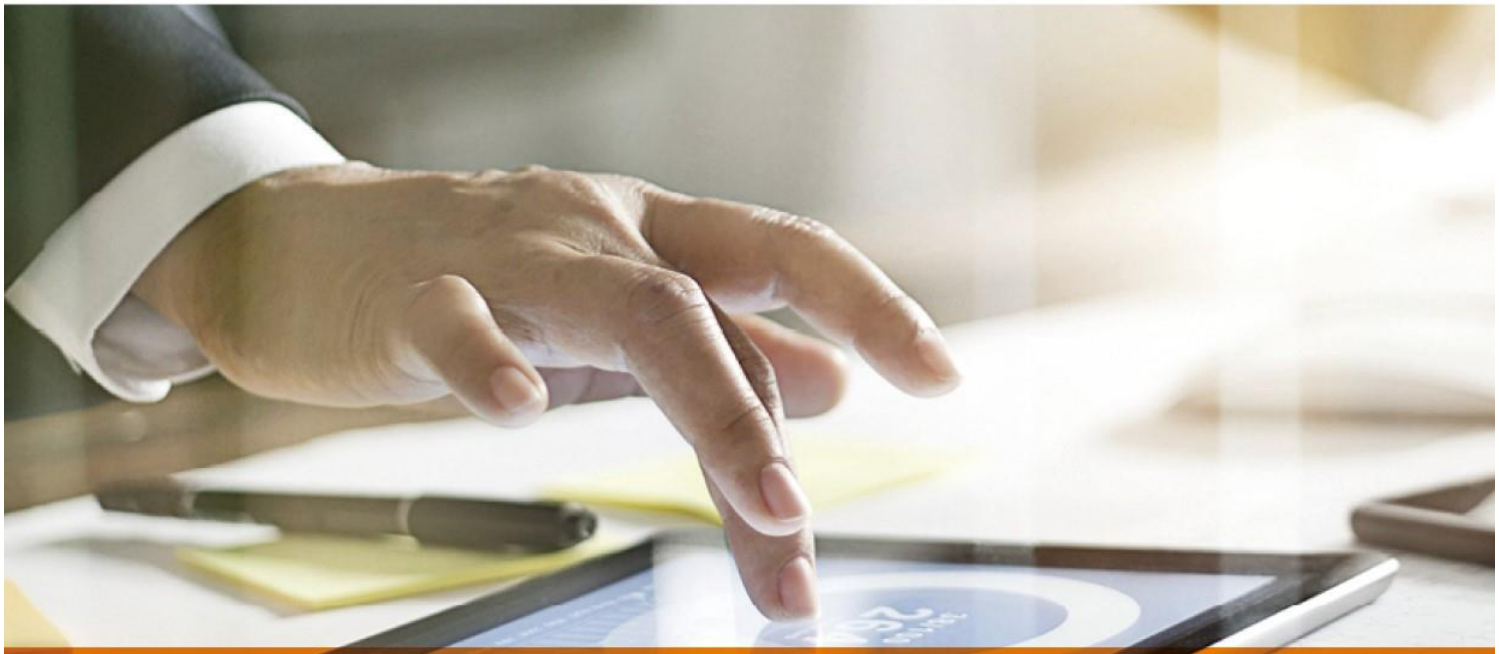
BEIERHOLM
VI SKABER BALANCE



April 2022

Enversion Holding ApS

ISAE 3402 TYPE 2 ERKLÆRING

CVR 41907991

Revisors erklæring vedrørende afdækning af de tekniske og organisatoriske sikringsforanstaltninger i tilknytning til driften af IT-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 kontrolmiljø i tilknytning til driften af IT-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

Enversion Holding ApS behandler personoplysninger på vegne af kunder i henhold til databehandleraftale om Enversion Holding ApS' IT-løsninger.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Enversion Holding ApS' IT-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.

Enversion Holding ApS bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af Enversion Holding ApS' kontrolmiljø i tilknytning til driften af Enversion Holding ApS' IT-løsninger i hele perioden 1. januar 2021 - 31. december 2021. 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 Enversion Holding ApS' IT 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 ved Enversion Holding ApS' IT-løsninger foretaget i forbindelse udførelse af revisionsopgaven

(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. januar 2021 - 31. december 2021. 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. januar 2021 - 31. december 2021.

(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 Enversion Holding ApS' standardaftale samt tilhørende databehandleraftale, grundlaget for IT-løsninger og ydelser omkring de tekniske og organisatoriske sikringsforanstaltninger. Kriterierne for dette grundlag var:

(i) Enversion Holding ApS – Overordnet informationssikkerhedspolitik
(ii) Enversion Holding ApS – Informationssikkerhedspolitikker og procedurer for udvalgte kontrolmål i ISO27002
(iii) Enversion Holding ApS – kontrakter og databehandleraftaler

Aarhus, den 1. april 2022

Direktør, Jacob Høy Berthelsen

Enversion Holding ApS, Fiskerivej 12, 1., 8000 Aarhus C, CVR-nummer 41907991

KAPITEL 2:

Beskrivelse af kontrolmiljøet i tilknytning til de generelle it-kontroller i relation til Enversion Holding ApS

Indledning

Formålet med nærværende beskrivelse er at levere information til Enversion Holding ApS', herefter omtalt som Enversion Holding Group, kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører.

Denne kontrolbeskrivelse afdækker de tekniske og organisatoriske sikkerhedsforanstaltninger, som der er implementeret i tilknytning til driften og udviklingen af IT-løsninger (SaaS-løsninger), som leveres af Enversion A/S og Kaunt A/S.

Beskrivelse af Enversion Holding Group

Enversion Holding Group er en IT-virksomhed med base i Aarhus, DK. Vi har siden 2009 arbejdet med at udvikle intelligente assistenter, der hjælper vores kunder med at træffe de bedste beslutninger på baggrund af proaktiv brug af data. Vores faglige kompetencer inden for datamodellering, maskinlæring og kunstig intelligens er i verdensklasse, og vores ambitioner om at levere det bedste på markedet er tårnhøje. Vi vil til enhver tid hellere prøve en god ide af i praksis end slå den ihjel med regneark og businesscases, og vi insisterer på retten til at være lige dele idealister og opportunister i vores tilgang til verden. Hver dag går vi på arbejde med vores mission for øje: At levere markedets smarteste dataløsninger og bidrage til at gøre menneskers liv bedre, gladere og længere.

