Serienummer: CVR:20222670-RID:52744874
IP: 77.243.xxx.xxx
2021-09-30 08:09:03 UTC
NEM ID

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2021-09-30 08:28:50 UTC
NEM ID

Brian Østberg
Managing Director
Serienummer: PID:9208-2002-2-483421471339
IP: 195.249.xxx.xxx
2021-10-01 11:30:36 UTC
NEM ID