et trygt samfund med it og data

Revisorerklæring

CVR Nr.: 31 43 07 47

Emply ApS

Erklæring fra uafhængig revisor – ISAE 3000
Erklæringsafgivelse med høj grad af sikkerhed i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov som databehandler for leverancen af Emply ApS' SaaS løsning i perioden d. 12. marts 2020 til d. 31. marts 2021.

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Maj 2021

Indholdsfortegnelse

Afsnit 1:	Emply ApS' systembeskrivelse	1
Afsnit 2:	Emply ApS' udtalelse	11
Afsnit 3:	Uafhængig revisors erklæring med høj grad af sikkerhed om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov for perioden fra d. 12. marts 2020 til d. 31. marts 2021	13
Afsnit 4:	Kontrolmål, udførte kontroller, test og resultater heraf	16

Afsnit 1: Emply ApS' systembeskrivelse

Indledning

Formålet med nærværende beskrivelse er at levere informationer til Emply ApS' kunder og deres revisorer vedrørende kravene i ISAE 3000, som er den internationale revisorstandard for erklæringsopgaver omkontroller hos serviceleverandøren.

Formålet med denne beskrivelse er en afdækning af de tekniske og organisatoriske foranstaltninger, som er impliceret i forbindelse med driften af Emply ApS' Software-as-a-Service løsninger (SaaS løsning).

Som supplement til ovenstående beskrivelse er der tilføjet et selvstændigt afsnit (Overensstemmelse med rollen som databehandler) med beskrivelse af centrale krav i forbindelse med rollen som databehandler, kombineret med generelle krav fra databehandleraftaler.

Derudover giver beskrivelsen informationer om de kontroller, der er anvendt til driften af Emply ApS' SaaS løsning, samt hvorledes de er implementeret.

Beskrivelse af Emply ApS

Emply blev grundlagt i København i 2010 af Michael Ahlstrøm og Gert Abildskov. SaaS løsningen blev udviklet til at servicere HR medarbejdernes behov for en moderne løsning. Platformen kan tilpasses til alle virksomheder uanset branche, størrelse, organisationsstruktur eller HR-arbejdsgange, uanset hvor i verden virksomheder er placeret. I dag er Emply tilgængelig på mere end 16 sprog og bliver benyttet i mere end 50 lande.

Emply ApS leverer egenudviklet Software-as-a-Service, som omfatter 100% drift, service og support, konsulentydelser og undervisning. Emply leverer løbende tilpasninger af funktionalitet og integrationer, så systemerne lever op til kunders krav samt gældende lovgivning og reguleringer.

Emply ApS' SaaS løsning leveres i dag til det private og offentlige virksomheder. Løsningen driftes i Danmark og afvikles som en private cloud løsning hos GlobalConnect i Glostrup. Emply ApS drifter løsningen og GlobalConnect leverer "kun" housing, strøm og adgang til internet.

Forretningsstrategi/ IT-sikkerhedsstrategi

Det er Emply ApS' strategi, at den nødvendige sikkerhed skal være indbygget i forretningen, så selskabet ikke påføres uacceptable risici.

Hensigten med sikkerhedspolitikken er desuden at tilkendegive over for alle, som har en relation til Emply at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Emply fremstår troværdig både nationalt og internationalt.

For at fastholde Emply ApS' troværdighed skal det sikres, at information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som Emply ApS' mest kritiske ressource. Der lægges derfor vægt på driftssikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, så Emply ApS' image og med- arbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen medarbejdere skal være hævet over sikkerhedsbestemmelserne.

Målene er derfor, at:

- Opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud ogdatatab - TILGÆNGELIGHED
- Opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- Opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- Opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- Opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

Det er Emplys mål at opretholde et informationssikkerhedsniveau, der som minimum:

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

Den danske Databeskyttelseslov og EU's persondataforordning udgør den lovgivningsmæssige ramme for behandling af persondata i IT-service. Der indgås databehandleraftaler mellem kunder og Emply ApS.

Vores ansvar er at foretage de nødvendige tekniske og organisatoriske foranstaltninger 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 understøtte driften af vores SaaS løsninger med en revisionsproces med det formål at leve op til kravene i en ISAE 3000 erklæring. Emply ApS' SaaS løsninger understøttes af en leverandør til housing (GlobalConnect) der leverer en ISAE 3402 erklæring.