Forretningsstrategi/ IT-sikkerhedsstrategi

Det strategiske formål i Enversion Holding Group er at indbygge den nødvendige sikkerhed i vores forretning, så selskabet ikke påføres uacceptable risici til ulempe for os og – ikke mindst – vores kunder. Hos Enversion Holding Group har vi dedikeret os til at hjælpe vores kunder ved hjælp af data. Derfor er informationssikkerhed i fokus og en integreret del af hverdagen hos os. For yderligere information, besøg kaunt.com: https://www.kaunt.com/om-os og Enversion.com: https://www.enversion.com/da/om-os/

Enversion Holding Groups målsætning for informationssikkerheden er, at Enversion Holding Group gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed** af vores løsninger: At opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud.
- **Integritet**: At opnå en pålidelig og korrekt funktion i vores løsninger 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 Enversion Holding Groups 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) og Databeskyttelsesloven udgør den lovgivningsmæssige ramme for behandling af persondata i IT-løsninger, som indgås mellem kunden (dataansvarlige) og Enversion Holding Group (databehandler). Vores ansvar er at foretage de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, der sikrer, at personoplysninger behandles på en sikker og forsvarlig måde.

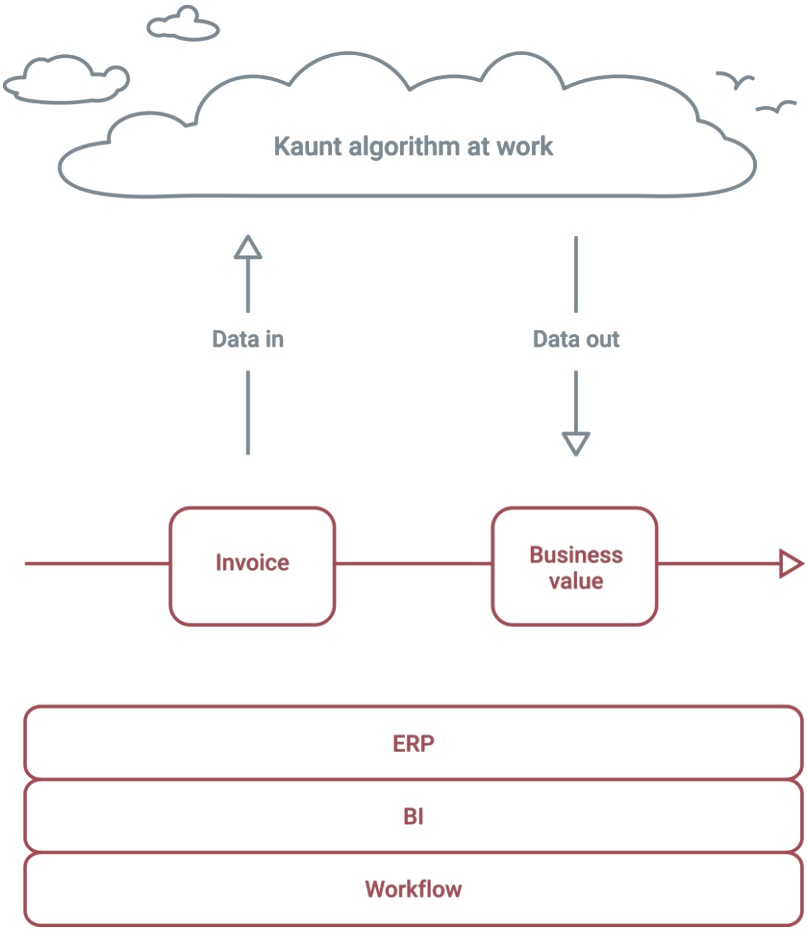
For at sikre en ensartet leverance, som lever op til branchens bedste standarder, har vi valgt at underlægge driften af vores løsninger en revisionsproces med det formål at leve op til kravene i en ISAE 3402 erklæring. Revisionsprocessen gentages årligt, og resulterer i en revisionserklæring.

Beskrivelse af Enversion A/S' ydelser

Enversion er et mangesidigt fællesskab der både rummer datahåndtering, forskning, rådgivning og design. Vi hjælper vores kunder gennem konsulentydelser og projekter, med at opdage nye muligheder inden for databaseret sundhed for at imødekomme behovet for optimeret sundhedspleje på tværs af alle sektorer. Vi har en holistisk tilgang, som kombinerer vores indsigt i sundhedsdata, AI-nyheder og antropologiske feltstudier for at designe og implementere digitale transformationer, der hjælper vores kunder med at fremskaffe den samlede værdi af deres virksomheds hensigter og gøren.

Beskrivelse af Kaunt A/S' ydelser

Kaunt leverer en IT-løsning, hvor kundernes fakturadata indlæses, hvorefter der – baseret på læring fra historiske data – prædikteres et konteringsforslag eller en bogføring, som leveres tilbage til kundens økonomisystem. Kunden kan til enhver tid følge med i Kaunts performance på deres online dashboard.



Omfang for denne beskrivelse

Enversion Holding Group er leverandør af software-as-a-service inden for blandt andet automatisk fakturahåndtering (kaunt™). Desuden bistår Enversion Holding Group en række offentlige aktører med datamodellering, maskinlæring og brug af kunstig intelligens inden for sundhedsdata.

Enversion Holding Group har ansvaret for at etablere og opretholde passende procedurer og kontroller med henblik på at adressere alle relevante it-sikkerhedsaspekter, herunder også overholdelse af krav fra GDPR og Databeskyttelsesloven.

Enversion Holding Group er certificeret inden for de internationale standarder for informationssikkerhed, ISO/IEC 27001 og ISO/IEC 27701.

Enversion Holding Groups organisation og organisering af it-sikkerheden

Overordnet ansvarlig er Enversion A/S' CEO og Kaunt A/S' CEO, der har uddelegeret ansvaret for IT-sikkerheden til Enversion Holding Groups Chief Information Security Officer og Data Protection Officer.

Der udarbejdes altid en samarbejdsaftale og databehandleraftale med kunden, inden Enversion Holding Group behandler data på vegne af kunden.

