Unik System Design A/S

CVR-nr. 17 51 26 92

Uafhængig revisors ISAE 3000-erklæring om kontrolforanstaltninger i henhold til Unik System Design A/S' standarddatabehandleraftale af 22. oktober 2018

Perioden 1. december 2020 - 30. november 2021

UNIK
vi kender din softwaredag

Indhold

1 Ledelsens udtalelse

Unik System Design A/S (Unik) behandler personoplysninger på vegne af Uniks kunder i henhold til software-løsningerne Unik Advosys og Unik Bolig.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Unik Advosys og/eller Unik Bolig, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som underleverandører og Uniks kunder 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.

Unik anvender Sentia, som varetager driften af den underliggende infrastruktur til Unik Hosting. Beskrivelsen i afsnit 3 medtager kun kontrolmål og kontrolaktiviteter hos Unik og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af vores kontroller, er passende designet og operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos Uniks kunder, der forudsættes i designet af Uniks kontroller, er passende designet og operationelt effektive sammen med relaterede kontroller hos Unik. Beskrivelsen omfatter ikke kontrolaktiviteter udført af Uniks kunder.

Unik bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af Unik Advosys og Unik Bolig, der har behandlet personoplysninger for Uniks kunder i perioden fra 1. december 2020 - 30. november 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (I) Redegør for, hvordan aktiviteter og kontroller var designet og implementeret, herunder redegør for:

      i. De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger.

      ii. De processer i både it-systemer og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger.

      iii. De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.

      iv. 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.

      v. 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.

      vi. De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede.

      vii. 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.

      viii. Ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.

ix. Kontroller, som vi med henvisning til Unik Advosys' og Unik Boligs 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.

x. 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 til Unik Advosys og Unik Bolig til behandling af personoplysninger i perioden fra 1. december 2020 - 30. november 2021.

(III) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne 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 behandlingen af personoplysninger, som den enkelte dataansvarlige måtte anse for vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og operationelt effektive i perioden fra 1. december 2020 til 30. november 2021, hvis relevante kontroller hos underleverandører var operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af Uniks kontroller i hele perioden fra 1. december 2020 - 30. november 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 identificerede,

(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 designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. december 2020 - 30. november 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.

Vejle, den 25. februar 2022
Unik System Design A/S

Jens Find
adm. direktør

2 Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om kontrolforanstaltninger i henhold til Unik System Design A/S' standarddatabehandleraftale af 22. oktober 2018

Til: Unik System Design A/S og Unik System Design A/S' kunder

Omfang

Vi har fået som opgave at afgive erklæring om Uniks beskrivelse i afsnit 3 af kontrolforanstaltninger i henhold til Unik System Design A/S' standarddatabehandleraftale af 22. oktober 2018 i hele perioden fra 1. december 2020 - 30. november 2021 (beskrivelsen) og om designet og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Uniks kontroller, er passende designet og er operationelt effektive sammen med relaterede kontroller hos Unik. Vores handlinger har ikke omfattet kontrolaktiviteter udført af de dataansvarlige, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos de dataansvarlige.

Unik anvender Sentia, som varetager driften af den underliggende infrastruktur til Unik Hosting. Beskrivelsen i afsnit 3 medtager kun kontrolmål og relaterede kontroller hos Unik og medtager således ikke kontrolmål og relaterede kontroller hos Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørels kontroller, der forudsættes i designet af Uniks kontroller, er passende designet og operationel effektive sammen med de relaterede kontroller hos Unik. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Sentia, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

Oplysningerne medtaget i afsnit 5, Ledelseskommentarer til afvigelser i ISAE 3000-erklæring for perioden fra 1. december 2020 - 30. november 2021, er præsenteret af ledelsen af Unik med henblik på at give supplerende oplysninger og er ikke omfattet af Uniks beskrivelse. Information om Uniks kommentarer til afvigelser i ISAE 3000-erklæringen har ikke været omfattet af vores handlinger om Uniks beskrivelse, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter, og udtrykker derfor ingen konklusion herom.

Uniks ansvar

Unik er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 3, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene, identifikation af de risici der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier der er præsenteret i ledelsens udtalelse, samt for at designe, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

EY Godkendt Revisionspartnerselskab er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Uniks beskrivelse samt om designet og operationel effektivitet 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 med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og operationel effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes design og operationelle effektivitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, 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

Uniks beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved kontrolforanstaltninger, 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 den operationelle effektivitet 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 kontrolforanstaltninger, således som disse var designet og implementeret i hele perioden fra 1. december 2020 - 30. november 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 designet i hele perioden fra 1. december 2020 - 30. november 2021, hvis kontroller hos underleverandører var operationelt effektive, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Uniks kontroller i hele perioden fra 1. december 2020 - 30. november 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 været operationelt effektive i hele perioden fra 1. december 2020 - 30. november 2021, hvis kontroller hos underleverandører var operationelt effektive, og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Uniks kontroller, har været operationelt effektive i hele perioden fra 1. december 2020 - 30. november 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Unik Advosys og Unik Bolig, 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, 25. februar 2022
EY Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Jesper Due Sørensen
partner

Per Højmark
statsaut. revisor
mne9230

3 Systembeskrivelse

Kontrollerne i denne rapport er baseret på kravene til de tekniske og organisatoriske foranstaltninger nævnt i Uniks standarddatabehandleraftale med deres kunder. Udvælgelsen af kontroller er sket på basis af en risikovurdering, hvor de mest relevante it-generelle kontroller er udvalgt.