Revisionsprocessen gentages årligt, og resultatet i en revisionserklæring, fremvises til eksisterende under samt nye mulige kunder. Erklæringen kan bidrage til kunders (dataansvarlig) kontrol af, hvorvidt Emply lever op til instruksen i den indgåede databehandleraftale.

Emply ApS har omkring IT-sikkerhedsstrategien brugt metoder til at implementere de relevanteforanstaltninger inden for følgende områder:

- Informationssikkerhedspolitik
- Organisering af IT-sikkerheden
- Medarbejdersikkerhed
- Adgangsforhold
- Fysisk sikkerhed og leverandørforhold
- Driftssikkerhed
- Netværkssikkerhed
- Udviklingsmiljø
- Styring af sikkerhedshændelser
- Beredskabsstyring
- Overensstemmelse med rollen som databehandler (Compliance)

Risikostyring i Emply ApS

Det er Emply ApS' politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde en normal drift.

Emply har indarbejdet procedurer for risikovurdering af forretningen. Det sikres dermed, at de risici, som er forbundet med services, vi stiller til rådighed, er minimeret til et acceptabelt niveau.

Risikovurdering foretages periodisk, samt når der ændres i eksisterende systemer eller implementeres nye systemer, som vurderes. Risikovurderingen er en del af den IT-sikkerhedsansvarliges ansvar.

Informationssikkerhedspolitik

Ledelsen hos Emply har det daglige ansvar for IT-sikkerhed, og dermed sikres det, at de overordnede krav og rammer for IT-sikkerhed er overholdt. IT-sikkerhedspolitikken skal som minimum revideres en gang om året.

Emply ApS' IT-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen/sikkerhedshullet omgående. Der følges bestemte procedure som sikrer gennemsigtighed, forebyggende og korrigerende handlinger.

Alle servere, storage og netværksenheder er dokumenteret i Emply ApS. Her logges alle ændringer af vores system. Konfigurationsfiler til netværksenheder (firewall, routere, switches og lignende) er opbevaret og tilgængeligt.

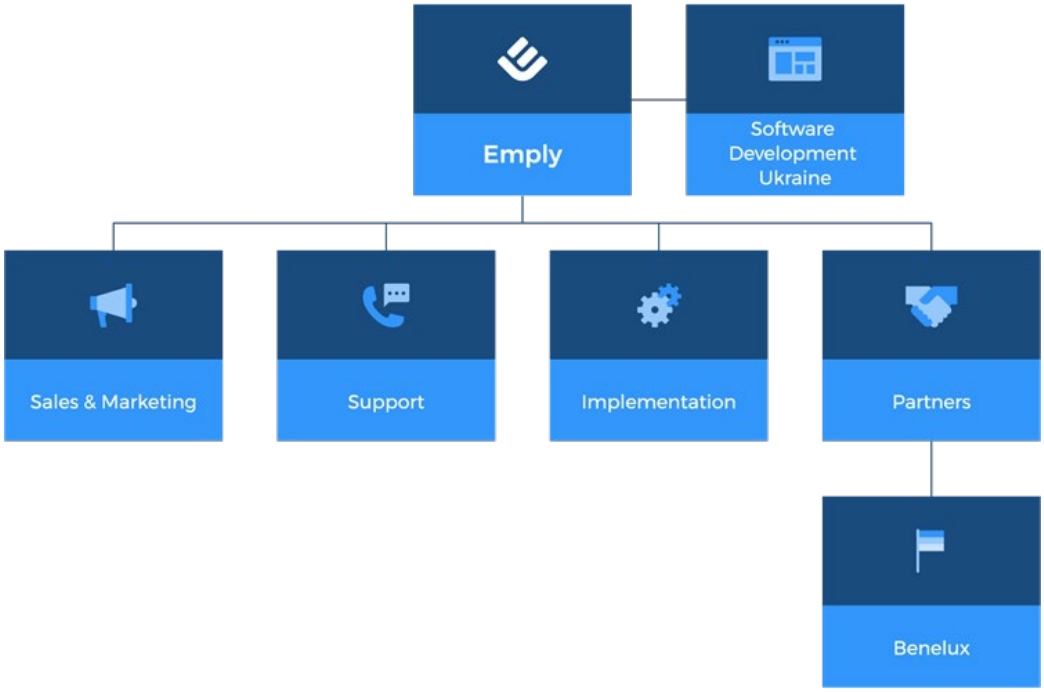
Sikkerhedspolitikken er udarbejdet, så alle medarbejdere i Emply ApS har et fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

Emply ApS' organisation og organisering af IT-sikkerheden

Emply blev i januar 2021 opkøbt af Lessor Group, markedets førende leverandør af software til løn-, HR-, tidsregistrerings- og vagtplanlægnings-løsninger til små og store virksomheder i Danmark, Sverige og Tyskland. De har 180 ansatte og mere end 65.000 virksomheder bruger i dag et eller flere systemer fra Lessor Group.