Risikostyring i Enversion Holding Group

Det er Enversion Holding Groups politik, at de risici, der følger selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde og tilbyde en tilfredsstillende SaaS-løsning til kunderne. Enversion Holding Groups kvalitetsledelsessystem (opbygget iht. krav i ISO 27001:2013) samt ISO 27701:2019 sikrer, at processer og procedurer er effektivt implementeret, hvilket monitoreres løbende.

Enversion har indarbejdet faste procedurer for risikovurdering af forretningen og de kunderelaterede løsninger. Det sikres dermed, at de risici, som er forbundet med de services, som udbydes, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vi vurderer relevante i forbindelse med at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderingen ligger hos ledelsen.

Håndtering af IT-sikkerhed

Chief Information Security Officer (CISO)) hos Enversion Holding Groups har det daglige ansvar for IT-sikkerhed, og derved sikres det, at de overordnede krav og rammer for IT-sikkerhed er overholdt. Gennem den centrale IT-sikkerhedspolitik har ledelsen beskrevet Enversion Holding Groups struktur for IT-sikkerhed. IT-sikkerhedspolitikkerne revideres minimum én gang årligt.

Enversion Holding Groups kvalitetsledelsessystem er defineret ud fra den overordnede målsætning om at levere stabil og sikker SaaS til kunderne. For at kunne gøre det, er der indført politikker og procedurer, der sikrer, at Enversion Holding Groups leverancer er ensartede og gennemsigtige.

Enversion Holding Groups IT-sikkerhedspolitikker er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere. IT-sikkerhedspolitikkerne er udarbejdet, så Enversion Holding Group har ét fælles regelsæt. Dermed opnås en høj kvalitet og et højt sikkerhedsniveau af SaaS. Der foretages løbende forbedringer af både politikker, procedurer og processer.

Enversion Holding Group har omkring IT-sikkerhedsstrategien valgt at tage udgangspunkt i ISO/IEC 27002:2013 samt ISO/IEC 27701:2019, 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
- Fysisk sikkerhed og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetablering-styring
- Overensstemmelse med lov- og kontraktkrav (GDPR)

Rammen for hvilke kontrolmål og underliggende kontrolpunkter (sikkerhedselementer), som Enversion Holding Groups ledelse har defineret relevante for arbejdet med et passende sikkerhedsmiljø er nærmere beskrevet i bilag 1.

HR, medarbejdere og uddannelse

Medarbejdernes domæneviden og kompetencer er en vigtig forudsætning for Enversion Holding Groups forretning. Det er vigtigt at vedligeholde og udbygge de kompetencer, vi råder over, så vi er i stand til at imødekomme udfordringerne i en omskiftelig branche. Medarbejderne har løbende mulighed for faglig videreuddannelse, og alle medarbejdere trænes løbende i informationssikkerhed.

HR arbejder med faste procedurer for bl.a. rekruttering og ansættelse og fratrædelser. Nye medarbejdere gennemgår et grundigt introduktionsforløb til virksomheden. Forløbet omfatter træning i informationssikkerhed via Enversion Holding Groups Informationssikkerhedssystem, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd, dataklassifikation og særligt fokus på Enversion Holding Groups rolle som databehandler.

Enversion Holding Groups medarbejdere har mulighed for at arbejde fra andre faciliteter end kontorerne i Aarhus og København. Virksomheden har udarbejdet en procedure, der beskriver regler og gode råd til fjernarbejdsplads. Vi 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 drøftes relevante IT sikkerhedsemner løbende på Enversion Holding Groups månedsmøder.

Styring af aktiver

Enversion Holding Groups aktiver (udstyr) registreres på en liste som vedligeholdes af CISO. På hvert aktiv påføres en ejer. For så vidt angår brug af Enversion Holding Groups Udstyr indeholder vores informationsledelsessystem politikker vedrørende softwareinstallation, vedligehold samt afskaffelse af udstyr. Desuden har vi politikker for digital kommunikation samt for anti-virus og anti-malware og password politik.

Al information hos Enversion Holding Group klassificeres efter vores Information Classification Guideline.

Hos Enversion Holding Group benyttes ikke bærbare og fysiske medier til behandling af data i forbindelse med levering af vores SaaS løsninger.

Tilbagelevering af aktiver sikres via en off-boarding check list, som gennemgås ved fratrædelse.

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. Adgangsstyringen dokumenteres i et centralt system.

Krav til password - alle brugere oprettet i Enversion Holding Groups centrale brugerdatabase skal skifte password hver 365. dag. Passwordet skal være på mindst 14 og skal leve op til 3 ud af 5 følgende krav:

- Store bogstaver
  - a b c
- Små bogstaver
  - A B C
- Tal
  - 1 2 3
- Tegn
  - @ % ?
- Unicode karakterer som kategoriseres som en alfabetisk karakter, men ikke stor eller lille
  - 百 万 兆

Nye enheder (telefoner, routere, PC'ere mv.) konfigureres og sættes op med nyt administratorpassword, forskellig fra default.

Fysisk sikkerhed

Hosting ved ECIT

ECIT er godkendt hostingleverandør hos Enversion Holding Group. Leverandøren sikrer den højeste driftsstabilitet og sikkerhed i forbindelse med hele Enversion Holding Groups IT-infrastruktur.

Beskrivelse af ydelse ved ECIT

ECIT's hosting-miljø er dækket ind med eget nødstrømsanlæg bestående af nødstrømsakkumulator (UPS) samt diesel generator.

Hosting-miljøet er sikret mod brand med et automatisk brandbekæmpelsessystem.

Alle rackskabe er forsynet med to stk. 32 ampere (A)-grupper i separat fremførte kabelforsyninger. Disse fordeles til otte undersikringer af hver maks. 10 ampere (A). Alle fremføringer sidder parvist på hver sin hovedsikring.

ECIT's kølingsanlæg består af et fuldt ud redundant system, hvor de enkelte kølingsenheder overvåges centralt.

For at sikre mod tyveri er ECIT's datacenter sikret med nyeste alarmteknologi med adgangskontrol på samme sikkerhedsniveau som terrorsikring. Eksternt bliver hele bygningen overvåget via IP-kameraer med bevægelsesdetektorer. Inde i datacentret er der konstant måling af temperatur, røg og brand.

Der er hundepatrulje tilknyttet datacentret 24 timer i døgnet. Sikkerhedsvagten tilkaldes med straks-kørsel i tilfælde af alarm.

