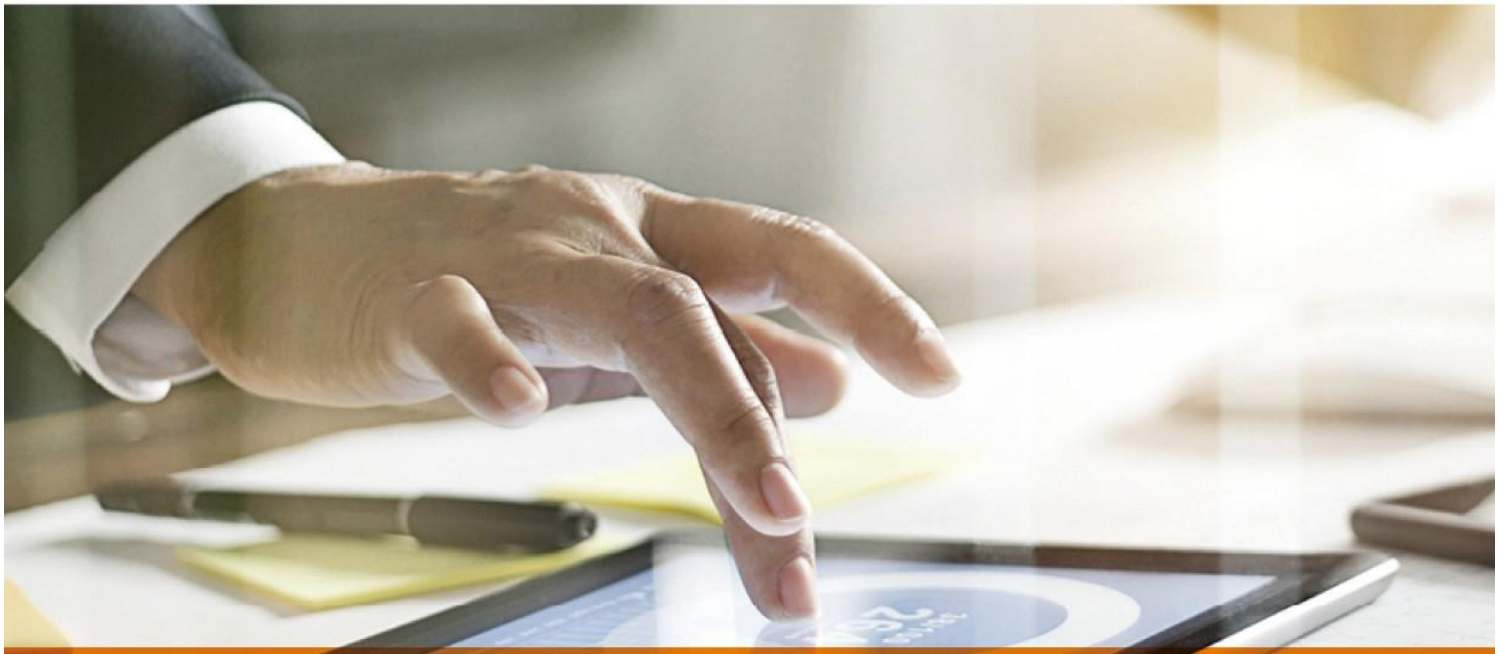
BEIERHOLM
VI SKABER BALANCE



Juni 2023

Ajour System A/S

ISAE 3402 TYPE 2 ERKLÆRING

CVR 84667811

Revisors erklæring vedrørende afdækning af de tekniske og organisatoriske sikringsforanstaltninger i tilknytning til Ajour System A/S' SaaS-løsninger.

Herudover er der tilføjet et afsnit i kontrolbeskrivelse i forhold til rollen som databehandler i henhold til Databeskyttelsesforordningen.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Beskrivelse af kontrolmiljøet i tilknytning til udvikling og drift af Ajour System A/S' SaaS-løsninger.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet.

Kapitel 4:
Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf.

KAPITEL 1:

Ledelseserklæring

Ajour System A/S behandler personoplysninger på vegne af kunder i henhold til databehandleraftale om Ajour System A/S' SaaS-løsninger.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Ajour System A/S' SaaS-løsninger, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene til kontrolmiljøet samt databeskyttelsesforordningen er overholdt.

Ajour System A/S bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af Ajour System A/S' kontrolmiljø i tilknytning til driften af Ajour System A/S' SaaS-løsninger i hele perioden 1. april 2022 - 31. marts 2023. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne var udformet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
- De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
- De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
- De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
- De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
- De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
- De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
- Kontroller, som vi med henvisning til Ajour System A/S' SaaS-løsningers afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Indeholder relevante oplysninger om ændringer i Ajour System A/S' SaaS-løsninger til behandling af personoplysninger foretaget i perioden 1. april 2022 - 31. marts 2023

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller 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 kontroller, som den enkelte kunde måtte anse som vigtig efter deres særlige forhold.

(B) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. april 2022 - 31. marts 2023. Kriterierne for dette udsagn er, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. april 2022 - 31. marts 2023.

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

(D) Den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2, er udarbejdet med baggrund i overholdelse af Ajour System A/S' standardaftale samt tilhørende databehandleraftale, grundlaget for SaaS-løsninger og ydelser omkring de tekniske og organisatoriske sikringsforanstaltninger. Kriterierne for dette grundlag var:

(i) Ajour System A/S – Informationssikkerhedspolitikker
(ii) Ajour System A/S – Databehandleraftale

Odense, den 29. juni 2023

Senior Vice President , Aleksander Bjaaland
Ajour System A/S, Østerbro 5B st. th., DK-5000 Odense C, CVR-nr.: 84667811

KAPITEL 2:

Beskrivelse af kontrolmiljøet i tilknytning til udvikling og drift af Ajour System SaaS-løsninger

Indledning

Denne beskrivelse er udarbejdet for kunder, der har modtaget professionelle ydelser leveret af Ajour System A/S.

Rammen for nærværende beskrivelse er at levere information om Ajour systemet til kunder og deres revisorer vedrørende kravene i ISAE 3402 som er den internationale revisorstandard for erklæringsopgaver.

Denne kontrolbeskrivelse afdækker de tekniske og organisatoriske sikkerhedsforanstaltninger, som der implementeret i tilknytningen til driften af Ajour systemet.

Beskrivelse af Ajour System A/S

Ajour System A/S er en af landets førende softwareleverandører til bygge- & ejendomsbranchen, og vi udvikler og sælger brugervenlige digitale værktøjer og BIM-løsninger udviklet i samarbejde med brancheeksperter og baseret på den nyeste teknologi.

Vi bringer byggeriets parter sammen om at levere kvalitet, bæredygtigt med færre ressourcer, smidige processer og vores platform bruges dagligt af mere end 40.000 brugere i flere lande.
Ajour System A/S udvikler SaaS løsningerne AjourBuild og AjourCollab.

AjourBuild er software til anvendelse i forbindelse med kvalitetssikring i byggerier, vedligeholdelse af bygninger, udbud og projektweb. AjourBuild produktet indbefatter også en app der kan anvendes på iOS og Android enheder.