Databehandler behandler personoplysninger på vegne af den dataansvarlige med det formål at opfylde aftaler mellem den dataansvarlige og databehandleren om databehandlerens levering af og support på systemerne Unik Advosys og Unik Bolig med tilhørende infrastruktur. For nogle dataansvarlige vil der endvidere være en Unik hostingaftale om driftsafvikling af disse systemer.

Unik behandler personoplysninger i forbindelse med udførelse af opgaver, der ligger inden for rammerne af de i hovedaftalen beskrevne tjenesteydelser og leverancer. Formålet for databehandlingen er derfor overordnet set, at databehandleren kan forestå levering af de aftalte tjenesteydelser og leverancer samt varetage sine forpligtelser over for den dataansvarlige bedst muligt, herunder yde den bedst mulige drift, support og programservice.

Databehandling

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om behandlinger, der måtte opstå i relation til drift, support eller service på Unik Bolig eller Unik Advosys med tilhørende infrastruktur.

Databehandleren indestår alene for integriteten af systemerne Unik Advosys og Unik Bolig og kan ikke administrere eller i det daglige behandle personoplysningerne, der måtte indgå i den dataansvarliges system.

Behandlinger vil derfor primært opstå i de tilfælde, hvor der på baggrund af en etableret aftale arbejdes i kundens systemer gennem en online-forbindelse i forbindelse med support eller service. Disse behandlinger kan bl.a. inkludere redigering, organisering, tilpasning eller ændring og søgning.

For kunder i Unik vil der derudover være behandlinger, der har karakter af opbevaring og drift for den dataansvarlige.

Dertil vil der være behandlinger, der inkluderer bl.a. opbevaring, redigering, organisering, tilpasning eller ændring, sletning og søgning, når databehandleren under instruks fra den dataansvarlige behandler tilsendte kopier af den dataansvarliges databaser.

Personoplysninger

Typen af personoplysninger, der behandles:

- Almindelige personoplysninger, herunder navne- og adresseoplysninger, registreringsoplysninger, herunder CVR-numre (enkeltmandsvirksomhed), kommunikationsoplysninger (telefon, mobil, mail, fax osv.), kopi af legitimation (fx pas) til hvidvask, saldo- og betalingsoplysninger, herunder kontooplysninger og opkrævningsoversigt, inkassooplysninger (herunder RKI-registrering), oplysninger vedrørende gældssanering, medlemsstatus for ansøgere (ind- og udmeldelsesdato, husstandens størrelse, ansøgertype, opnoteringer osv.), oplysninger om lejemål og bi-lejemål og lejemålshistorik, herunder diverse kommunikation med lejer.
- Fortrolige personoplysninger i form af personnumre (CPR-numre), jf. databeskyttelsesloven.

Unik har ingen mulighed for at kontrollere eller regulere, hvad der skrives i fritekstfelter og tilknyttede dokumenter – men Uniks systemer er ikke designet til at indeholde følsomme oplysninger.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- For Unik Advosys:
  - Kredsen af registrerede udgør fortrinsvis den dataansvarliges ansatte, jobansøgere, praktikanter, klienter, sagsparter, sagsmodparter (tredjemand), vidner, kreditorer og debitorer, arvinger, leverandører og samarbejdspartnere.

- For Unik Bolig:
  - Kredsen af registrerede udgør fortrinsvis den dataansvarliges ansatte, jobansøgere, praktikanter, lejere, kreditorer og debitorer, leverandører og samarbejdspartnere.

Praktiske tiltag

Der er formuleret og implementeret passende tekniske og organisatoriske foranstaltninger til sikker behandling af personoplysninger. Disse foranstaltninger er udarbejdet på baggrund af anerkendte branchestandarder og retningslinjer fra databeskyttelsesforordningen og tilsynsmyndigheden.

Foranstaltningerne er fastholdt i et dokumenthierarki, hvor de overordnede politikker for virksomheden er beskrevet i henholdsvis informationssikkerhedspolitikken og persondatapolitikken. Begge politikker er godkendt af ledelsen og er de overordnede, strategiske dokumenter for databehandlerens foranstaltninger omkring og håndtering af persondata.

Disse politikker er forankret i virksomheden gennem en række områdespecifikke vejledninger og instrukser, samt en mere generel håndbog, der alle udspringer af de overordnede politikker. Alle medarbejdere er bekendt med vejledningerne, instrukserne og håndbogen, der tillige altid er tilgængelige til opslag, da de ligger på intranettet. Det er indholdet af disse dokumenter, både den formelle og den løbende awareness-træning af medarbejdere, der tages udgangspunkt i.