ECIT tilstræber at have serverkapacitet efter følgende princip for delte miljøer: At udstyret er kraftigt nok til at afvikle den aftalte drift hos Enversion Holding Group.

Der anvendes serverhardware fra markedsledende producenter såsom HP C-class blade infrastructure, Proliant servere m.v.

Til storage-system anvendes markedsledende SAN/Storage-teknologi som eksempelvis HP enterprise class dedikeret storage. Desuden anvendes andres SAN-systemer. Den tekniske opbygning af SAN-systemerne er sådan, at der er fysisk separation af dels controllere og dels storage enclosures. Sådan garanteres, at spejling af data sker som mirror, og at data findes på to harddiske på to forskellige fysiske enclosures bag ved to fysisk separate controllere. SAN-systemerne er SSD/Flash Storage-accelererede.

Der tages daglig backup af alle servere på datacentret.

ECIT overvåger hvert 5. minut linjer, switche, routere og driftsanlægget generelt, herunder røg, brand og temperatur via alarmcentral.

Firewall: BSD- og Linux-baserede security appliances for afgrænsning mod internettet i redundant setup. Systemet anvender intrusion detection og stateful packet inspection.

Kontroller udført hos ECIT er ikke indeholdt i denne erklæring. Her henvises til ECIT 3402-erklæring.

Hosting hos Microsoft Ireland Operations Ltd.
Der anvendes Microsoft Azure infrastruktur og services som en del af løsningen til at fremme databehandlingen og lette integrationer, samt sikre skalerbarhed ift. udvidelse af løsningen efter behov.

Microsoft Azure miljøet er forbundet via site2site vpn med whitelisting af IP'er til ECIT miljøet.

Kontroller udført hos Microsoft Ireland Operations Ltd er ikke indeholdt i denne erklæring. Her henvises til 3402-erklæring vedrørende Microsoft Azure.

Kontrol med fysisk sikkerhed på kontorlokationer
Enversion Holding Groups primære kontor (hovedkontor) er beliggende på Fiskerivej 12, 1. sal i Aarhus. Kontoret er til enhver tid aflåst, og medarbejdere får udleveret nøglebrikker i forbindelse med ansættelsen. På selve lokationen er fortrolige områder tydeligt markeret – og det er i disse områder, at medarbejderne udfører opgaver, der relaterer sig til kundernes data.

Enversion Holding Groups kontor i København er beliggende i kontorfælleskabet Fintech Lab, Applebys Pl. 7.. Kontorerne er aflåst ved hovedindgangen, og medarbejdere oprettes i Fintech Labs adgangsystem som styres via en mobilapp på den enkelte medarbejdes telefon som iteragerer med en tablet, ved hovedadgang.

Der er ingen lokal hosting af data på Enversion Holding Groups kontorer og der er politikker for adgang til digital data.

Driftssikkerhed

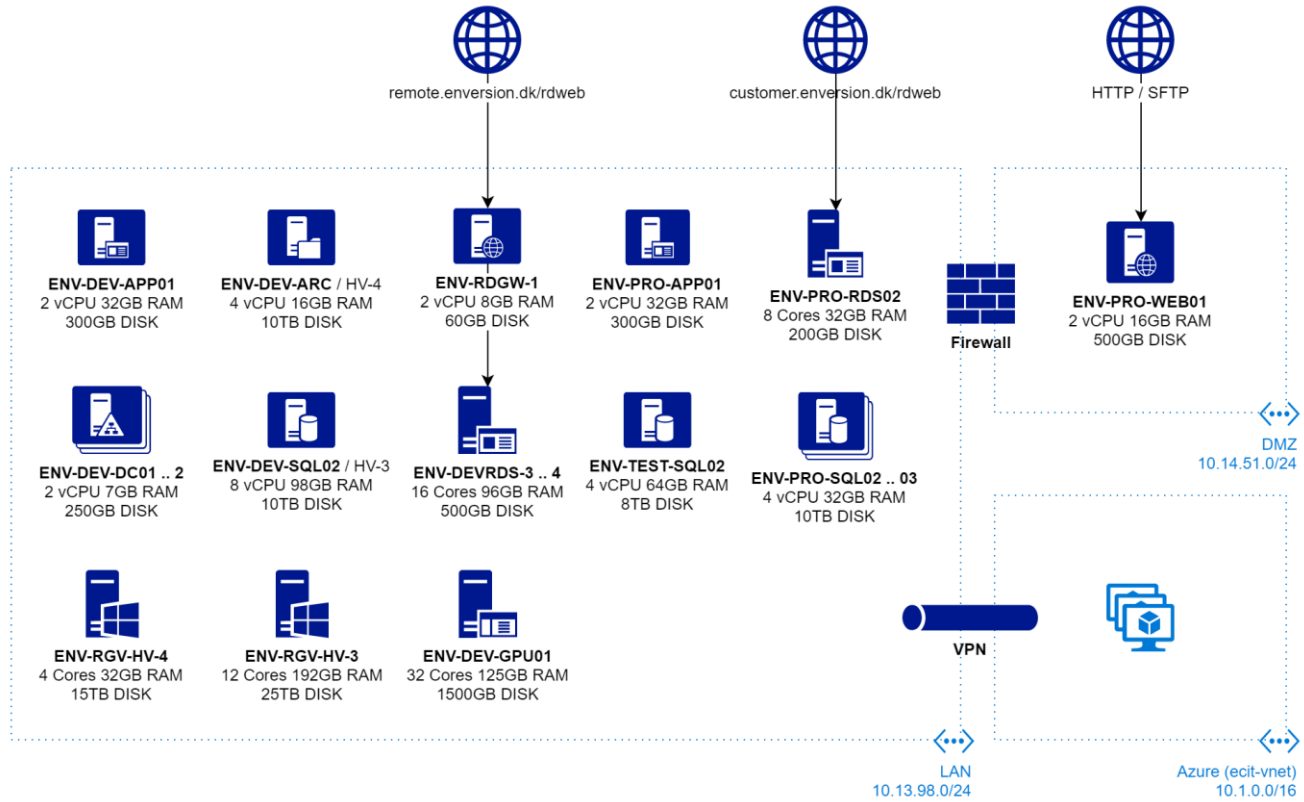
Enversion Holding Group anvender bl.a. af hensyn til driftssikkerheden, hostede løsninger ved hhv. ECIT og Microsoft Azure. Derved overlades driften af kritisk hardware til ovenstående, for at have den højest mulige driftssikkerhed. Hos ovenstående er der for produktionsmiljøerne oprettet servere med failover funktionalitet, samt SLA om høj oppe tid.