AjourCollab software anvendes til opsamling og redigering af data fra BIM-modeller. Dette produkt indbefatter udover SaaS løsningen også plugin til Revit.

Ajour System A/S har indtil 1. april 2022 været en dansk privatejet virksomhed. Ajour System A/S er opkøbt af EG A/S og bliver pr. 1. april 2023 fuldt ud sammenkørt med EG A/S.

Forretningsstrategi/ it-sikkerhedsstrategi

Det er Ajour System A/S´ strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, således at selskabet ikke påføres uacceptable risici. Som leverandør til private og offentlige virksomheder, arbejder Ajour System A/S med informationssikkerhed på et forretningsstrategisk niveau. Målsætningen er at være en professionel produktleverandør, der har en skarp holdning til at passe på de data, kunderne betror os.

Det er Ajour System A/S´ holdning, altid at sikre overholdelse af gældende lovgivning og gøre, hvad der er teknisk og økonomisk muligt, for at sikre databehandlingens fortrolighed, integritet og tilgængelighed på et højt niveau.

Informationssikkerheden er i højsædet på alle niveauer af organisationen. Alle medarbejdere skal være vidende om vigtigheden af dette fokus og selv være medvirkende til løbende at forbedre arbejdet omkring sikkerhed.

Ajour System A/S´ målsætning for informationssikkerheden er, at Ajour System A/S gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed** af Ajour systemet: At opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud.
- **Integritet**: At opnå en pålidelig og korrekt funktion af Ajour systemet og minimeret risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.
- **Fortrolighed**: At sikre fortrolig databehandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang.

Det er Ajour System A/S´ mål at opretholde et informationssikkerhedsniveau, der som minimum:

- Følger gældende lovgivning
- Følger god brancheskik
- Lever op til kundens ønsker, krav og forventninger til en professionel leverandør

Databeskyttelsesforordningen (GDPR) udgør den lovgivningsmæssige ramme for behandling af persondata i SaaS-løsninger, som indgås mellem kunden (dataansvarlige) og Ajour System A/S (databehandler). Ajour System A/S´ ansvar er at foretage de nødvendige tekniske og organisatoriske sikringsforanstaltninger, der sikrer, at personoplysninger behandles på en sikker og forsvarlig måde.

For at sikre en ensartet leverance, som lever op til branchens bedste standarder, har Ajour System A/S valgt at underlægge driften af Ajour systemet en revisionsproces med det formål at leve op til kravene i en ISAE3402 erklæring. Revisionsprocessen gentages årligt, og resulterer i en revisionserklæring.

Erklæringen kan bidrage til kundens (dataejerens) kontrol af, hvorvidt Ajour System A/S lever op til instruksen i den indgåede databehandleraftale.

Ajour System A/S har omkring it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27001 og 2, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse (lovgivning)

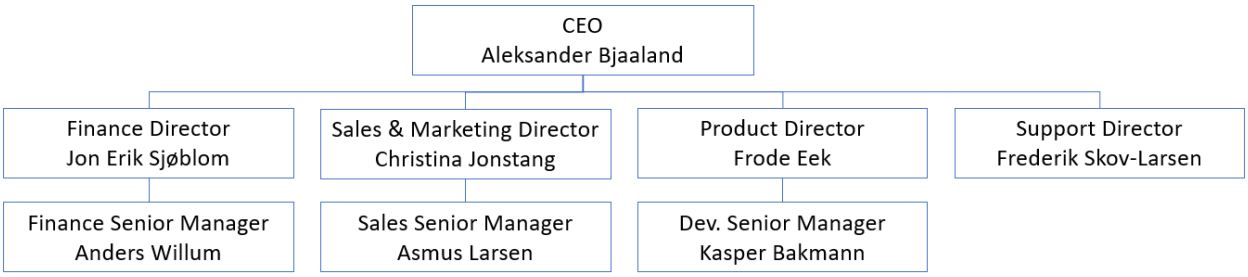
Rammen for hvilke kontrolmål og underliggende kontrolpunkter (sikkerhedselementer), som Ajour System A/S´ ledelse har defineret relevant for arbejdet med et passende sikkerhedsmiljø er nærmere beskrevet i bilag 1.

Omfang for denne beskrivelse

I det følgende beskrives Ajour System A/S' services, som er omfattet af de generelle it-kontroller som denne erklæring omhandler. Erklæringen omfatter generelle processer og system setup m.v. hos Ajour System A/S.

Kontroller i applikationssystemerne er ikke omfattet af denne erklæring.

Ajour System A/S' organisation og organisering af it-sikkerheden



Risikostyring i Ajour System A/S

For at kunne fokusere indsatsen af it-sikkerhedsarbejdet hos Ajour System A/S, arbejdes der efter en struktureret tilgang til risikostyring. Resultatet af risikostyringen, herunder vurdering af risici foretages i Ajour System A/S´ ledelse.

Ledelsen orienteres desuden straks om væsentlige afvigelser i det aktuelle trusselsbillede og den tilpasning, som dette afleder i forhold til indsatsområderne og kontrollerne. Mindre afvigelser opsamles og rapporteres periodisk over for Ajour System A/S´ direktion, og indgår tillige i den årlige rapportering.

Håndtering af it-sikkerhed

For at sikre en funktionsadskillelse og forankringer af ansvar omkring it-sikkerheden i Ajour er de primære roller og ansvar for informationssikkerheden beskrevet herunder.

Direktionens ansvar

Direktionen har det overordnede ansvar for it-sikkerheden i Ajour. Hermed følger også ansvaret for, at:

- Der stilles de fornødne rammer og ressourcer til rådighed for at opnå det ønskede it-sikkerhedsniveau
- Det sikres, at en relevant it-sikkerhedspolitik er implementeret
- Der drages nødvendige konsekvenser ved væsentlige sikkerhedsbrud.

Den daglige ledelses ansvar

Ledelsen sikrer, at it-sikkerhedspolitikken efterleves. Herunder at:

- Sikre, at it-sikkerhedspolitikken overholdes og er tilstrækkeligt implementeret gennem forretningsgange, procedurer og retningslinjer
- Skabe fælles organisatorisk forståelse for, at it-sikkerhed er et fælles ansvar, og at retningslinjer, forretningsgange mv. gælder for alle parter internt som eksternt
- Sikre, at roller og ansvar er beskrevet og tildelt både internt i Ajour og over for samarbejdspartnere og leverandører
- Iværksætte it-sikkerhedsinitiativer
- Udarbejde afvigelsesrapporter til direktionen.

Databeskyttelsesansvarlig

Der er ikke udnævnt en DPO (Databeskyttelsesansvarlige) i Ajour System A/S, da Ajour System A/S ikke behandler personoplysninger som en kerneaktivitet og ikke behandler personoplysninger i stort omfang. Denne beslutning er truffet ud fra Datatilsynets "Vejledning om databeskyttelsesrådgivere" afsnit 3.1, dateret december 2017.