Der er udarbejdet en backup- og restore-strategi, som er forankret i Intern IT. Ledelsen og relevante medarbejdere er bekendt med indholdet af disse.

Risikovurdering

For hver behandlingsaktivitet, it-system/informationsaktiv og datamodtager, er der foretaget en vurdering af sandsynligheden for, at der sker tab af fortrolighed, integritet eller tilgængelighed. I denne vurdering er der taget udgangspunkt i kendte, potentielle trusler og i de foranstaltninger, der er implementeret for at beskytte oplysningernes fortrolighed, integritet og tilgængelighed. Der er tillige foretaget en vurdering af, hvad konsekvensen for de registrerede potentielt ville være ved tab af fortrolighed, integritet eller tilgængelighed. Vurderingen er baseret på, om oplysningerne er almindelige, fortrolige eller følsomme og de eventuelle indirekte konsekvenser med hensyn til typen af persondata.

Baseret på vurderingen af sandsynligheden og konsekvensen ved behandlingsaktiviteten er der udregnet en risiko-rating. Disse vurderinger foretages af de ansvarlige for behandlingsaktiviteterne i samarbejde med de GDPR-ansvarlige. På baggrund af vurderingerne vil der blive igangsat en konsekvensanalyse og en handlingsplan, hvis det vurderes, at risikoen for den konkrete behandling ligger for højt.

Kontrolforanstaltninger

I det følgende refereres der til kontrolaktiviteterne med de referencenumre, som de er beskrevet ud for i kapitel 4.

Medarbejdere

Alle medarbejdere er underlagt passende tavshedspligt (Kontrolaktivitet A.1). Både i onboarding-processen og gennem løbende awareness træning bliver medarbejderne trænet i behandlingen af persondata (Kontrolaktivitet A.2 og A.3).

Adgang til persondata gives, hvor der foreligger et aftalemæssigt grundlag herfor. Dernæst skal der være et arbejdsbetinget behov, som styres gennem rettighedstildeling baseret på organisatorisk placering. Det betyder segmentering mellem Unik Advosys' og Unik Boligs kundesystemer, således at alene medarbejderne i den relevante afdeling kan tilgå dem. Teknisk afdeling har som udgangspunkt adgang til alle kunders systemer (Kontrolaktivitet D.1 og D.4). Det betyder ligeledes segmentering mellem udvikling- og driftsmiljø (Kontrolaktivitet G.6).

Både ved til- og fratrædelse opretter nærmeste leder en sag hos Intern IT, der opretter eller nedlægger brugeren. Minimum én gang årligt kontrolleres det, at alle adgange for alle fratrådte medarbejdere er nedlagt korrekt og rettidigt. Der foretages tillige kontrol af, om nuværende medarbejdere har de korrekte adgangsrettigheder (Kontrolaktivitet D.2-D.3).

Alle medarbejdere anvender passwords, der følger vedtagen politik på området, og som er fastholdt internt i en håndbog. Håndbogen foreskriver, at medarbejderes password er personlige og fortrolige og derfor ikke må udleveres til andre. Ligeledes anbefales det at undgå at anvende samme password til private og arbejdsmæssige formål (Kontrolaktivitet C.1-C.4).

Særlige adgange

I de tilfælde, hvor en kunde specifikt instruerer, at deres database skal behandles internt i Uniks systemer, følges en nedskreven proces (Kontrolaktivitet I.3). Processen sikrer, at persondata i databasen bliver anonymiseret, medmindre kunden udtrykkeligt instruerer Unik i noget andet. Databasen stilles herefter til rådighed for de medarbejdere, der er specielt udpeget til at skulle have adgang for at løse den specifikke opgave. Adgang styres gennem medarbejderens individuelle Windows-login gennem integrated security (Kontrolmål F.1 og F.2).

Ingen normale brugerkonti har privilegerede rettigheder i systemerne. Der er oprettet særskilte brugerkonti med privilegerede rettigheder. Det kontrolleres halvårligt, at der kun findes privilegerede brugere tilgængelige for medarbejdere, der har et arbejdsbetinget behov for det (Kontrolaktivitet E.1-E.2).

Fysisk sikkerhed

Der er etableret passende fysisk sikkerhed, der sikrer, at ingen uvedkommende kan få adgang til Uniks lokaliteter. Dette inkluderer lås på alle døre, hvor individuelle nøglebrikker styres fra et program, som kun få har adgang til (Kontrolaktivitet B.3-B.4). Det inkluderer ligeledes passende alarmer (Kontrol-aktivitet B.7).

For Uniks eget serverrum, der er placeret på 1. sal for at beskytte mod oversvømmelse, er der etableret yderligere lås, så kun medarbejdere med identificeret arbejdsbetinget behov har adgang (Kontrolaktivitet B.1, B.2 og B.5). Her er desuden etableret alarmering for indbrud samt forhøjet temperatur og fugtighed, som serviceres regelmæssigt (Kontrolaktivitet B.6).

Den fysiske sikkerhed inkluderer desuden, at fysiske, flytbare, databærende medier bortskaffes på forsvarlig vis (Kontrolaktivitet H.1 og H.2).