Lessor Group har siden 2018 været ejet af Paychex, Inc., den førende leverandør af integrerede HCM-løsninger på det amerikanske marked.
Emply ApS er ejet 100% af grundlæggerne til firmaet – Gert Abildskov og Michael Ahlstrøm.

Emply ApS' organisationsstruktur:



Management er ansvarlig for den daglige drift af både organisationen samt indenfor IT.

Sales & Marketing er afdelingen der varetager alt kommunikation til kunder i forbindelse med salg, software demonstrationer, deltager på messer, afgiver tilbud og lukker ordrer.

Support er afdelingen der leverer et højt supportniveau til alle vores kunder.

Implementation er afdelingen der sikrer at alle nye kunder får en positiv oplevelse ved opstart hos Emply.

Partners er afdelingen der sikrer at Emply kan sælges og leveres udenfor Danmark.

Software Development Ukraine er afdelingen der udvikler Emply software. Ukraine har udelukkende med udvikling og test af software. Databehandling foregår i Danmark. Ved særlige opgaver, som genskabelse af databaser mv, kan Emply med kundens samtykke give Ukrainsk udvikler adgang til at løse en sådan opgave.

I Emply ApS har vi udpeget Gert Abildskov til at være IT-sikkerhedsansvarlig. Den organisatoriske forankring af IT-sikkerheden er således en naturlig del af ledelsens ansvarsområde.

Medarbejdersikkerhed

Emply ApS' medarbejdere er en vigtig forudsætning for Emply ApS' forretning. Det er vigtigt at vedligeholde og udbygge de kompetencer, vi råder over, så vi kan tilpasse os kundernes behov. Vi arbejder med et årligt KPI-mål, som gør os i stand til at løfte i flok.

Emply ApS anvender sin egenudviklede SaaS løsning. Nye medarbejdere gennemgår en introduktion til alle områder i Emply. Både eksisterende og nyansatte gennemgår Emply ApS' politikker og procedurer. Dette sker for alle medarbejdere.

Alle Emply ApS' medarbejdere har en fortrolighedserklæring der også omhandler hvorledes kunders data behandles. Emply ApS' ansatte har i begrænset omfang mulighed for at arbejde fra andre faciliteter.

Adgangsforhold

Kun autoriserede Emply brugere/ansatte har adgang til Emply systemerne. Tildeling af adgang til drifts-miljø sker i overensstemmelse med formål. Der tildeles rettigheder og adgang til informationer, som man har behov for at kunne udføre sine opgaver/roller bedst muligt.

Adgangsstyring sker fra Emply ledelsen.

Fysisk sikkerhed og leverandørforhold

- *Datacenter*
  Global Connect (tidl. Nianet) har et omfattende sikkerheds-setup og har implementeret formelle politikker, procesbeskrivelser med henblik på adgangskontrol til systemer, faciliteter og datacentre.

  Kontrol med Global Connect:
  Global Connect leverer årligt en ISAE 3402 om fysisk sikring samt en ISAE 3000 om net- og informati-onssikkerhed.

- *Strømsikring og køling*
  Datacentret er opført i henhold Uptime Tier2- eller Tier3-definition. Datacentret forsynes fra den lo-kale el-distributør, gennem standby-generatorer og via UPS-anlæg, som sikrer stabil elforsyning ved nedbrud på offentlig forsyning.

  Køling af rackskabe i datacentret sker under hævede edb-gulve. Køleanlægget sørger for, at køling, filtreret luft "skubbes" op gennem rackskabet nedefra. I Global Connects datacentre anvendes oftest kuber, hvor kold luft forsynes i "kolde gange", og varm luft fra udstyr blæses ud i de omgivende rum, hvorfra et køleaggregat opsuger den opvarmede luft og via kølevand afsætter kalorier i udendørs en-heder. Alle områder og rackskabe har en temperatur på maksimalt 25 grader og en luftfugtighed på maksimalt 60%.

- *Sikring mod vand*
  Datacentret er bygget med forhøjet gulvniveau og der er vand- og fugtdetektorer.