IT-sikkerhedsansvarlig
Development Senior Manager har det it-sikkerhedsmæssige ansvar, og er derfor også den IT-sikkerhedsansvarlige, samt det daglige og operationelle ansvar for it-sikkerheden, herunder:

- Det kontinuerlige arbejde med og videreudvikling af it-sikkerhedsniveauet hos Ajour, så det er i overensstemmelse med kravene i it-sikkerhedspolitikken. Dette omfatter alle tilhørende forretningsgange og retningslinjer samt overensstemmelse med gældende lovgivning.
- At sikre, at leverandører efterlever de stillede krav i outsourcing-aftaler, herunder at aftalegrundlag med leverandører er i overensstemmelse med it-sikkerhedspolitikken for så vidt angår kontrol, opfølgning og rapportering
- Monitorere og rapportere på eventuelle it-sikkerhedsmæssige hændelser i overensstemmelse med denne it-sikkerhedspolitiks fastsatte regelsæt.
- At iværksætte egne undersøgelser eller tests i det omfang, der vurderes behov herfor.
- Varetagelse af en overordnet it-sikkerhedskoordinator rolle.
- At fungere som kontaktperson til den eksterne revision i forbindelse med it-revision.
- At fungere som kontaktpunkt i forhold til de registrerede, samarbejdspartnere og tilsynsmyndighed. Herunder at anmelde brud på persondatasikkerheden til tilsynsmyndigheden.
- Sikre at databeskyttelsesforordningens bestemmelser efterleves i Ajour System A/S, herunder føre kontrol med organisationens efterlevelse af databeskyttelsesreglerne og relevant dokumentation der understøtter dette.
- Deltage i, og udarbejde materiale til uddannelses- og awareness aktiviteter for organisationen.
- Være organisationens interne kontaktpunkt I forhold til vejledning og rådgivning.

Styring af aktiver
Ajour System A/S holder styr på aktiver ved at have en proces for udlevering og aflevering af udstyr til og fra medarbejdere. Derudover har Ajour System A/S klare anvisninger på hvordan usb-nøgler må anvendes og hvordan udgået IT-udstyr skal bortskaffes.

De immaterielle aktiver styres ved hjælp af liste over aktiver. I listen dokumenteres følgende:

- Ajour kategorisering
- Informationsarkiv
- Beskrivelse
- Hjemmel
- Type af information
- Data klassifikation
- Kommentarer
- Ejer
- Ajour ansvarlig
- Leverandørkontakt

Listen vedligeholdes af den IT-sikkerhedsansvarlige og ledelsen i Ajour System A/S.

Medarbejdere og uddannelse
Medarbejderne er den vigtigste udviklings- og driftsressource for Ajour System A/S, men udgør samtidigt også en risiko i forhold til informationssikkerheden. Fokus på efterlevelse af it-sikkerhedspolitikken og udarbejdelse af relevante medarbejderinstrukser for de enkelte områder er derfor afgørende for sikkerhedsniveauet i Ajour System A/S.

Enhver medarbejder bør opfatte sig selv som it-sikkerheds ambassadør. Medarbejderne har et medansvar for it-sikkerheden og er forpligtet til at efterleve de regler, der er fastlagt af it-sikkerhedspolitikken med tilhørende forretningsgange, retningslinjer, procedurer mv.

På baggrund af en konkret vurdering i hvert enkelt tilfælde kan overtrædelser blive anset som en misligholdelse af ansættelsesforholdet.

Medarbejdernes domæneviden og kompetencer er en vigtig forudsætning for Ajour System A/S´ forretning. Ajour System A/S arbejder med løbende erfaringsudveksling og uddannelse ud fra den enkelte medarbejders behov, således at medarbejdernes faglige udvikling understøttes.

Nye medarbejdere gennemgår et grundigt introduktionsforløb til virksomheden. Forløbet omfatter information i informationssikkerhed, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd, dataklassifikation og særligt fokus på Ajour System A/S´ rolle som databehandler.

Ajour System A/S´ medarbejdere har i begrænset omfang mulighed for at arbejde fra andre faciliteter end kontorerne i Odense, København, Reykjavik, Malmø og Wroclaw. Virksomheden har udarbejdet en procedure, der beskriver regler og gode råd til fjernarbejdsplads. Ajour System A/S har har etableret tekniske foranstaltninger, der sikrer en krypteret opkobling til kontorfaciliteter. Adgang til backend-systemer og driftsmiljøer er teknisk begrænset.

Alle medarbejdere har en fortrolighedsklausul i deres ansættelseskontrakter. Som en del af vores fratrædelsesprocedure indgår en exit-samtale med nærmeste leder, hvor vi minder om, at fortrolighedsklausulen fortsat er gældende efter endt ansættelse.

For at sikre en kontinuerlig tilgang til informationssikkerhedskulturen har Ajour System A/S et årligt IT-Sikkerhed informationsmøde. Informationen revurderes årligt af informationssikkerhedsorganisationen.

Brugerstyring/ adgangssikkerhed

Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne.

Tildeling af adgang til driftsmiljø skal ske i overensstemmelse med forretningsbetingede formål og informationernes klassifikation. Både fysisk og logisk adgang er baseret på principperne "need-to-know" og ”least privillege”, hvor der tildeles adgang til de informationer, som man har behov for, for at kunne udføre sine opgaver/sit job eller rolle.

Anmodning om adgang til interne it-systemer og produktionsmiljøer følger en fastlagt procedure, der sikrer en adskillelse i anmodning, godkendelse, verifikation og implementering.

Fysisk sikkerhed

Ajour System A/S gør brug af 2 eksterne leverandører som hostingleverandører: EnergiFyn og Microsoft Azure til interne servere og Ajour systemet. Det betyder, at Ajour System A/S har overladt de grundlæggende datacenteropgaver til leverandøren, der har erfaring med opbygning og drift af datacentre.

EnergiFyn er ansvarlig for fysisk sikring, brand-, og vanddetektion og -bekæmpelse, strøm og køling. Hostingleverandørernes datacenter giver flere lag sikkerhed og opfylder anerkendte internationale standarder for informationssikkerhed vedr. managementsystemer og business continuity management.

Pr. 3. december 2022 er al hosting flyttet til Team Blue, som varetager al drift af infrastruktur. EG CloudOps varetager driften af software services.
Hostingleverandørernes datacenter giver flere lag sikkerhed og opfylder anerkendte internationale standarder for informationssikkerhed vedr. managementsystemer og business continuity management.

Drift af Ajour systemet

Faste driftsopgaver udføres med faste intervaller. Disse opgaver styres i Ajour System A/S af DevOps teamet og i samarbejde med EG CloudOps.

Malwarebeskyttelse

For at sikre at Ajour System ikke bliver angrebet af malware er der gjort følgende tiltag:
Medarbejdere er undervist i hvordan de skal opdage og håndtere mistænkelige henvendelser. Det være sig både telefonisk og pr. email.

Alle kontor bærbare anvender antivirus software, der er sat til automatisk at opdatere og hente nye definitioner.