Unik Hosting driftsafvikles fra eksternt datacenter hos Sentia. Herfra modtages årligt en revisorerklæring, der gennemgås for at sikre, at den fysiske sikkerhed på stedet lever op til Uniks eget niveau (Kontrolaktivitet J.1).

Teknisk sikkerhed

Der er opsat passende tekniske foranstaltninger for at beskytte mod udefrakommende angreb på både servere og klienter (Kontrolaktivitet G.1-G.3). Der er ligeledes opsat tekniske foranstaltninger, der sammen med almindelig medarbejder-awareness og kommunikation om Uniks retningslinjer for behandling af personoplysninger skal forhindre medarbejdere i uautoriserede eller uforsætlige ændringer eller misbrug af persondata eller virksomhedens øvrige aktiver (Kontrolaktivitet G.5 og A.2).

Der er etableret formel patch management-procedurer for egne systemer og kundesystemer som Unik driftsafvikler (Kontrolaktivitet G.2). Kundesystemer kan alene tilgås online gennem et værktøj, der tilsikrer, at den enkelte medarbejder ikke får kendskab til logon-credentials hos kunden. Alt tilgang til kundesystemer bliver desuden logget gennem værktøjet, og loggen monitoreres på anmodning (Kontrolaktivitet G.5).

Der foretages regelmæssig backup af både Uniks egne servere og også kundeservere i Hosting. Sidstnævnte overvåger Unik gennem daglige rapporter fra Sentia (Kontrolaktivitet J.2 og J.3).

Unik bestræber sig på at gennemføre en årlig penetrationstest på enten det interne miljø eller det outsourcede hostingmiljø.

Hosting

Unik har defineret reglerne for firewall i hostingmiljøet, der alene omfatter Uniks kunder. Leverandøren administrerer denne firewall på vegne af Unik og sender løbende rapporter herom til identificerede nøglepersoner.

Unik har egne servere, der er dedikeret til Uniks kunder, hos Sentia. De forskellige kundesystemer er adskilt af VLAN-opdeling , og denne segmentering bliver periodisk testet af ekstern, uvildig part. Erklæringen omfatter ikke aktiviteter og kontroller hos serviceleverandører.

Unik får årligt tilsendt revisionsrapport fra Hosting-leverandøren, der bliver gennemgået for at kontrollere, at leverandøren fortsat lever op til kravene for sikkerhed som fastsat i databehandleraftalen (Kontrolaktivitet J.1).

Kryptering

Der er etableret tekniske foranstaltninger, der sikrer kryptering af mailkorrespondance efter Datatilsynets retningslinjer på området . Der anvendes bl.a. Vipre Secure Mail til kryptering af e-mails med TLS version 1.2 (Kontrolaktivitet I.1-I.3).

De konkrete kontroller fremgår af nærværende erklærings afsnit 4.

Komplementerende kontroller hos de dataansvarlige

Foruden databehandlerens kontrolforanstaltninger er det den dataansvarliges ansvar at:

- sikre, at personoplysninger i systemerne holdes ajourførte.
- vurdere, hvilke personoplysninger systemet skal indeholde.
- have identificeret et formål og en gyldig hjemmel for behandlingerne.
- sikre, at givne instrukser er lovlige set i forhold til den til enhver tid gældende persondataretlige lovgivning.
- sikre, at instruksen til databehandleren er hensigtsmæssig set i forhold til databehandleraftalen og hovedydelsen.
- sikre, at der alene gives adgang til kundeløsningen, som supporthenvendelsen forudsætter.

4 Tests udført af EY

I dette afsnit beskrives de af Unik definerede kontrolmål og tilknyttede kontroller, som sikrer opnåelse af de enkelte kontrolmål. Herudover beskrives de af EY udførte faktiske tests af Uniks kontroller samt resultaterne af de udførte tests.

4.1 Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores test af kontrollers design og operationelle effektivitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår nedenfor. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Uniks kunder, der anvender løsningen, beskrevet i afsnit 1, er ikke omfattet af vores test.

Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden 1. december 2020 til 30. november 2021.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og operationelle effektivitet er 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 af passende personale hos Unik. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

4.3 Resultater af test

I nedenstående oversigt opsummeres tests udført af EY som grundlag for at vurdere de generelle it-kontroller hos Unik.

Kontrolmål A

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
A.1	Alle medarbejdere underskriver en fortrolighedsaftale som et led i ansættelsen. Der foretages en årlig kontrol heraf.	Forespurgt til procedure i forbindelse med ansættelse af nye medarbejdere. Inspiceret stikprøvevis, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret dokumentation for at den årlige kontrol af nyansatte medarbejdere.	Ingen afvigelser konstateret.
A.2	Der gennemføres en eller flere GDPR-/awareness-træning i årets løb med emner, der relaterer sig til GDPR og it-sikkerhed	Inspiceret oversigt over GDPR-/awareness-træning, der er gennemført i løbet af året omfattende emner som GDPR og generel it-sikkerhed. Inspiceret oversigt over GDPR-/awareness-træning, der er gennemført af den enkelte medarbejder.	Ingen afvigelser konstateret.
A.3	Det kontrolleres, at medarbejdere gennemfører awareness-træningen vedrørende GDPR og it-sikkerhed.	Inspiceret eksempler på dokumentation for, at der er foretaget opfølgning på medarbejdernes gennemførelse af awareness-træning vedrørende GDPR og generel it-sikkerhed.	Ingen afvigelser konstateret.