Enversion Holding Groups kontorer har en enkelt fiber forbindelse til internettet, og som backup har alle medarbejdere mobiler med mulighed for mobilt hotspot.

Alle opdateringer, ændringer og patches planlægges nøje i samarbejde med ECIT således at potentiel nedetid og påvirkning af Enversion Holding Groups kunders SaaS er så minimal som mulig.

Teknisk setup

Nedenstående figur viser det tekniske setup mellem ECIT/Enversion Holding Group. På figuren ses, hvilke servere der findes hos ECIT, og at miljøet er sikret. Adgang til miljøet sker kun gennem Remote Desktop med tofaktorgodkendelse.



Figur 1 – Teknisk setup ECIT/Enversion

Malwarebeskyttelse

Enversion Holding Group har en politik og procedure for anti-virus og malware beskyttelse.
Alle computere skal have anti-virus og malware software med realtidsscanning.

For så vidt angår infrastruktur hosted i Azure, skal Microsofts antimalware for Azure Cloud Services and Virtual Machines være aktiveret.

Backup

Formålet med backup er at sikre, at kundens data i Enversion Holding Groups SaaS løsninger, samt egne interne data, kan genskabes nøjagtigt og hurtigt, så kunderne undgår unødvendig nedetid. Enversion Holding Group har en politik for backup af data, herunder beskrevet med krav til hvornår, hvor ofte og hvor længe backups skal foretage og opbevares. Backup af Enversion Holding Groups SaaS løsninger og interne systemer driftes og overvåges af ECIT jf. SLA'er og kontrakt mellem Enversion Holding Group og ECIT. Primære kontaktpersoner i Enversion Holding Group informeres direkte af ECIT i tilfælde af problemer.

Logning og overvågning

Enversion Holding Groups hostingpartner (ECIT) har etableret og står for log og overvågning af servere, storagesystemer, netværk, m.v.. Hvis der sker hændelser, som kan påvirke driften, vil nøglemedarbejdere i Enversion Holding Group blive involveret. Der forefindes en indarbejdet procedure for eskalation sluttende med, at den adm. direktør involveres.

For Kaunts SaaS løsning er der intern overvågning og logning af driften, hvor Kaunts egne medarbejdere informeres i tilfælde af problemer.

Patch management / ændringshåndtering

Formålet med patch management er at sikre, at alle relevante opdateringer som patches, fixes og service packs fra leverandører implementeres for at sikre systemerne mod nedetid og uautoriseret adgang, og at implementeringen sker på en inspiceret måde.

Enversion Holding Groups hostingpartner ECIT, står for patchning og ændringshåndtering af alt IT-infrastruktur under ECITs kontrol. Alle ændringer og patches som der påvirker driften, planlægges i fællesskab mellem Enversion Holding Group og ECIT, ift. passende driftsvinduer.

Kommunikationssikkerhed

Enversion Holding Group har en politik for klassificering af informationer og dertilhørende retningslinjer for udveksling af information.

Personoplysninger, der behandles på vegne af vores kunder sendes ikke over mail. Hvis der skulle forekomme tilfælde, hvor det måtte blive nødvendigt, kræves som minimum kryptering på transportlaget.

Kontoret i Aarhus har eget internt trådet og trådløst netværk. Det trådløse netværk er sikret med adgangskode, mens det trådet netværk kun er tilgængeligt på kontoret, hvor adgang kun er muligt vha. adgangsbrik. Opdatering og patchning af netværksudstyret sker automatisk.
Netværk på kontoret i København styres af Fintech Lab.

Kommunikation mellem klient-enheder (Enversion Holding Group medarbejderes udstyr) og Enversion Holding Groups IT-infrastruktur ved ECIT, sker udelukkende gennem en Remote Desktop adgang. Remote Desktop adgangen bruger krypteret transportlag, og er sikret via en gateway, hvor der skal logges ind med bruger, password og 2 faktor godkendelse.

Udvikling og Change Management

Når Enversion Holding Group udvikler software (SaaS-løsninger) bruges der dedikerede udviklings- og testmiljøer, hvorfra softwaren kan afvikles til hhv. udvikling og test. Disse miljøer er forskellige fra de miljøer, som kundernes software afvikles på. Eventuelle fejl i data og systemintegrationer på disse miljøer er således afgrænset til kun at have indflydelse på integriteten af testdata. Testdata er fiktive data oprettet i systemet til formålet (= ikke kundedata). Under de afsluttende testfaser kan der være behov for at teste med data, der ligner live-miljøernes.

Der er fastlagte procedurer for udvikling, test og godkendelse i virksomhedens kvalitetsstyringssystem. Alt udvikling styres gennem agile processer baseret på Microsoft Azure Devops, herunder også brugen af git repositories til ændringsstyring af kildekode.

Leverandørforhold

Enversion Holding Group har en politik for godkendelse af leverandører.
Alle leverandører evalueres og opgøres på en leverandørliste, som godkendes af den øverste ledelse.

For leverandører der behandler personoplysninger på vegne af Enversion Holding Group indgås altid en databehandleraftale.

Der føres kontrol med databehandler minimum én gang årligt.

Styring af IT-sikkerhedshændelser

Sikkerhedshændelser og svagheder i Enversion Holding Groups systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Alle medarbejdere i Enversion Holding Group er bekendt med procedurerapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af Enversion Holding Groups 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

Enversion Holding Group har en beredskabsplan, som beskriver i hovedtræk, hvordan man skal håndtere en krisesituation. Planen indeholder overordnet en punktopstilling, hvoraf det fremgår, hvem der skal involveres hvornår, hvilke systemer og i hvilken rækkefølge man skal genetablere driften.

Overensstemmelse, med rollen som databehandler

Det er ledergruppen hos Enversion Holding Group, der er ansvarlig for at sikre, at alle relevante juridiske og kontraktuelle krav er identificeret og korrekt overholdt. Relevante krav kan omfatte blandt andet:

- Databeskyttelsesforordningen (GDPR)
- Databeskyttelsesloven
- Databehandleraftaler
- Enversion Holding Group Service Level Agreement

Tilstedeværelsen af alle nødvendige aftaler, et omfattende ISMS (ledelsessystem for styring af informationssikkerhed) samt andre relevante dokumenter sikrer overholdelsen af relevante juridiske og kontraktuelle krav.