Backup

Formålet med backup er at sikre, at kundens data i Ajour systemet kan genskabes nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid. Backup af Ajour systemet sendes til en ekstern partner. Den eksterne partner er ansvarlig for, at selve backup-servicen er kørende. Ajour System A/S overvåger om backup er kørt korrekt.

Backuppolitik
Med Ajour System A/S' databackup sikres data ud fra en aftalt sikringspolitik.
Nedenstående politikker er gældende som standard. Standard kan ændres af Ajour System A/S eller af kunden selv, hvis kunden har administrative rettigheder til den pågældende server. Den aktuelt gældende politik kan ses i serverens konfigurationsfil.

Al vital data for videreførsel af Ajour systemet tages der backup af. Dette indbefatter filer, SQL-databaser, EventStore noder. Derudover tages der backup af interne servere.

Kryptering af data
Ved at kryptere data bliver disse ulæselige for alle andre end dem, som kender krypteringsnøglen. Ajour System A/S krypterer også de data, som opbevares i Ajour System A/S databackup.

Logning og overvågning

Ajour System A/S har etableret automatisk overvågning af servere, storagesystemer, netværk, m.v.

Hvis en fejl konstateres, afsendes alarm både visuelt på en overvågningsskærm og på SMS. Opstår en situation, hvor der konstateres en fejl på en komponent, der ikke er en del den automatiske overvågning, tages der skridt til, at den fremover registreres i systemet. Hostingcentret overvåges med hensyn til strømafbrydelser, temperatur, brand, vand og hele hostingcenteret er i øvrigt kameraovervåget.

Hvis der sker hændelser, som kan påvirke driften, vil overvågningssystemet automatisk alarmere vagtberedskabet, og der forefindes en indarbejdet procedure for eskalation sluttende med, at den adm. direktør involveres.

Listen over personer med adgang til Ajour systemet revideres løbende jvf. procedure herfor.

Kommunikationssikkerhed

Ved opdaget unormal aktivitet vil DevOps teamet i samarbejde med EG CloudOps teamet, analysere trafik på netværket og FW trafik og i samråd med den IT-sikkerhedsansvarlige vurdere om der er behov for indgreb i netværket.

Adgang til trådløse netværk for gæster
Gæster, hvis identitet er kendt, må få udleveret adgangskode til Ajour System A/S´ gæste WiFi, og anvende eget udstyr til det.

Tilslutning af udstyr til netværk
Det er tilladt, at ansatte kobler udstyr til netværket efter aftale med den IT-ansvarlige. Udstyret må ikke forstyrre driften, og den IT-ansvarlige kan kræve det frakoblet

Opdeling af netværk
Ajour System A/S har opdelt det fysiske netværk i to subnets. Et subnet for produktionsmiljø (Production), det vil sige hvor Ajour System A/S´ egenudviklede software driftes. Og et subnet for kontormiljøet (Office), det vil sige hvor medarbejdere i Ajour System A/S kan tilgå fællesdrev og internet. Derudover er der et subnet til administration (Administration) og VPN adgang (VPN).

Udviklingsmiljøet
Ajour System A/S anvender et udviklingsmiljø der er adskilt fra produktionsmiljøet.

For at sikre at der ikke opstår bagdøre i Ajour systemet, der kan udnyttes uretmæssigt, støttes udviklingsprocessen ved undervisning af udviklere i sikker udvikling.

Udviklingsprocessen holdes op mod ti største udfordringer defineret af OWASP (https://owasp.org/www-project-top-ten/). Det indebærer at når der ny udvikles eller ændres i eksisterende software, vurderes de principper der findes i OWASP i forhold til ændringen. Medarbejdere der udvikler software i Ajour System A/S undervises hver 6. måned i sikker udvikling.

Leverandørstyring
Som leverandør til kritiske dele af driftsmiljøet, fører Ajour System A/S årligt kontrol med, om hostingleverandørerne lever op til krav og SLA for deres ydelser. Ajour System A/S evaluerer leverandørens certificeringer og sammenholder dem med egne observationer. Herefter vurderer Ajour System A/S, om leverandøren lever op til de aftalte serviceydelser, og hvorvidt der er grund til at tage aspekter op med dem.

Leverandører til Ajour System A/S, bør altid følge følgende politikker:

- Overholder GDPR og andre lovkrav
- Har implementeret ISAE 3402 eller lignende standard for IT-sikkerhed

Styring af it-sikkerhedshændelser
Sikkerhedshændelser og svagheder i Ajour System A/S systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Alle medarbejdere i Ajour System A/S er bekendt med procedurerapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af Ajour System A/S drift. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til ledelsen.

Ledelsen har ansvaret for at definere og koordinere en struktureret proces, der sikrer en passende reaktion på sikkerhedshændelser.

Beredskabsstyring
Ajour System A/S´ ledelse har det overordnede ansvar for håndtering af sikkerhedsbrud. Den IT-sikkerhedsansvarlige har ansvar for at fastlægge procedurer, der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

Alle medarbejdere i Ajour System A/S har ansvar for at rapportere informationssikkerhedsbrud. Medarbejderne skal instrueres om, at alle har ansvar for at reagere ved tegn på sikkerhedstruende eller tabsgivende hændelser

Overensstemmelse, med rollen som databehandler

Det er ledergruppen hos Ajour System A/S der er ansvarlig for at sikre, at alle relevante juridiske og kontraktuelle krav er identificeret og korrekt overholdt. Relevante krav omfatter blandt andet:

- Databeskyttelsesforordningen (GDPR)
- Databeskyttelsesloven
- Databehandleraftaler

Desuden gennemgår ledergruppen regelmæssigt alle Ajour System A/S´ sikkerhedspolitikker.

EU Databeskyttelsesforordningen (GDPR)
Ajour System A/S´ SaaS-løsninger understøtter kundernes arbejdsprocesser. Ajour System A/S ejer ikke de data, kunderne indsamler, men udvikler og driver de SaaS-løsninger, som kunderne anvender til at udføre den nødvendige persondatabehandling. Ifølge Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er Ajour System A/S databehandler, og kunden er dataansvarlig.

Ajour System A/S har sørget for at have relevante kontrakter med alle nøgleinteressenter (herunder kunder, samarbejdspartnere, nøgleleverandører osv.) med henblik på at sikre overholdelse af loven. Desuden samarbejder Ajour System A/S med sine kunder om at sikre, at kunderne er bekendt med og overholder de relevante GDPR-regler.

Privatliv og beskyttelse af personoplysninger
Som nævnt er Ajour System A/S databehandler for sine kunder, i og med at kunderne tilbydes en it-service, hvortil der overføres og behandles data, der kan indeholde personoplysninger. Ajour System A/S er ikke ansvarlig for data, som kunderne producerer med Ajour System A/S software. Med udgangspunkt i kategorier og fortrolighed af de typer af data, kunden overlader til behandling, skal Ajour System A/S iværksætte alle nødvendige sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

Nedenfor beskrives Ajour System A/S´ procedurer for, hvordan man opererer som databehandler under instrukser fra de dataansvarlige.