Kontrolmål B
Der efterleves procedurer og kontroller, der sikrer, at der er etableret passende fysisk sikkerhed på lokaliteter, hvor der behandles personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
B.1	Adgang til Uniks lokale datacenter er sikret ved nøglebrik eller systemnøgle til medarbejdere med arbejdsmæssigt behov. Der fortages halvårlig kontrol af medarbejdere med adgang til Uniks lokale datacenter.	Observeret, at adgang til Uniks lokale datacenter kun kan opnås ved anvendelse af nøglebrik eller systemnøgle. Inspiceret dokumentation for halvårlig kontrol af medarbejdere med adgang til Uniks lokale datacenter.	En enkelt it-medarbejdere har haft adgang til datacentret siden maj 2021 uden at have et permanent arbejdsmæssigt behov. Ingen yderligere afvigelser konstateret
B.2	Tildeling af adgang til datacenter kan alene ske efter henvendelse til den administrerende direktør eller økonomichefen.	Forespurgt til procedure for tildeling af fysisk adgang til Uniks lokale datacenter. Inspiceret oversigt over brugere med adgang til systemet der anvendes til kodning af nøglebrikker med henblik på at konstatere, om adgang er begrænset til CEO og CFO.	Foruden økonomichefen har to personer adgang til systemet, der anvendes til kodning af nøglebrikker. Ingen yderligere afvigelser konstateret.
B.3	Fysisk adgang til selskabets domicil i Vejle er sikret ved nøglebrik samt systemnøgle. Uden for normal åbningstid skal der anvendes pinkode sammen med nøglebrik.	Forespurgt om fysisk adgang til selskabets domicil i Vejle, uden for normal åbningstid kræver anvendelse af pinkode sammen med nøglebrik. Observeret, at døren til Uniks domicil i Vejle er aflåst, og at adgang kan opnås ved anvendelse af nøglebrik. Inspiceret dokumentation for opsætning af UniLock vedr. krav om anvendelse af pinkode.	Ingen afvigelser konstateret.
B.4	Fysisk systemnøgle kan alene rekvireres af direktionen eller økonomichefen.	Forespurgt til procedure for udlevering af systemnøgle. Inspiceret, at der foreligger en procedure for anvendelse af fysisk nøgle.	Der er ikke udleveret nye systemnøgler i 2021. Ingen afvigelser konstateret.
B.5	Loggen over adgang til datacenter gennemgås og kontrolleres halvårligt.	Inspiceret dokumentation for, at forsøg på at opnå adgang til Uniks lokale datacenter logges Inspiceret dokumentation for halvårlig kontrol af loggen over forsøg på at opnå adgang til Uniks lokale datacenter.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, der sikrer, at der er etableret passende fysisk sikkerhed på lokaliteter, hvor der behandles personoplysninger.			
B.6	Der er etableret alarm ved forhøjet temperatur samt ved fugt og oversvømmelse i datacentret. Der er desuden etableret aftale om eftersyn af nød-strømsanlæg (UPS) og køleanlæg i datacentret.	Forespurgt, om der foretages serviceeftersyn og test af alarmer ved forhøjet temperatur samt ved fugt og over-svømmelse i datacentret. Inspiceret aftale om etablering af serviceaftale omfattende UPS- og køleanlæg.	Der foreligger ikke dokumentation for serviceeftersyn og test af alarmer vedr. forhøjet temperatur samt ved fugt og oversvømmelse i datacentret. Ingen yderligere afvigelser konstateret.
B.7	Der er etableret indbrudsalarm og aftale om, at der foretages serviceeftersyn heraf.	Inspiceret, at der er etableret indbrudsalarm. Forespurgt, om der foretages serviceeftersyn og test af indbrudsalarm.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, der sikrer, at databehandleren har implementeret passende sikkerhed for tilgang til databehandlerens systemer, herunder krav om kvalitets-passwords.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
C.1	*"Håndbog for IT og Persondata"* foreskriver, at med-arbejdernes password er personlige og fortrolige. *"Håndbog for IT og Persondata"* reviewes og ajourfø-res én gang årligt.	Inspiceret afsnit i *"Håndbog for IT og Persondata"* vedrø-rende beskyttelse af brugernes password. Inspiceret dokumentation for at *"Håndbog for IT og Person-data"* er reviewet og ajourført i 2021.	Ingen afvigelser konstateret.
C.2	Unik har fastsat kvalitetskrav til password og imple-menteret disse i Active Directory på det interne net-værk samt i Microsoft Azure.	Inspiceret password-indstillinger i Active Directory på det interne netværk samt i Microsoft Azure.	Ingen afvigelser konstateret.
C.3	Adgang til systemer og databaser, hvori der sker be-handling af personoplysninger fra et eksternt net-værk, er omfattet af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger der tilgås fra et eksternt netværk.	Ingen afvigelser konstateret.
C.4	Password til system- og servicekonti opbevares i et system, hvortil adgang er begrænset til udvalgte medarbejdere med et arbejdsmæssigt behov.	Forespurgt til procedure for tildeling af adgang af password til system- og servicekonti. Inspiceret oversigt over personer med adgang til password til system- og service-konti.	Ingen afvigelser konstateret.