Enversion Holding Group er forpligtet til at inddrage juridiske eksperter efter behov for at sikre et passende niveau i forhold til overholdelsen af lovgivningen.

Desuden gennemgår ledergruppen regelmæssigt alle Enversion Holding Groups sikkerhedspolitikker. Enversion Holding Groups ISMS revideres regelmæssigt af en uvildig, ekstern part, og revisionsrapporten deles ved forespørgsel med alle Enversion Holding Groups kunder og gøres tilgængelig på Enversion og Kaunts relevante hjemmesider.

EU Databeskyttelsesforordningen (GDPR)
Enversion Holding Groups IT-løsninger understøtter kundernes arbejdsprocesser. Enversion Holding Group ejer ikke de data, kunderne indsamler, men udvikler og driver de IT-løsninger, som kunderne anvender til at udføre den nødvendige persondatabehandling. Ifølge Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er Enversion Holding Group databehandler, og kunden er dataansvarlig.

Enversion Holding Group 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 Enversion Holding Group med sine kunder om at sikre, at kunderne er bekendt med og overholder de relevante GDPR-regler.

Ifølge GDPR sikrer efterlevelsen af ISO/IEC 27001 og ISO/IEC 27701-standarden et passende informationssikkerheds-niveau samt passende sikkerhed for persondata. Udover at overholde de relevante ISO-krav, sikrer Enversion Holding Group data privacy og –sikkerhed på et kontraktuelt niveau.

Databeskyttelsesrådgiver (DPO)
Enversion Holding Group har udpeget en Databeskyttelsesrådgiver, der varetager databeskyttelsesretlige opgaver for selskaberne i koncernen.

Privatliv og beskyttelse af personoplysninger
Som nævnt er Enversion Holding Group databehandler for sine kunder, i og med at kunderne tilbydes en it-service, hvortil der overføre og behandles data, der kan indeholde personoplysninger. Enversion Holding Group er ikke ansvarlig for data, som indlæses fra kunderne. Med udgangspunkt i kategorier og fortrolighed af de typer af data, kunden overlader til behandling, skal Enversion Holding Group iværksætte alle nødvendige sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

Nedenfor beskrives Enversion Holding Groups procedurer for, hvordan man opererer som databehandler under instrukser fra de dataansvarlige.

Databehandleraftaler
Enversion Holding Group indgår databehandleraftaler med alle sine kunder. Databehandleraftalen er en fastlagt procedure ved kontraktindgåelse, og der benyttes enten Enversion Holding Groups egen skabelon eller kundens skabelon. Aftalerne beskriver roller og ansvar for så vidt angår rollen som databehandler og dataansvarlig.

Som databehandler pålægges Enversion Holding Group 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 IT-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 Databeskyttelsesforordningen).
- 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 Enversion Holding Group 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
Enversion Holding Group tilbyder løsninger som *Software as a Service*, der driftes af Enversion Holding Groups driftsafdeling. Udvikling, test og release varetages af egen udviklingsafdeling eller relevante underleverandører. Driftsafdelingen påtager sig dermed det fulde ansvar for behandling af kunders data. Generelt har medarbejdere alene adgang til kundedata, såfremt deres specifikke arbejdsopgaver taler herfor.

Enversion Holding Group 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 via vores ISMS
- Procedure for tildeling og revision og kontrol af adgange til kundedata.
- Regler for behandling af kundedata i Enversion Holding Groups ISMS.

Enversion Holding Group logger og overvåger adgangen til kundernes data for at sikre, at ingen uautoriserede personer får adgang, eller tildelte adgange misbruges.

Væsentlige ændringer i forhold til it-sikkerhed

Per 1/12-21 er kravene til adgangskoder ændret fra minimum 8 karakterer og skift hver 90 dage, til 14 karakterer og skift hver 365 dage. Ændringen følger best-practice indenfor IT-Sikkerhed, og tilføjelsen af 6 karakterer til adgangskoder giver markant længere tid for brute-force attack, hvilket er afspejlet i den længere tid mellem adgangskodeskift.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Dette kapitel beskriver den generelle ramme for Enversion Holding Groups services, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Ansvaret for de forretningssystemer og brugersystemer, som drives via Enversion Holding Groups 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 Enversion Holding Group og det er kundernes ansvar at skabe den nødvendige datatransmission til Enversion Holding Groups datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Enversion Holding Groups beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af Enversion Holding Groups løsninger. Der kan udarbejdes specifikke beredskabsplaner for den enkelte kunde efter behov i forhold til risiko ved afbrydelse i forretningsprocesser.

BILAG 1:

Enversion Holding ApS har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27002:2013

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 sikkerhed

12.1. Driftsprocedurer og ansvarsområder
12.2. Malwarebeskyttelse
12.3. Backup
12.4. Logning og overvågning
12.5. Styring af driftssoftware
12.6. Sårbarhedsstyring

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

18. Overensstemmelse

18.1. Overensstemmelse med lov- og kontraktkrav (GDPR)

** Begrænset ansvar **
Ansvaret for opfyldelse af kontrolmålet er delt mellem Enversion Holding ApS og underdatabehandlerne/leverandørerne.

Se beskrivelsen af kontroller i henhold til afdækning af risikoen, herunder også hvordan Enversion Holding ApS løbende overvåger driftssikkerheden hos underdatabehandlerne/leverandørerne.

KAPITEL 3:

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

Til kunder af Enversion Holding ApS' IT-løsninger og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Enversion Holding ApS' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af kontrolmiljøet i tilknytning til driften af Enversion Holding ApS' IT-løsninger jævnfør databehandleraftaler med kunder, i hele perioden 1. januar 2021 - 31. december 2021, 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. Enversion Holding ApS anvender i forhold til grundlæggende kontrolmiljø eksterne samarbejdspartnere på følgende områder - hosting (den fysiske sikkerhed omkring produktionsmiljøet). Erklæringen dækker ikke kontrol eller tilsyn med underleverandører tilknytning til driften i applikation. Disse underleverandører er nærmere oplistet i databehandleraftaler med kunderne i forhold de enkelte IT-løsninger.

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.