Databehandleraftaler
Ajour System A/S indgår databehandleraftaler med alle sine kunder. Databehandleraftalen er en fastlagt procedure ved kontraktindgåelse, og der benyttes Ajour System A/S´ egen skabelon. Aftalerne beskriver roller og ansvar for så vidt angår rolle som databehandler og dataansvarlig.

Som databehandler pålægges Ajour System A/S et særligt ansvar defineret i Databeskyttelsesforordningen, dette omfatter blandt andet kravet om at:

- Føre fortegnelse over, hvilke kategorier af persondata der behandles i de respektive SaaS-løsninger.
- Beskrive de tekniske og organisatoriske sikkerhedsforanstaltninger, som er iværksat med henblik på at værne om persondata.
- Bidrage til at opfylde kundens forpligtelser vedr. den registreredes rettigheder (jf. kapitel 3 i EU Persondataforordningen).

- Stille ekspertise til rådighed for kunden for at sikre efterlevelse af Artikel 32 – 34.
  - Artikel 32 – Behandlingssikkerhed
  - Artikel 33 – Anmeldelse af brud på persondatasikkerheden
  - Artikel 34 – Underretning om brud på persondatasikkerheden for de registrerede
- Iagttage kundens krav vedr. overførsel af persondata uden for EØS.
- Registrere navn og kontaktinformation på leverandører, der er underdatabehandlere.
- Sikre, at krav vedr. persondatabehandling fra kunden matcher krav til en underdatabehandler.

Formålsbestemthed og hjemmel
Som databehandler arbejder Ajour System A/S med persondata på baggrund af instrukser fra kunderne, der beskriver en formålsafgrænsning for, hvad data må benyttes til.

Den dataansvarlige er ansvarlig for at sikre, at der er hjemmel til behandling af de omfattede personoplysninger.

Adgang til kundedata
Ajour System A/S tilbyder løsninger som *Software as a Service*, der driftes af Ajour System A/S´ DevOps team. Udvikling, test og release varetages af egen udviklingsafdeling eller relevante underleverandører. DevOps afdelingen påtager sig dermed det fulde ansvar for behandling af kunders data. Generelt har medarbejdere alene adgang til kundedata, såfremt deres specifikke arbejdsopgaver taler herfor.

Ajour System A/S har indført principper for medarbejderes adgang til og arbejde med kunders data:
- Der er kun adgang til kundedata, når man har et arbejdsbetinget behov.
- Omfattende introduktionsforløb med fokus på regler for omgang med kundedata og opfølgning via awarenes-kampagner

Væsentlige ændringer i forhold til it-sikkerhed
Ajour System A/S fører hændelseslog, der dokumenterer ændringer i hardware, software og andre hændelser i produktionsmiljøet. Ligeledes hvis der opstår en uregelmæssighed i driften dokumenteres det i hændelsesloggen.

Kundernes ansvar (komplementerende kontroller hos kunderne)
Dette kapitel beskriver den generelle ramme for Ajour System A/S´ services, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Ansvaret for de forretningssystemer og brugersystemer, som drives via Ajour System A/S´ løsning er kundernes eget. Kunderne har ansvaret for at sikre de nødvendige kontroller i forbindelse med systemudvikling, anskaffelse og ændringshåndtering.

Kunderne er ansvarlige for datatransmission til Ajour System A/S. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Ajour System A/S´ beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af Ajour System A/S´ løsninger.

Væsentlige ændringer i kontrolperioden
Ajour System A/S blev opkøbt af EG A/S pr. 1. april 2022. Ajour System A/S er fortsat en særskilt juridisk enhed med eget CVR nr.

Ajour System A/S flyttede kontoradresse fra Sanderumvej 16B, 5250 Odense SV til Østerbro 5B, 5000 Odense C den 13. juni 2022. Lejekontrakten på kontorlokalerne på Sanderumvej blev opsagt pr. denne dato.

Ajour System A/S har derefter haft lejekontrakt på serverrum og et kontor.

Serverummet på Sanderumvej 16B, blev migreret til hosting miljø hos EG A/S (Team Blue) den 3. december 2022. Udstyret i serverrummet på Sanderumvej, blev bortskaffet den 15. december 2022. Og lejekontrakt på serverrum og kontor blev opsagt den 19. december 2022.

BILAG 1:

Ajour System A/S har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27002:2017

5. Informationssikkerhedspolitik

5.1. Retningslinjer for styring af informationssikkerhed

6. Organisering af informationssikkerhed

6.1. Intern organisering
6.2. Mobilt udstyr og fjernarbejdspladser

7. Medarbejdersikkerhed

7.1. Før ansættelse
7.2. Under ansættelsen
7.3. Ansættelsesforholds ophør eller ændring

8. Styring af aktiver

8.1. Ansvar for aktiver
8.2. Klassifikation af information
8.3. Mediehåndtering

9. Adgangsstyring

9.1. Forretningsmæssige krav til adgangsstyring
9.2. Administration af brugeradgang
9.3. Brugernes ansvar
9.4. Styring af system- og applikationsadgang

11. Fysisk sikkerhed og miljøsikring

Begrænset ansvar
11.1. Sikre områder
11.2. Udstyr

12. Driftssikkerhed

Begrænset ansvar
12.1. Driftsprocedurer og ansvarsområder
12.2. Malwarebeskyttelse
12.3. Backup
12.4. Logning og overvågning
12.5. Styring af driftssoftware
12.6. Sårbarhedsstyring
12.7. Overvejelser i forbindelse med audit af informationssystemer

13. Kommunikationssikkerhed

Begrænset ansvar
13.1. Styring af netværkssikkerhed
13.2. Informationsoverførsel

14. Anskaffelse, udvikling og vedligeholdelse af systemer

14.1. Sikkerhedskrav til informationssystemer
14.2. Sikkerhed i udviklings- og hjælpeprocesser
14.3. Testdata

15. Leverandørforhold

15.1. Informationssikkerhed i leverandørforhold
15.2. Styring af leverandørydelser

16. Styring af informationssikkerhedsbrud

16.1. Styring af informationssikkerhedsbrud og forbedringer

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

17.1. Informationssikkerhedskontinuitet
17.2. Redundans

18. Overensstemmelse

18.1. Overensstemmelse med lov- og kontraktkrav (GDPR)

** Begrænset ansvar **
Ansvaret for opfyldelse af kontrolmålet er delt mellem Ajour System A/S og underdatabehandlerne/leverandørerne.

Se beskrivelsen af kontroller i henhold til afdækning af risikoen, herunder også hvordan Ajour System A/S løbende overvåger driftssikkerheden hos underdatabehandlerne/leverandørerne.

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til kunder af Ajour System A/S' SaaS-løsninger og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Ajour System A/S' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af kontrolmiljøet i tilknytning til driften af Ajour System A/S' SaaS-løsninger jævnfør databehandleraftale med kunder, i hele perioden 1. april 2022 - 31. marts 2023, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. Erklæringen dækker ikke kontrol eller tilsyn med underleverandører i relation til Ajour System A/S' SaaS-løsninger. Disse underleverandører er nærmere oplistet i databehandleraftaler med kunderne.