Kontrolmål D
Der efterleves procedurer og kontroller, der sikrer, at databehandlerens medarbejdere alene har adgang til systemer, herunder systemer med kundedata, i det omfang, der er arbejdsbetinget behov herfor.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
D.1	*"Informationssikkerhedspolitikken"* foreskriver, at adgangsrettigheder skal begrænses til den enkelte medarbejders henholdsvis den eksterne konsulents arbejdsmæssige behov. *"Informationssikkerhedspolitikken"* reviewes og ajourføres én gang årligt.	Inspiceret *"Informationssikkerhedspolitikken"* vedrørende tildeling af adgangsrettigheder til medarbejdere og eksterne konsulenter. Inspiceret dokumentation for at *"Informationssikkerhedspolitikken"* er reviewet og ajourført i 2021.	Ingen afvigelser konstateret.
D.2	Brugernes placering i organisatoriske grupper i Active Directory revurderes regelmæssigt til sikring af tildelte adgangsrettigheder	Forespurgt, om der foretages regelmæssig vurdering og godkendelse af brugernes placering i organisatoriske grupper i Active Directory. Inspiceret seneste revurdering af brugerplaceringer.	Kontrollen er i 8 ud af 16 tilfælde ikke udført i erklæringsperioden. Ingen yderligere afvigelser konstateret.
D.3	Der er etableret en formel procedure for oprettelse og nedlæggelse af brugere, der indebærer, at oprettelse og nedlæggelse af brugere skal godkendes. Tildeling og vedligeholdelse af rettigheder sker via en manuel proces på grundlag af en service request. Det er kontrolleret, at nedlæggelse af brugere sker på grundlag af en service request.	Inspiceret, at der foreligger procedurer for oprettelse og nedlæggelse af brugere og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret, at der foreligger en formel godkendelse inden oprettelser og nedlæggelser af brugere. Inspiceret dokumentation for kontrol af nedlæggelse af brugere. Stikprøvevis inspiceret, at oprettelse af brugere er foretaget via den fastlagte procedure.	Nedlæggelse af brugere er i 4 ud af 35 tilfælde sket uden, at der foreligger en service-request. Ingen yderligere afvigelser konstateret.
D.4	Der foretages halvårlig kontrol af, at privilegerede rettigheder er begrænset til medarbejdere i it-afdelingen samt til eksterne konsulenter med arbejdsmæssigt behov.	Stikprøvevis inspiceret tildelte privilegerede rettigheder. Inspiceret dokumentation for halvårlig kontrol af brugere med privilegerede adgangsrettigheder.	En it-medarbejder er tildelt privilegerede adgangsrettigheder udover et arbejdsmæssigt behov. Ingen yderligere afvigelser konstateret.

Kontrolmål F
Der efterleves procedurer og kontrollerer, der sikrer hensigtsmæssig og arbejdsbetinget brug af in-house kundedata, efter konkret aftale med den pågældende dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
F.1	Der foreligger skriftlig politik og procedurer, som indeholder retningslinjer om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages kvartalsvis kontrol af, at behandling af kundedata alene sker efter instruks fra dataejer.	Stikprøvevis inspiceret dokumentation for kontrol af, at kundedata alene sker efter instruks fra dataejer.	Ingen afvigelser konstateret.
F.2	Der foretages halvårlig kontrol af, at adgang til in-house kundedatabaser alene er tildelt medarbejdere med et arbejdsbetinget behov.	Stikprøvevis inspiceret dokumentation for kontrol af medarbejdere med adgang til in-house kundedatabaser.	Ingen afvigelser konstateret.

Kontrolmål G
Der efterleves procedurer og kontrollerer, der sikrer, at databehandleren har implementeret passende tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
G.1	Der foretages kvartårlig kontrol af at, der er installeret antivirus på servere i det hostede miljø.	Stikprøvevis inspiceret dokumentation for kvartårlig kontrol af antivirus på servere i det hostede miljø.	Ingen afvigelser konstateret.
G.2	Patches til systemer og databaser følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer, herunder sikkerhedspatches. Der foretages halvårlig kontrol af patchning af servere i det hostede miljø.	Stikprøvevis inspiceret dokumentation for halvårlig kontrol af patchning af servere i det hostede miljø.	Ingen afvigelser konstateret.