Enversion Holding ApS' ansvar

Enversion Holding ApS er ansvarlig for udarbejdelsen af kontrolbeskrivelsen i kapitel 2 (inkl. bilag 1) og den medfølgende ledelseserklæring i kapitel 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, ISQC 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 Enversion Holding ApS' 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 Enversion Holding ApS 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 Enversion Holding ApS

Enversion Holding ApS' 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 Enversion Holding ApS' ydelser og kontrolmiljø i tilknytning til driften af Enversion Holding ApS' IT-løsninger, således som de var udformet og implementeret i hele perioden 1. januar 2021 - 31. december 2021, 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. januar 2021 - 31. december 2021, 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. januar 2021 - 31. december 2021.

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 Enversion Holding ApS' 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 1. april 2022

Beierholm
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Allan Nielsen
IT-auditor, Konsulent

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 Enversion Holding ApS har levet op til kontrolmålene i perioden 1. januar 2021 - 31. december 2021.

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som Enversion Holding ApS 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 Enversion Holding ApS. 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 IT-løsninger. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

Enversion Holding ApS' 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 IT-løsninger. 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 inspiceret, at der for IT-løsninger arbejdes med en løbende vurdering af den risiko, som opstår som følge af de forretningsmæssige forhold. Vi har inspiceret, at risikovurderingen er forankret ned igennem virksomhedens organisation. Vi har inspiceret, 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.

Enversion Holding ApS' 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 Enversion Holding ApS' seneste IT-sikkerhedspolitik. Gennem revisionen har vi inspiceret, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Samtidig har vi ved revisionen inspiceret, at de underliggende støttepolitikker er implementeret. Vi har inspiceret, at politikken er godkendt og underskrevet af virksomhedens bestyrelse og direktion, og at den er gjort tilgængelig for medarbejderne via Enversion Holding ApS' intranet.	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.

Enversion Holding ApS' 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. Der foreligger passende forretningsgange for medarbejdere omkring angivelse af tavshedserklæring.	Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret. Vi har inspiceret, at it-sikkerheden er forankret på tværs af organisationen i forhold til IT-løsninger. Ved interview har vi inspiceret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder. Gennem forespørgsler og stikprøve på ansættelsesaftale har vi inspiceret, at medarbejdere i Enversion Holding ApS er bekendte med deres tavshedspligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til anvendelsen er håndteret.	Det er inspiceret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevis inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos Enversion Holding ApS 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.

Enversion Holding ApS' 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 Enversion Holding ApS. 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 Enversion Holding ApS' personalepolitik.	Vi har inspiceret, 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 inspiceret, at væsentlige medarbejdere er bekendt med deres tavshedspligt. Vi har gennemgået centrale medarbejderes stillingsbeskrivelser, og efterfølgende testet den enkelte medarbejders kendskab til arbejdsmæssige roller og tilhørende sikkerhedsansvar. Revision har påset, at Enversion Holding ApS' personalepolitik er nemt tilgængelig, og har et afsnit omkring vilkår for fortrolighed, som følge af information opnået ifm. arbejde udført hos Enversion Holding ApS.	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 IT-løsninger får et passende beskyttelsesniveau.

Beskyttelsesforanstaltningerne skal også omfatte destruktion af forældet eller beskadiget udstyr.

Enversion Holding ApS' 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 Enversion Holding ApS' løsninger.	Vi har gennemgået og inspiceret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til driften af Enversion Holding ApS' løsninger. Gennem observation og kontrol har vi inspiceret relationer over til de centrale knowhow-systemer for driften af IT-løsninger. Vi har ved observationer og forespørgsler inspiceret, at Enversion Holding ApS overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Informationer og data i relation til Enversion Holding ApS' løsninger og den efterfølgende drift af it-løsningerne er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed.	Vi har inspiceret, at der findes en passende opdeling af aktiver for Enversion Holding ApS' løsninger. I den forbindelse har vi inspiceret om interne procedurer/forretningsgange omkring ejerskab af applikationer og data er overholdt. Vi har inspiceret, at kontrakter og SLA anvendes som et centralt værktøj til at sikre definitionen, adskillelsen og afgrænsningen mellem Enversion Holding ApS' ansvarsområder og overgangen til kundens ansvarsområde ifm. adgang til informationer og data. Derved påhviler der typisk kunden et eget ansvar med at sikre, at der er et passende beskyttelsesniveau på egne informationer og data.	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.

Enversion Holding ApS' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for Enversion Holding ApS' adgangsstyring.	Vi har: • forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i Enversion Holding ApS. • stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. Enversion Holding ApS' retningslinjer. • gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger Enversion Holding ApS' 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 forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i Enversion Holding ApS. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende autorisationssystemer i relation til adgangsstyring i Enversion Holding ApS. • at den formaliserede forretningsgang for tildeling og afbrydelse i brugeradgang er implementeret i Enversion Holding ApS' 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.

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 Enversion Holding ApS. 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 var opsat kvalitetskrav til password i perioden fra 1. januar 2021 til 30. november 2021 Følgende var påkrævet: minimumslængde (8 tegn) og maksimal løbetid (max 90 dage), lige som password opsætninger medfører, at password ikke kan genbruges (husker de seneste 24 versioner). Der er fortaget ændring kvalitetskrav til password, således at der i perioden fra 1. december 2021 og fremadrettet er krævet en minimumslængde (14 tegn) og maksimal løbetid (max 365 dage), lige som password opsætninger medfører, at password ikke kan genbruges (husker de seneste 24 versioner).	Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i Enversion Holding ApS. 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 • maksimal levetid for password • minimum historik for password Vi har påset, at ændringen til passwords kvalitetskrav er implementeret.	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.

Enversion Holding ApS' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret en sikker fysisk afgrænsning af kontor og lokaler. Kontormiljøet er beskyttet med adgangskontrol og der er etableret aftale med alarmselskab.	Ved interview har vi kontrolleret, at de tekniske foranstaltninger er etableret og at de fysiske adgange til Enversion Holding ApS er i overensstemmelse med ledelsens fastsatte krav. Vi har påset, at er der er etableret aftale med alarmselskab og at der er udført test og kontrol med sikkerhedsudstyret.	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.