Erklæringen behandler ikke kundespecifikke forhold. Desuden omfatter erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. kontrolbeskrivelsen kapitel 2, afsnittet om komplementerende kontroller.

Ajour System A/S' ansvar

Ajour System A/S er ansvarlig for udarbejdelsen af kontrolbeskrivelsen i kapitel 2 (inkl. bilag 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet er præsenteret; for leveringen af de ydelser beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

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

Vi er underlagt international standard om kvalitetsstyring, ISQM 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om Ajour System A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til 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 overholder etiske krav samt 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 beskrivelse, udformning og funktionalitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens 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 udformet eller ikke fungerer effektivt.

Vores handlinger har omfattet test af funktionaliteten 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 nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som Ajour System A/S har specificeret og beskrevet i kapitel 2 (inkl. bilag 1).

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

Begrænsninger i kontroller hos Ajour System A/S

Ajour System A/S' beskrivelse 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 vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på datasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er kriterier, der er beskrevet i kapitel 1 i ledelsens erklæring. Det er vores opfattelse,

a) at beskrivelsen af de af Ajour System A/S' ydelser og kontrolmiljø i tilknytning til driften af Ajour System A/S' SaaS-løsninger, således som de var udformet og implementeret i hele perioden 1. april 2022 - 31. marts 2023, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. april 2022 - 31. marts 2023, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. april 2022 - 31. marts 2023.

Beskrivelse af test kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt Ajour System A/S' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Søborg, den 13. juli 2023

Beierholm
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Allan Nielsen
Seniorkonsulent, IT-revision

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Vi har struktureret vores arbejde i overensstemmelse med ISAE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør. For hvert kontrolmål indleder vi med et kort resumé af kontrolmålet, som det er beskrevet i referencerammen ISO27002:2017.

Hvad angår periode har vi i vores test forholdt os til, om Ajour System A/S har levet op til kontrolmålene i perioden 1. april 2022 - 31. marts 2023.

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som Ajour System A/S jf. sin dokumentation har iværksat for at leve op til kravene.
- Anden kolonne viser, hvordan vi har valgt at teste, om det forholder sig som beskrevet.
- Tredje kolonne viser resultatet af vores test.

De udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design, implementering og operationelle effektivitet er foretaget ved metoderne beskrevet nedenfor.

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel til passende personale hos Ajour System A/S. Forespørgsler har omfattet, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

KONTROLMÅL - INDLEDNING:

Risikovurdering og – håndtering

Risikovurdering skal identificere og prioritere risici med udgangspunkt i driften af SaaS løsninger. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Gennem en risikovurdering er der sket identificering og prioritering af risici. Udgangspunkt for vurderingen er de i beskrivelsen definerede SaaS løsninger fra Ajour System. Resultatet bidrager til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.	Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen. Vi har kontrolleret, at der for Ajour System A/S' SaaS løsninger arbejdes med en løbende vurdering af den risiko, som opstår som følge af de forretningsmæssige forhold. Vi har kontrolleret, at risikovurderingen er forankret ned igennem virksomhedens organisation. Vi har kontrolleret, at der sker løbende behandling af virksomhedens risikobillede, og med dertil hørende løbende tilpasning af konsekvenser og sandsynlighed.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 5:

Informationssikkerhedspolitikker

Ledelsen skal udarbejde en informationssikkerhedspolitik, som bl.a. skal indeholde ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. Informationssikkerhedspolitikken vedligeholdes under hensyn til den aktuelle risikovurdering.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er en skriftlig strategi, som bl.a. indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. It-sikkerhedspolitikken og de tilhørende støttepolitikker er godkendt af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation. Politikken er tilgængelig for alle relevante medarbejdere. Politikken revurderes efter planlagte intervaller.	Vi har indhentet og revideret Ajour System A/S' seneste it-sikkerhedspolitik. Gennem revisionen har vi kontrolleret, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Samtidig har vi ved revisionen kontrolleret, at de underliggende støttepolitikker er implementeret. Vi har kontrolleret, at politikken er godkendt og underskrevet af virksomhedens ledelse, og at den er gjort tilgængelig for medarbejderne.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 6:

Organisering af informationssikkerhed

Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikkerhedsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret. It-sikkerheden er koordineret på tværs af virksomhedens organisatoriske rammer.	Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret. Vi har kontrolleret, at it-sikkerheden er forankret på tværs af organisationen i forhold til Ajour System A/S' SaaS løsninger. Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevis kontrolleret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos Ajour System A/S har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, således at området er afdækket i forhold til risikovurderingen for området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

Det skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Via fastlagte arbejdsprocesser og procedurer er det sikret, at alle nye medarbejdere får oplyst deres særlige ansvar og rolle i forbindelse med ansættelse i Ajour System A/S. Herunder de fastlagte rammer for deres arbejde og den omkringliggende it-sikkerhed. Eventuelle sikkerhedsansvar er fastlagt og nærmere beskrevet gennem stillingsbeskrivelse og i form af vilkår i ansættelseskontrakten. Medarbejderne er bekendte med deres tavshedspligt via en underskrevet ansættelseskontrakt og via Ajour System A/S' personalepolitik.	Vi har kontrolleret, at de af ledelsen udarbejdede forretningsgange og procedurer i forbindelse med ansættelse og ansættelsesophør er overholdt. Gennem stikprøver har vi testet, om ovenstående forretningsgange og procedurer er overholdt både i forhold til ansættelse og ansættelsesophør. Ved interview har vi kontrolleret, at væsentlige medarbejdere er bekendt med deres tavshedspligt. Gennem stikprøver på ansættelseskontrakter har vi kontrolleret, at Ajour System A/S' medarbejdere er bekendt med deres tavshedspligt. Revision har påset, at Ajour System A/S' personalepolitik er nemt tilgængelig, og har et afsnit omkring vilkår for fortrolighed, som følge af information opnået ifm. arbejde udført hos Ajour System A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 8:

Styring af aktiver

Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og funktionsmæssige informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig "ejer". Virksomheden skal sikre, at informationsaktiver i forhold til Ajour System A/S' SaaS løsninger får et passende beskyttelsesniveau.