Kontrolmål G Der efterleves procedurer og kontrollerer, der sikrer, at databehandleren har implementeret passende tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
G.3	Det interne netværk hos Unik er sikret med en firewall, hvori der kun er åbnet for godkendte porte.	Forespurgt til procedure for administration og ændring af firewall.	Der er på nuværende tidspunkt ikke etableret en formel proces for administration og ændring af firewall. Der foretages ikke regelmæssig kontrol af de åbne porte i firewall. Ingen yderligere afvigelser konstateret.
G.4	Unik bestræber sig på at foretage penetrationstest én gang årligt, enten på det outsourcede hostingmiljø eller på det interne netværk.	Forespurgt, om der er foretaget penetrationstest i 2021.	Penetrationstest er ikke foretaget i erklæringsperioden. Ingen yderligere afvigelser konstateret.
G.5	Der er opsat logning af al tilgang til kundesystemer, der ligger i kundens eget miljø eller i Unik hostingmiljø, som sker via RDM.	Forespurgt til opsætning af logning af brugeraktiviteter i systemer og databaser, der anvendes til behandling af personoplysninger, herunder gennemgang og opfølgning på logs. Inspiceret opsætning af logning i RDM.	Ingen afvigelser konstateret.
G.6	Dette er implementeret en change management-procedure hvorved opdateringer til applikationerne i Unik hostingmiljø bliver godkendt forud for opdatering.	Forespurgt til procedure for test, godkendelse og deployment af ændringer til Advosys og Bolig4. Stikprøvevist inspiceret dokumentation for godkendelse af opdateringer til Advosys og Bolig4 i Unik hostingmiljøet.	Ingen afvigelser konstateret.

Kontrolmål H Der efterleves procedurer og kontrollerer, der sikrer forsvarlig håndtering og afskaffelse af flytbare medier.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
H.1	Der er kontrol, der sikrer, at flytbare medier bortskaffes på forsvarlig vis, når der ikke længere er behov for dem.	Forespurgt, om der er etableret en procedure for bortskaffelse af flytbare medier.	Ingen afvigelser konstateret.
H.2	Det kontrolleres, at databærende medier bliver slettet og destrueret efter aftale.	Inspiceret eksempel på dokumentation for, at data på flytbare medier er fjernet i henhold til aftale.	Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, der sikrer, at der er implementeret passende kryptering, hvor det er en del af aftalen.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
I.1	E-mails, der afsendes fra Unik til de dataansvarlige via Vipre, krypteres med TLS version 1.2.	Inspiceret dokumentation for opsætning af kryptering.	Ingen afvigelser konstateret.
I.2	Adgang til at vedligeholde opsætningen hos Vipre er begrænset til medarbejdere med et arbejdsmæssigt behov.	Inspiceret, at adgang til Vipre er tildelt ud fra et arbejdsmæssigt behov.	Ingen afvigelser konstateret.
I.3	Der anvendes secure FTP-server, når den dataansvarlige overfører kundedatabaser til Unik.	Inspiceret, at der anvendes secure FTP-server ved overførsel af kundedata.	Det er kundernes ansvar at benytte den af Unik etablerede FTP-server, når kunderne sender data til Unik. Ingen afvigelser konstateret.

Kontrolmål J

Der efterleves procedurer og kontrollerer, der sikrer, at databehandleren har implementeret passende sikkerhedsforanstaltninger for kundedata i det outsourcede hostingmiljø.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
J.1	Unik deltager i kvartalsvise Key Account-møder med Sentia. Én gang årligt gennemgås revisorerklæringer fra Sentia vedrørende generelle it-kontroller (ISAE 3402) samt overholdelse af GDPR (ISAE 3000). Én gang årligt gennemgås revisorerklæringer eller lignende fra øvrige kritiske underleverandører.	Inspiceret dokumentation for, at der er gennemgang af de seneste revisorerklæringer fra Sentia vedrørende generelle it-kontroller (ISAE 3402) samt overholdelse af GDPR (ISAE 3000) samt af revisorerklæringer fra Vipre.	Ingen afvigelser konstateret.
J.2	Der tages dagligt sikkerhedskopiering af al væsentlig data i henhold til de indgåede kundeaftaler og interne retningslinjer. Der foretages dagligt kontrol af, at backup er udført som planlagt.	Inspiceret proceduren for daglig kontrol af backup af systemer og data. Stikprøvevis inspiceret dokumentation for, at der er gennemført daglig opfølgning på fejlede backup-jobs.	Ingen afvigelser konstateret.
J.3	Reetablering af backup testes halvårligt eller efter særlig aftale med kunden.	Inspiceret dokumentation for, at der er gennemført restore-test af backup.	Ingen afvigelser konstateret.

5 Ledelseskommentarer til afvigelser i ISAE 3000-erklæring for perioden fra 1. december 2020 - 30. november 2021

Informationen indeholdt i dette afsnit 5 er udarbejdet af Unik System Design A/S for at give yderligere information til Uniks kunder, der anvender løsningerne. Afsnittet er ikke at betragte som en del af systembeskrivelsen i afsnit 3. Oplysningerne i afsnit 5 er ikke omfattet af EY's handlinger, der udføres for at vurdere, om systembeskrivelsen er retvisende, om kontroller, der understøtter de kontrolmål, der er præsenteret i afsnit 4, har været passende udformet, implementeret og operationelt effektive i perioden 1. december 2020 til 30. november 2021. Således omfatter EY's konklusion ikke oplysningerne i afsnit 5.