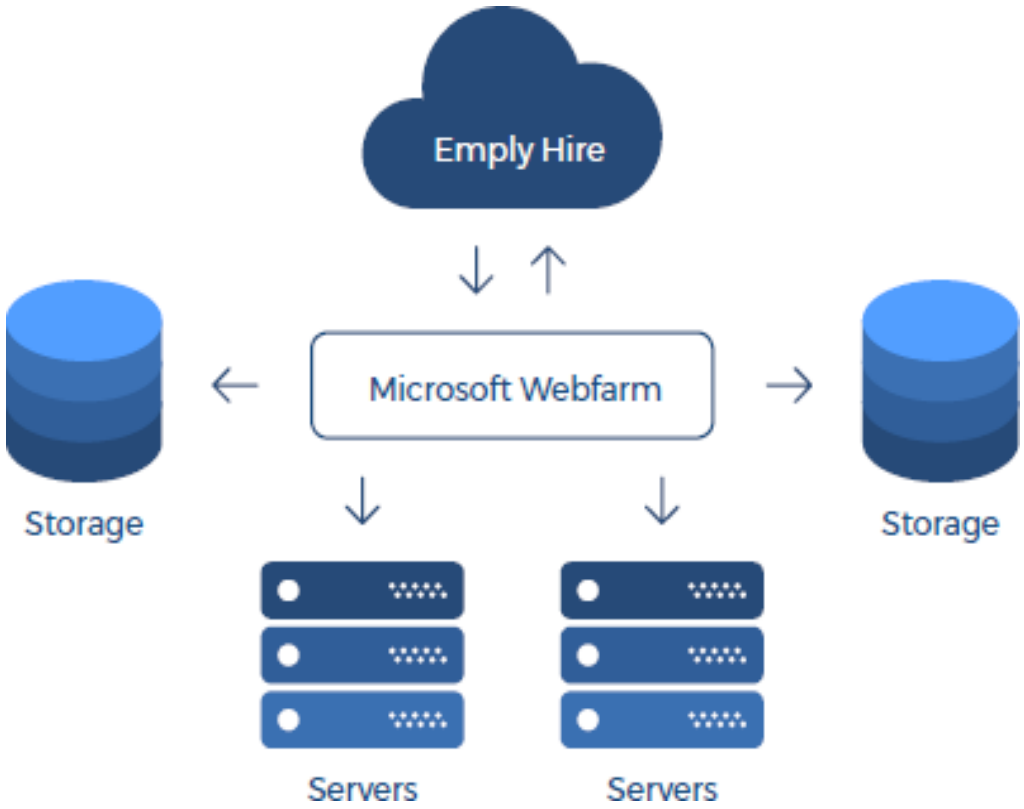
- *Brandsikring*
  De områder, hvor Global Connect har opstillet Emply ApS' udstyr, er opført i brandhæmmende ma-terialer.

Datacenteret er beskyttet af Argonite- eller Inergen anlæg, der er koblet til brandmeldingsanlæg. Der er tilkoblet optiske og ioniserende røgalarmer i både loftet og under det hævede gulv i lokalerne. Disse overvåger konstant områderne og afgiver endvidere audiovisuel alarm. Der er etableret automatiseret og overvåget brandslukningsanlæg. Desuden har Global Connect periodiske serviceeftersyn af UPS, dieselgeneratorerne, brandslukningsanlæggene og klimaanlæggene.

- *Hardware setup*
  Emply leveres som en privat cloud-tjeneste, der bliver kørt på en virtuel Microsoft webfarm. Applikationen hostes på flere virtuelle maskiner. Hver enkelt virtuelle maskine kører på en VMware cluster-løsning. VMware cluster-løsningen kører på seks fysiske servere og al data opbevares i et SD-lagersystem.

  Emply SaaS løsningen er bygget med Microsoft.Net. Alle kunder benytter forskellige SQL-databaser for at sikre en stabil og sikker softwareløsning. Emply løsningen bliver derudover overvåget af flere softwareløsninger, for at opnå et stabilt produktionsmiljø.

  Emply løsningen har adskillige integrationer såsom SSO (Single Sign-on), ADFS, to-faktor godkendelse og flere udvidede webservice-API'er i både SOAP og RES. Alle transaktioner i Emply ApS er gemt og opbevaret i flere logfiler.