Beskyttelsesforanstaltningerne skal også omfatte destruktion af forældet eller beskadiget udstyr.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver. Der er udpeget en ejer for alle væsentlige aktiver i forbindelse med driften af Ajour System A/S' løsninger.	Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til driften af Ajour System A/S' SaaS løsninger. Vi har kontrolleret, at der er udføres risikovurdering for nye aktiver. Vi har ved forespørgsler kontrolleret, at Ajour System A/S overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Informationer og data er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed.	Vi har kontrolleret, at der findes en passende opdeling af aktiver for Ajour System A/S' SaaS-løsninger. I den forbindelse har vi kontrolleret om interne procedurer/forretningsgange omkring ejerskab af applikationer og data er overholdt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.	Vi har: • forespurgt ledelsen om hvilke procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået procedurerne for destruktion af databærende medier, til bekræftelse af, at de er formelt dokumenterede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 9:

Adgangsstyring

At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for Ajour System A/S' adgangsstyring.	Vi har: • forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i Ajour System A/S. • stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. Ajour System A/S' retningslinjer. • gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger Ajour System A/S' retningslinjer, og at autorisationer tildeles i henhold til aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang. Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåges.	Vi har ved stikprøvevis inspektion påset: • at der anvendes passende autorisationssystemer i relation til adgangsstyring i Ajour System A/S. • at den formaliserede forretningsgang for tildeling og afbrydelse i brugeradgang er implementeret i Ajour System A/S' systemer, og at der foretages løbende opfølgning på registrerede brugere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Interne brugeres adgangsrettigheder gennemgås regelmæssigt efter en formaliseret forretningsgang.	Vi har ved stikprøvevis inspektion påset, at der eksisterer en formaliseret forretningsgang for opfølgning på kontrol af autorisationer i henhold til retningslinjerne, herunder: • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med udvidede rettigheder • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med almindelige rettigheder	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 9:

Adgangsstyring

At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Tildeling af adgangskoder styres gennem en formaliseret og inspiceret proces, som bl.a. sikrer, at der sker skift af standardpassword.	Vi har forespurgt ledelsen, om der er etableret procedurer for tildeling af adgangskoder i Ajour System A/S. Vi har ved stikprøvevis inspektion påset, • at der ved tildeling af adgangskode sker en automatisk systemmæssig kontrol af, at password skiftes ved første login. • at standardpassword ved implementering af systemsoftware mv. skiftes. • hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standardpassword.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Adgange til operativsystemer og netværk er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde (8 tegn), krav til kompleksitet og maksimal løbetid (max 180 dage).	Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i Ajour System A/S. Vi har ved stikprøvevis inspektion påset, at der er etableret passende programmerede kontroller for sikring af kvalitetspassword, der sikrer efterlevelse af politikker for: • minimum længde for password • kompleksitet for password • maksimal levetid for password	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 11:

Fysisk sikkerhed og miljøsikring

Der skal være beskyttelse af virksomhedens lokaler og informationsaktiver mod uautoriseret fysisk adgang samt fysiske skader og forstyrrelser. Der skal opbygges sikkerhedstiltag, som sikrer, at der undgås tab af, skader på eller kompromittering af virksomhedens informationsaktiver samt forstyrrelser af virksomhedens forretningsaktiviteter. Beskyttelsesforanstaltningerne skal også omfatte destruktion af forældet eller beskadiget udstyr samt sikring af nødvendige forsyninger som el, vand og ventilation samt kabelinstallationer.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret en sikker fysisk afgrænsning af bygning og kontor og disse er beskyttet mod uautoriseret adgang.	Vi har forespurgt ledelsen om alle relevante procedure er implementeret. Vi har gennem observation kontrolleret, at bygninger og kontorer er afgrænset samt der er implementeret beskyttelse mod uautoriseret adgang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Driftsprocedurer og ansvarsområder

En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter, og de heraf afledte kapacitetskrav.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er dokumenteret driftsafviklingsprocedurer for forretningskritiske systemer, og den er tilgængelige for personale med et arbejdsbetinget behov. Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse.	Vi har: • forespurgt ledelsen om alle relevante driftsprocedurer er dokumenteret. • i forbindelse med revisionen af de enkelte driftsområder stikprøvevist kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud. Der foretages kapacitetsovervågning som sikrer, at der kan ske skalering i forhold til kundebehov samt kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.	Vi har: • forespurgt ledelsen om procedurerne og kontrolaktiviteterne er udført. • kontrolleret, at ressourceforbruget i driftsmiljøet bliver overvåget og tilpasset i forhold til det forventede og nødvendige kapacitetsbehov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Malwarebeskyttelse

At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret både forebyggende, opklarende og udbedrende sikrings- og kontrolforanstaltninger, herunder den nødvendige uddannelses- og oplysningsindsats for virksomhedens brugere af informationssystemer mod skadevoldende programmer.	Vi har: • forespurgt og kontrolleret de procedurer/ kontrolaktiviteter, der udføres i tilfælde af virusangreb eller –udbrud. • forespurgt og kontrolleret de aktiviteter, som skal gøre medarbejdere opmærksomme på forholdsregler ved virusangreb eller -udbrud. • kontrolleret at der er implementeret antivirusprogrammer og kontrolleret virusscanningsrapporter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Backup

At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foretages sikkerhedskopiering af alle virksomhedens væsentlige informationsaktiver, herunder eksempelvis parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået backupprocedurer, til bekræftelse af at de er formelt dokumenterede. • stikprøvevist gennemgået backup-log, til bekræftelse af at backup er gennemført succesfuldt, og at tilfælde af mislykket backup håndteres rettidigt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Logning og overvågning

At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerheds-relaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Operativsystemer og netværks-transaktioner eller -aktiviteter bliver overvåget. Afvigende for-hold undersøges og løses retti-digt. Audit logs er aktiveret på alle systemer. Kun ved mistanke om eller ved konstateret misbrug af syste-merne overvåges brugerne ak-tivt.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter der udføres, og påset, at parametre for logning er opsat, såle-des at handlinger, udført af brugere med udvidede rettigheder, bliver log-get. • Kontrolleret at unormale forhold under-søges og løses. • kontrolleret audit logs er aktiveret og gennemgås regelmæssigt.	Vi har ikke ved vo-res test konstateret væsentlige afvigel-ser.

Kontrolmål: Styring af driftssoftware samt sårbarhedsstyring

At sikre, at der er etableret passende forretningsgange og kontroller for implementering og vedli-geholdelse af styresystemer.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Ændringer til driftsmiljøet følger de fastlagte procedurer.	Vi har forespurgt ledelsen, om der er etable-ret procedurer for patch management i Ajour System A/S. Vi har ved stikprøvevis inspektion påset: • at der anvendes passende procedurer for kontrolleret idriftsætning af ændrin-ger til produktionsmiljø. • at ændringer til driftsmiljøer følger de gældende retningslinjer, herunder at registreringer og dokumentation af æn-dringsanmodninger foretages korrekt.	Vi har ikke ved vo-res test konstateret væsentlige afvigel-ser.