Enversion Holding ApS' 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 inspiceret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. • foretaget inspektion af brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud.	Vi har forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. Styring af driftsmiljøet er outsourcet til ECIT.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Malwarebeskyttelse

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

Enversion Holding ApS' 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 inspiceret de procedurer/ kontrolaktiviteter, der udføres i tilfælde af virusangreb eller –udbrud. • forespurgt og inspiceret de aktiviteter, som skal gøre medarbejdere opmærksomme på forholdsregler ved virusangreb eller -udbrud. • Inspiceret at der er implementeret antivirusprogrammer og inspiceret 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.

Enversion Holding ApS' 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. Backup på driftsmiljøet er outsourcet til ECIT. Vi har inspiceret, at backup krypteres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Logning og overvågning

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

Enversion Holding ApS' kontroller	Revisors test af kontroller	Resultat af test
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.	Vi har forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. Overvågning og logning af driftsmiljøet er outsourcet til ECIT.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Styring af driftssoftware samt sårbarhedsstyring

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

Enversion Holding ApS' kontroller	Revisors test af kontroller	Resultat af test
Ændringer til driftsmiljøet følger de fastlagte procedurer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i Enversion Holding ApS. Styring af driftsmiljøet er outsourcet til ECIT.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.		
Enversion Holding ApS' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og de transmitterede data.	Vi har forespurgt ledelsen, om der er etableret procedurer for netværksstyring i Enversion Holding ApS. Styring af netværksmiljøet er outsourcet til ECIT. Vi har inspiceret, at firmwareopdateringer til interne firewalls på kontorlokation overvåges og opdateres.	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 inspiceret, at der er er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i samarbejde ECIT 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 IT-løsninger er håndteret med en passende it-sikkerhed, herunder en passende funktionsadskillelse mellem produktion og udviklingsmiljø.		
Enversion Holding ApS' kontroller	Revisors test af kontroller	Resultat af test
Enversion Holding ApS har tilrettet lagt systemudvikling og vedligeholdelsesaktiviteter baseret på egenudviklet projektmodel. Alle ændringer, som skal idriftsættes i produktionsmiljøet, skal være testet og godkendt af udviklingsgruppen for IT-løsninger.	Vi har inspiceret, at der findes formelle procedurer og forretningsgange for adskillelse mellem produktion og udvikling. Vi har inspiceret, at der foreligger formelle procedurer for systemtest og kvalitetssikring inden release til produktionsmiljøet. Brugerstyringen sikrer, at der en passende kontrol i forbindelse med håndteringen af den logiske adgangskontrol. Vi har inspiceret, at der udføres periodevis kontrol af medlemmer af de forskellige brugergrupper. Udviklingsorganisationen er opbygget med en central styregruppe, som har ansvaret for udformning af passende forretningsgange samt tilhørende ledelseskontroller. Gennem vores revision har vi inspiceret, at der udføres intern uddannelse af medarbejderne, som der arbejder med IT-udvikling og det tilhørende udviklingsmiljø. I processen testede vi, hvorvidt medarbejderne er blevet uddannet i Enversion Holding ApS' kvalitetsmodel for udvikling. Kontrolmiljøet for udviklingsplatformen er baseret på samme it-sikkerhedsstruktur som angivet for produktionsmiljøet. Alle brugeraktiviteter bliver registeret og logget i central database.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
Enversion Holding ApS' 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 inspiceret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevist inspiceret, 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.
Ved ændringer, der påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden. Der anvendes udelukkende anerkendte leverandører.	Vi har forespurgt ledelsen om relevante procedurer, som udføres ifm. udvælgelse af eksterne samarbejdspartnere. Vi har påset, at der er etableret passende procedurer for håndtering af samarbejdet med eksterne leverandører. Vi har gennem kontrol testet, at centrale leverandører har opdaterede og godkendte kontrakter.	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 inspiceret, at der udføres løbende tilsyn gennem uafhængig revisors rapporter.	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.

Enversion Holding ApS' 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 inspiceret, 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 inspiceret, 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.

Enversion Holding ApS' 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 IT-løsninger i Enversion Holding ApS. 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 Enversion Holding ApS' 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.		
Enversion Holding ApS' 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 inspiceret, 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 inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, 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 inspiceret, 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 inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har inspiceret, 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.

Databehandling: Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.		
Enversion Holding ApS' 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 inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, 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 inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har inspiceret ved en stikprøver på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	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 inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at procedurerne er opdateret. Vi har inspiceret ved en stikprøve om der i forbindelse med databehandlinger findes underliggende dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.		
Enversion Holding ApS' 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 inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren anvender til behandling af personoplysninger alene underdatabehandlere, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret 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.
Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	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 inspiceret, at der foreligger underskrevne underdatabehandleraftaler med alle de anvendte underdatabehandlere, som fremgår af databehandlerens oversigt) Inspiceret 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.

Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Vi har 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.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.		
Enversion Holding ApS' 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 inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, 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 inspiceret, 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. Inspiceret 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.		
Der skal foreligge en fortegnelse over behandlingsaktiviteterne for den enkelte IT-løsning kombineret med en tilhørende dataansvarlig.	Vi har inspiceret dokumentationen for, at der foreligger en fortegnelse over behandlingsaktiviteterne for den enkelte IT-løsning sammenstillet med en dataansvarlig.	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 inspiceret dokumentationen for, at fortegnelsen over behandlingsaktiviteterne for den enkelte dataansvarlige er opdateret og korrekt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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.		
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 inspiceret, 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 inspiceret 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 inspiceret 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.

Databeskyttelsesrådgiver: Der efterleves procedurer og kontroller, som sikrer, at der - i de tilfælde hvor det er krævet - er udpeget en databeskyttelsesrådgiver, som opfylder krav om tilstrækkelig kompetence, og som er anmeldt til tilsynsmyndigheden.		
Enversion Holding ApS' kontroller	Revisors test af kontroller	Resultat af test
Databehandler har udpeget en databeskyttelsesrådgiver som lever op til krav om tilstrækkelig kompetence.	Vi har inspiceret dokumentationen for databehandlerens vurdering af, hvorvidt der skal udpeges en databeskyttelsesrådgiver eller ej.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.	Vi har inspiceret dokumentationen for, at kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Kontaktoplysninger på databeskyttelsesrådgiveren er meddelt tilsynsmyndigheden.	Vi har inspiceret dokumentationen for, at kontaktoplysninger på databeskyttelsesrådgiveren er meddelt tilsynsmyndigheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.