Driftssikkerhed

Driftsopgaver udføres af Emply ApS med faste intervaller. Emply ApS varetager ligeledes kontroller, vedligeholdelse samt drift af samtlige servere.

Overvågning

Driftsmiljøet overvåges 24/7/365 via automatiseret service. Der overvåges ressourcer for servere (CPU, RAM, disk, netværk) og tilgængelighed. Overvågningen omfatter også relevante IT-services eksempelvis backups, tilgængelighed for web samt systemer til kunder samt internt brug.

Den primære overvågning foregår internt i driftsmiljøet, men for også at dække den eksterne tilgængelighed har vi etableret en fjernovervågning.

Ved fejl rapporteres direkte til Emply ApS, hvorefter fejlen bliver undersøgt. Er der tale om kritiske fejl i servere eller services, adviseres den vagthavende driftsmedarbejder direkte.

Kunder der oplever driftsproblemer skal kontakte Emply ApS via de supportkanaler, der er aftalt, enten via telefon eller via support@emply.com.

Vi har åben for kunde henvendelser i dagtimerne mandag-torsdag fra kl. 8.30-16.30 og fredag fra kl. 8.30-15.30.

Logning

Logning er et værdifuldt værktøj til overvågning, fejlhåndtering og efterforskning. Da logs indeholder mange forskellige informationer, kan vi opdele disse i to niveauer:

- Systemlog: Emply ApS har udviklet sit eget system til monitorering af fejl.
- Brugerlog: Alle Emply kunder har i Emply systemet adgang til at se hvilke aktiviteter de som kunde har foretaget. Her kan søges efter aktiviteter på kundens egens brugere, specifik dato, projekter, mv.

Backup

Formålet med backup er at sikre, at kundens data kan genskabes nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid. Der tages backup på forskellige niveauer som virtuelle servere, konfigurationer og data. Alle Emply kunder har sin egen database, dette sker for at sikre hurtig og let genetablering via backup.

Alle kunders databaser bliver gemt som krypteret i Veem Backup Solution. Backup etableres dagligt og gemmes via dedikerede backup servere i driftsmiljøet. Daglige backups af kundedatabaser opbevares i 14 dage. Herefter opbevares den sidste backup i hver måned. Backups, der er ældre end 1 måned slettes automatisk.

Patch management

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

Vedligeholdelse af Windows operativsystemer og tilhørende backend-systemer fra Microsoft, håndteres af Microsofts indbyggede WSUS (Windows Server Update Service), hvor sikkerheds- og kritiske patches installeres automatisk med faste intervaller.

Kommunikationssikkerhed

Datalinjer og netværkssikkerhed
Forbindelsen til driftsmiljøet består af 2 uafhængige fiberlinjer. Bryder den primære linje ned, routes trafikken automatisk via den sekundære. Når den primære er reetableret, routes trafikken igen via denne.

Firewallen er regelbaseret og har som udgangspunkt en "deny all" trafikregel. Herpå er der udarbejdet et regelsæt, der tillader specifikke protokoller mod en given servergruppering. Firewallen har en indbygget "Load Balancer", der benyttes til at sikre fordelingen af den samlede trafik til flere servere.

Endelig foretager firewallen inspektion af datapakker (IDS). Automatiseret scanning og blokering af trafik baseres på sårbarhedssituationen holdes dagligt opdateret.

Udviklingsmiljø

Når Emply ApS udvikler software, bruges der dedikerede testmiljøer, hvorfra softwaren kan afvikles til udvikling og test. Disse miljøer er ikke de miljøer som Emply ApS' kunder anvender.

Styring af sikkerhedshændelser

Emply ApS har etableret procedurer for hændelsesstyring og afvigerapportering, herunder sikkerhedsbrud.

Procedurerne sikrer, at der arbejdes systematisk, foretages nødvendige dataindsamling og dokumentation, således at der efterfølgende er et godt grundlag at evaluere ud fra.

Det er ledelsen der er ansvarlig for at definere og koordinere en struktureret proces, der sikrer en passende reaktion på sikkerhedshændelser.

Beredskabsstyring

Emply ApS' IT-beredskabsplan skal sikre, at de IT-afhængige forretningskritiske arbejdsprocesser i Emply kan reetableres og er funktionelle efter at en kritisk hændelse direkte eller indirekte har forhindret normal drift for en periode. Dette sker for at sikre en stabil drift af Emply.