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Styring af driftssoftware samt sårbarhedsstyring

At sikre, at der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Ændringer i eksisterende brugersystemer og driftsmiljøer følger formaliserede forretningsgange og processer.	Vi har ved stikprøvevis inspektion påset, at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til produktionsmiljøerne, herunder at krav til patch management kontroller sikrer: • at der sker registrering og beskrivelse af ændringsanmodninger • at alle ændringer er underlagt formel godkendelse inden idriftsætning • at der sker identifikation af systemer, der påvirkes af ændringer • at dokumentationen opdateres så den i al væsentlighed afspejler de påførte ændringer • at procedurer er underlagt styring og koordination	Vi har ikke ved vores test konstateret væsentlige afvigelser.
De etablerede tekniske foranstaltninger testes regelmæssigt i form af sårbarhedsscanninger og penetrationstest.	Vi har spurgt ledelsen, om der findes procedurer for regelmæssig test af tekniske foranstaltninger, herunder udførelse af sårbarhedsscanninger og penetrationstest. Ved inspektion har vi stikprøvevis kontrolleret, at: • Der foreligger dokumentation for regelmæssig afprøvning af de fastsatte tekniske foranstaltninger. • eventuelle afvigelser eller svagheder i de tekniske foranstaltninger er blevet besvaret rettidigt og tilfredsstillende og meddelt de dataansvarlige, hvor det er relevant.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.		
Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og de transmitterede data. Effektiv kryptering anvendes ved overførsel af fortrolige og følsomme personoplysninger via internettet eller via e-mail.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • at der er etableret et ansvar for procedurer for styring af netværksudstyr • at styringen af virksomhedens netværk er koordineret for at sikre en optimal udnyttelse og et sammenhængende sikkerhedsniveau • at forbindelser til datakommunikation over internettet etableres via mere end én ISP-leverandør. • at kryptering anvendes ved overførsel af fortrolige og følsomme personoplysninger over internettet eller via email.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal være etableret passende forretningsgange for håndtering af trusler i form af angreb fra internettet (cyber-angreb). I tilknytning hertil skal der være udarbejdet værktøjer til håndtering af beredskabet i tilfælde af cyber-angreb.	Det er kontrolleret, at der er er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i forhold til håndtering af trusler i forbindelser med cyber-angreb. Vi har ved stikprøvevis inspektion påset: • at der er udarbejdet passende rammer for håndtering af cyber-angreb. • at der er udarbejdet og implementeret planer for håndtering af truslen. • at planerne har et tværorganisatorisk samarbejde mellem interne grupper.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 14:

(Anskaffelse), udvikling og vedligeholdelse af systemer

Sikre at SaaS løsninger er håndteret med en passende it-sikkerhed, herunder en passende funktionsadskillelse mellem produktion og udviklingsmiljø.		
Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Ajour System A/S har defineret formelle kontrolprocedurer for systemanskaffelse og udviklingsproces for systemudvikling og vedligeholdelse. Alle ændringer, der er beregnet til at blive sat i drift i produktionsmiljøet, skal godkendes, før de frigives til produktionsmiljøet. Softwareudvikling skal placeres i uafhængige testmiljøer.	Vi har: • spurgte ledelsen, om der er udarbejdet eller findes en generel kvalitetsstyringsmodel til styring af softwareudvikling. • i forbindelse med revisionen kontrolleret, at der findes procedurer og rutiner for udrulning af softwareændringer. Kontrolmiljøet for udviklingsplatformen er baseret på samme IT-sikkerhedsstruktur som angivet for produktionsmiljøet. Brugerstyring sikrer passende kontrolforanstaltninger i forbindelse med styring af den logiske adgangskontrol. Vi har kontrolleret, at de forskellige brugergrupper styres med faste intervaller. Vi har kontrolleret, om der findes procedurer for adskillelse af produktionsmiljøet og miljøet for udvikling og vedligeholdelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til leverandører håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevist kontrolleret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal udføres regelmæssig overvågning, herunder føres tilsyn med eksterne samarbejdspartnere.	Vi har påset, at findes passende processer og procedurer for løbende overvågning af eksterne leverandører. Vi har kontrolleret, at der udføres løbende tilsyn gennem indhentning af uafhængige revisionsrapporter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

At opnå, at sikkerhedshændelser og svagheder i virksomhedens informationsbehandlingssystemer rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt, og håndteringen sker på en ensartet og effektiv måde.	Vi har forespurgt ledelsen, om der er etableret procedurer for rapportering af sikkerhedshændelser. Vi har kontrolleret, at der er udarbejdet procedurer og forretningsgange for rapportering og behandling af sikkerhedshændelser, samt at rapporteringen tilgår rette steder i organisationen jf. retningslinjer. Vi har kontrolleret, at ansvaret for håndteringen af kritiske hændelser er klart placeret, og at de tilhørende forretningsgange sikrer, at der sker en hurtig, effektiv og metodisk håndtering af brud på sikkerheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Beredskabsstyring skal modvirke afbrydelser i virksomhedens forretningsaktiviteter, beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe samt sikre hurtig reetablering.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt for at fastlægge prioriteringen af afprøvning og vedligeholdelse.	Vi har forespurgt ledelsen, om der er udarbejdet beredskabsstyring for Ajour System A/S' SaaS løsninger. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for udarbejdelse af beredskabsstyring. • at der er udarbejdet og implementeret beredskabsplaner. • at planerne har en tværorganisatorisk beredskabsstyring. • at planerne indeholder passende strategi og procedurer for kommunikation med Ajour System A/S' interessenter. • at beredskabsplaner afprøves på regelmæssig basis. • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Principper for behandling af personoplysninger:

Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme i form af standardkontrakter, Service Level Agreement samt databehandleraftale el.lign., som indeholder oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, og at procedurerne indeholder krav til lovlig behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der udføres alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har kontrolleret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har kontrolleret, ved en stikprøve på et passende antal behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsen underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har kontrolleret, at ledelsen sikrer, at behandling gennemgået, og at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har kontrolleret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har kontrolleret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Databehandling:

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

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har kontrolleret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har kontrolleret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har kontrolleret, at procedurerne er opdateret. Vi har stikprøvevis kontrolleret, at der foreligger dokumentation for, at databehandlingen sker i overensstemmelse med databehandleraftalen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Den databehandlendes ansvar:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Kontrolleret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen Databehandleren anvender alene underdatabehandlere, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere. Kontrolleret ved en stikprøve på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har kontrolleret, at der foreligger underskrevne underdatabehandleraftaler med alle de anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Kontrolleret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Bistå den dataansvarlige:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. kontrolleret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har kontrolleret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har kontrolleret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Fortegnelse over behandlingsaktiviteter:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over den behandling af personoplysninger, som er under databehandlerens ansvar.

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der skal foreligge en fortegnelse over behandlingsaktiviteterne for den SaaS løsningerne.	Vi har kontrolleret dokumentationen for, at der foreligger en fortegnelse over behandlingsaktiviteterne.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der foretages løbende – og mindst en gang årligt – vurdering af, hvorvidt fortegnelsen er opdateret og korrekt.	Vi har kontrolleret dokumentationen for, at fortegnelsen over behandlingsaktiviteterne for den enkelte dataansvarlige er opdateret og korrekt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden:

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

Ajour System A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som opdateres mindst en gang årligt, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for håndtering af brud på persondatasikkerheden, herunder at rettidig kommunikation til den dataansvarlige er beskrevet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandler sikrer registrering af alle brud på persondatasikkerheden.	Vi har kontrolleret dokumentationen for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Vi har kontrolleret dokumentationen for, at ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Vi har ikke ved vores test konstateret væsentlige afvigelser.