IT-beredskabsplanen skal aktiveres, når en eller flere hændelser forstyrrer eller afbryder kritiske dele af Emply i længere tid og IT-systemerne ikke genoprettes under normal drift og fejlsøgning inden for den fastsatte tidshorisont, som er 2 timer indenfor normal arbejdstid, og 4 timer udenfor.

Planen beskriver håndteringen af 4 scenarier:

- Fysiske hændelser i Emply Datacenter (brand, vandskade eller andet) der sætter Emply ud af drift,
- helt eller delvist.
- IT-hændelser der påvirker driften på Emply
- IT-hændelser der påvirker Emplys IT-infrastruktur (virus udbrud og hackerangreb)
- IT-hændelser der omhandler kompromittering af Emply med risiko for datalækage, hvor andre
- uretmæssigt eller utilsigtet kan få adgang til Emply data eller Emply kunders data

Overensstemmelse, med rollen som databehandler

Det er ledelsen hos Emply ApS der er ansvarlig for at sikre at alle relevante juridiske og kontraktuelle krav er identificeret og korrekt overholdt. Relevante krav kan fx være:

- EU Persondataforordningen
- Dansk lov om Databeskyttelse
- Databehandleraftale
- Emplys hovedaftale
- Emplys brugervilkår

Tilstedeværelse af ovenstående aftaler, samt andre relevante dokumenter sikrer overholdelse af relevante juridiske og kontraktuelle krav.

EU Databeskyttelsesforordningen (GDPR)

Emplys SaaS løsning understøtter kundernes arbejdsprocesser indenfor HR. Emply ApS ejer ikke de data, kunderne indsamler og opbevarer i SaaS løsningen, men udelukkende udvikler og driver SaaS løsningen, som kunderne anvender til at udføre den nødvendige persondatabehandling. Ifølge Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er Emply ApS databehandler, og kunden er dataansvarlig.

Databehandleraftale

Som databehandler pålægges Emply ApS et særligt ansvar i Persondataforordningen, udmøntet som krav i en databehandleraftale. Emply ApS skal blandt andet:

- Føre fortegnelser over, hvilke kategorier af persondata der behandles
- 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
- Informere kunden om navn og kontakt detaljer på leverandører, der er underdatabehandler.
- Sikre at eventuelle krav fra kunden også afspejles hos underdatabehandleren.

Som databehandler arbejder Emply ApS med persondata på baggrund af instruks fra kunderne, der beskriver hvilket formål data må benyttes til. Det er Emply ApS ansvar at sikre at data indsamlet udelukkende anvendes til dette formål.

Adgang til kundedata

Emply løsningen er en SaaS løsning, der driftes af Emply ApS. Test og releases varetages af Emply ApS selv. Derfor har Emply ApS det fulde ansvar for behandling af kunders data. Generelt har medarbejdere i Emply ApS ikke adgang til kunders data, medmindre specifikke arbejdsopgaver taler herfor. Det er udelukkende support samt ledelsen i Emply ApS der har adgang til kunders data.

Alle medarbejdere i Emply ApS har underskrevet en fortrolighedserklæring med fokus på hvorledes vi i Emply behandler kunders data.

Væsentlige ændringer i perioden

Ingen væsentlige ændringer i perioden.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Dette kapitel beskriver de generelle forhold omkring Emply ApS' SaaS løsning, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Emply ApS er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgang til SaaS løsningen. Kunden er selv forpligtet til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Afsnit 2: Emply ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Emply ApS' kunder, som, i rollen som dataansvarlige, har anvendt Emply ApS' SaaS løsning, 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 i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Emply ApS anvender serviceunderleverandørerne GlobalConnect, Paychex Deutschland GmbH (kun for tyske kunder) og Prodesse B.V. (kun for Benelux kunder). Denne erklæring omfatter ikke kontroller hos serviceunderleverandørerne.

Emply ApS bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af Emply ApS' SaaS løsning, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i perioden fra d. 12. marts 2020 til d. 31. marts 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Emply ApS' SaaS løsning 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 Emply ApS' SaaS løsning 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 databehandlerens Emply ApS' SaaS løsning til behandling af personoplysninger foretaget i perioden fra d. 12. marts 2020 til d. 31. marts 2021

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne Emply ApS' SaaS løsning til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved Emply ApS' SaaS løsning, som den enkelte dataansvarlige måtte anse vigtigt 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 perioden fra d. 12. marts 2020 til d. 31. marts 2021. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra d. 12. marts 2020 til d. 31. marts 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.

Glostrup, den 25. maj 20 21

Emply ApS

Gert Abildskov
Direktør

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov for perioden fra d. 12. marts 2020 til d. 31. marts 2021

Til Emply ApS' ledelse, selskabets kunder i rollen som dataansvarlige og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring med høj grad af sikkerhed om Emply ApS' beskrivelse i "Afsnit 1" af Emply ApS' SaaS løsning, i perioden fra d. 12. marts 2020 til d. 31. marts 2021 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Emply ApS anvender serviceunderleverandørerne GlobalConnect, Paychex Deutschland GmbH (kun for tyske kunder) og Prodesse B.V. (kun for Benelux kunder). Denne erklæring omfatter ikke kontroller hos serviceunderleverandørerne.

Emply ApS' ansvar

Emply ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i "Afsnit 2", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), som er baseret på de grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

REVI-IT A/S anvender international standard om kvalitetsstyring, ISQC 11 , og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Emply ApS' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sit Emply ApS' SaaS løsning samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af 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 opnået. En erklæringsopgave med sikkerhed af denne type omfatter desuden vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "Afsnit 1".

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

Begrænsninger i kontroller hos en dataansvarlig

Emply ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Emply ApS' SaaS løsning, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. 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 de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

(a) at beskrivelsen af Emply ApS' SaaS løsning, således som denne var udformet og implementeret i perioden fra d. 12. marts 2020 til d. 31. marts 2021, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra d. 12. marts 2020 til d. 31. marts 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 opnået i alle væsentlige henseender, har fungeret effektivt i perioden fra d. 12. marts 2020 til d. 31. marts 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i det efterfølgende afsnit.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Emply ApS' SaaS løsning, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 25. maj 2021

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Partner, CISA

Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

Den følgende oversigt er udformet for at skabe et overblik over de kontroller, som Emply ApS har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte artikler i perioden d. 12. marts 2020 til d. 31. marts 2021 er efterlevet.

Emply ApS anvender serviceunderleverandørerne GlobalConnect, Paychex Deutschland GmbH (kun for tyske kunder) og Prodesse B.V. (kun for Benelux kunder). Denne erklæring omfatter ikke kontroller hos serviceunderleverandørerne.

De krav, som fremgår direkte af forordningen eller loven, kan ikke fraviges. Derimod kan der justeres på, hvordan sikkerheden implementeres, da sikkerhedskravene i forordningen på flere punkter er af mere generel og overordnet karakter, som bl.a. skal tage hensyn til formål, behandlingens karakter, kategorien af personoplysninger mv. Herudover kan der være konkrete krav i de enkelte kundekontrakter, der kan have en rækkevidde, der går ud over databeskyttelseslovens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos Emply ApS' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Vi har udført vores tests af kontroller hos Emply ApS via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Emply ApS. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
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.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Kortlægning af kontrolområder op mod GDPR-artikler, ISO 27701 og ISO 27001/2

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2.

Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Nyt område ift. ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Nyt område ift. ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15**,** 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15**,** 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til, at behandling skal følge instruks fra dataansvarlige. Vi har inspiceret politikken, og påset, at denne er opdateret i perioden.	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har inspiceret informationssikkerhedspolitikken, og stikprøvevis påset, at denne er i overensstemmelse med databehandleraftaler.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har forespurgt til, om der har været instrukser i perioden, som databehandleren har vurderet til at være ulovlige.	Vi er blevet informeret om, at der ikke har været instrukser i perioden, som databehandleren har vurderet til at være ulovlige. Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Vi har inspiceret, at procedurer er opdaterede.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikrings-foranstaltninger.	Vi har inspiceret risikoanalysen, og påset, at denne er blevet opdateret i perioden. Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har stikprøvevis inspiceret implementering af antivirus, og stikprøvevis påset, at dette er konfigureret i henhold til intern politik. Vi har inspiceret, at antivirus-software er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har stikprøvevis inspiceret firewalls, og stikprøvevis påset, at dette er konfigureret i henhold til intern politik.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har stikprøvevis inspiceret netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har stikprøvevis inspiceret adgange, og stikprøvevis påset, at der er et arbejdsbetinget behov for adgang til personoplysninger.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har stikprøvevis inspiceret overvågning af netværkskomponenter, og stikprøvevis påset, at disse er konfigureret i henhold til intern politik.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevis inspiceret kryptering af transmissioner, og stikprøvevis påset, at krypteringen af konfigureret i henhold til intern politik.	Ingen afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk.	Vi har stikprøvevis inspiceret den etablerede logning, og stikprøvevis påset, at dette er implementeret i henhold til intern politik.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at adgang til personoplysninger skal have et arbejdsbetinget behov. Vi har stikprøvevis inspiceret udviklingsprojekter i perioden, og påset, at adgang til personoplysninger har haft en arbejdsbetinget behov.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har inspiceret, at virksomheden har udført sårbarhedstest i perioden. Vi har inspiceret den løbende overvågning af sårbarheder.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har stikprøvevis inspiceret ændringer i perioden, og stikprøvevis påset, at disse følger den interne procedure for ændringer.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har stikprøvevis inspiceret oprettelse og afbrydelse af adgange i perioden, og stikprøvevis påset, at dette følger proceduren. Vi har forespurgt til løbende kontrol af adgange.	Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af tofaktor autentifikation.	Vi har stikprøvevis inspiceret adgange, og stikprøvevis påset, at dette sker med tofaktor autentifikation.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, så kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret oversigter over adgangsbrikker.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som er opdateret i perioden. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at informationssikkerhedspolitikken er i overensstemmelse med aftalerne	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har stikprøvevis inspiceret ansættelser i perioden, og stikprøvevis påset, at ansættelsesprocessen er blevet fulgt.	Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har stikprøvevis inspiceret ansættelser i perioden, og stikprøvevis påset, at disse har underskrevet en fortrolighedserklæring og er blevet introduceret til informationssikkerhedspolitik.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder deaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har stikprøvevis inspiceret fratrådte medarbejdere i perioden, og stikprøvevis påset, at adgange er ophørt og aktiver er tilbageleveret.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har stikprøvevis inspiceret awarenesstræning i perioden, og stikprøvevis påset, at relevante medarbejdere har deltaget.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver og bliver inddraget i relevante områder.	Vi har inspiceret, at virksomheden har antaget en databeskyttelsesrådgiver.	Ingen afvigelser konstateret.

Kontrolmål D – Tilbagelevering og sletning af personoplysninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én 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 opdaterede.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er aftalt slettefrister.	Ingen afvigelser konstateret.
D.3	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 stikprøvevis inspiceret ophørte dataansvarlige kunder i perioden, og stikprøvevis påset, at data er blevet returneret eller slettet.	Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én 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.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at opbevaring finder sted på aftale lokationer.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst én 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. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at databehandleren alene anvender underdatabehandlere til behandling af personoplysninger.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har forespurgt til, om der har været ændringer i anvendelse af underdatabehandlere i perioden.	Vi er blevet informeret om, at der ikke har været ændringer til anvendelsen af underdatabehandlere i perioden. Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har stikprøvevis inspiceret databehandleraftaler og underdatabehandleraftaler, og stikprøvevis påset, at databehandleren er blevet underlagt samme eller tilsvarende forpligtelser, og at underdatabehandleren er blevet pålagt det samme.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret databehandleraftaler, og påset, at underdatabehandlere fremgår af aftalen.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	VI har inspiceret proceduren for tilsyn med underdatabehandlere, og vi har påset, at der er blevet udført tilsyn med underdatabehandlere.	Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.	Vi har inspiceret databehandleraftaler, og påset, at overførelser til tredjelande er håndteret. Vi har inspiceret lokation for data.	Vi er blevet informeret om, at der ikke overføres til tredjelande, og vi finder dette sandsynliggjort, baseret på vores testhandlinger. Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har inspiceret databehandleraftaler, og påset, at overførsler til tredjelande er håndteret.	Vi er blevet informeret om, at der ikke overføres til tredjelande, og vi finder dette sandsynliggjort, baseret på vores testhandlinger. Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har inspiceret lokation for data.	Vi er blevet informeret om, at der ikke overføres til tredjelande, og vi finder dette sandsynliggjort, baseret på vores testhandlinger. Ingen afvigelser konstateret.

Kontrolmål H – De registreredes rettigheder

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H.1	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 én 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. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har forespurgt til, om der har været anmodninger i perioden.	Vi er blevet informeret om, at der ikke har været anmodninger i perioden, hvorfor vi ikke har kunnet teste procedurerne på området. Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har forespurgt til, om der har været brud i perioden.	Vi her blevet informeret om, at der ikke har været brud i perioden, hvorfor vi ikke har kunnet teste effektiviteten af procedurerne på området. Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har inspiceret, at der foreligger procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden.	Ingen afvigelser konstateret.