Kontrolref.	Kontroltekst	Resultat af test	Ledelsens svar
B.1	Adgang til Uniks lokale datacenter er sikret ved nøglebrik eller systemnøgle til medarbejdere med arbejdsmæssigt behov. Der fortages halvårlig kontrol af medarbejdere med adgang til Uniks lokale datacenter.	En enkelt it-medarbejdere har haft adgang til datacentret siden maj 2021 uden at have et permanent arbejdsmæssigt behov. Ingen yderligere afvigelser konstateret	Den pågældende medarbejder var ansat i Intern IT med en jobfunktion, som begrundede permanent adgang. I erklæringsperioden har den pågældende imidlertid fået ny jobfunktion, men assisterer i en overgangsperiode fortsat Intern IT med opgaver, som begrunder adgang på baggrund af et konkret arbejdsmæssigt behov.
B.2	Tildeling af adgang til datacenter kan alene ske efter henvendelse til den administrerende direktør eller økonomichefen.	Foruden økonomichefen har to personer adgang ti systemet, der anvendes til kodning af nøglebrikker. Ingen yderligere afvigelser konstateret.	Der er af Økonomichefen udpeget to personer, som ligeledes har adgang til systemet. Den ene er under direkte instruks af økonomichefen og assisterer bl.a. med tildeling af midlertidige adgange, eksempelvis til håndværkere. Den anden er en medarbejder i Intern IT, som har adgang til systemet med henblik på support og lignende.
B.6	Der er etableret alarm ved forhøjet temperatur samt ved fugt og oversvømmelse i datacentret. Der er desuden etableret aftale om eftersyn af nødstrømsanlæg (UPS) og køleanlæg i datacentret.	Unik har ikke modtaget rapportering vedr. serviceeftersyn og test af alarmer ved forhøjet temperatur samt ved fugt og oversvømmelse i datacentret. Ingen yderligere afvigelser konstateret.	I forlængelse af revisionen har Unik igangsat dialog med alarmleverandøren for fremover at få udvidet aftalen om serviceeftersyn og test med rapportering efter endt serviceeftersyn eller test.
D.2	Brugernes placering i organisatoriske grupper i Active Directory revurderes regelmæssigt til sikring af tildelte adgangsrettigheder	Kontrollen er i 8 ud af 16 tilfælde ikke udført i erklæringsperioden. Ingen yderligere afvigelser konstateret.	I forbindelse med den igangværende fusion har Unik undergået organisatoriske omstruktureringer af divergerende størrelser. Flere af disse er blevet gennemført relativt sent i erklæringsperioden, hvorfor netop denne kontrol blev igangsat senere end tiltænkt, hvilket gav en tilsvarende forsinket gennemførelse.

Kontrolref.	Kontroltekst	Resultat af test	Ledelsens svar
D.3	Der er etableret en formel procedure for oprettelse og nedlæggelse af brugere, der indebærer, at oprettelse og nedlæggelse af brugere skal godkendes. Tildeling og vedligeholdelse af rettigheder sker via en manuel proces på grundlag af en service request. Det er kontrolleret, at nedlæggelse af brugere sker på grundlag af en service request.	Nedlæggelse af brugere er i 4 ud af 35 tilfælde sket, uden at der foreligger en service request. Ingen yderligere afvigelser konstateret.	I forbindelse med revisionen og egne kontroller i relation dertil er Unik blevet opmærksom på, at nedlægning af brugere i visse tilfælde ikke er sket i fuldstændig overensstemmelse med vores procedure. Disse uregelmæssigheder giver derfor anledning til en gennemgang af processen og en afklaring af, hvor der eventuelt er behov for ændringer
D.4	Der foretages halvårlig kontrol af, at privilegerede rettigheder er begrænset til medarbejdere i it-afdelingen samt til eksterne konsulenter med arbejdsmæssigt behov.	En it-medarbejder er tildelt privilegerede adgangsrettigheder ud over et arbejdsmæssigt behov. Ingen yderligere afvigelser konstateret.	Den pågældende medarbejder var ansat i Intern IT med en jobfunktion, som begrundede permanent adgang. I erklæringsperioden har den pågældende imidlertid fået ny jobfunktion, men assisterer i en overgangsperiode fortsat Intern IT med opgaver, som begrunder visse privilegerede adgangsrettigheder på baggrund af et konkret arbejdsmæssigt behov.
G.3	Det interne netværk hos Unik er sikret med en firewall, hvori der kun er åbnet for godkendte porte.	Der er på nuværende tidspunkt ikke etableret en formel proces for administration og ændring af firewall. Der foreligger ikke skriftlig dokumentation for den årlige kontrol af åbne porte i firewall. Ingen yderligere afvigelser konstateret.	Uniks it-medarbejdere, der har adgang til at håndtere portene, gør brug af best practice i forbindelse med håndtering af forespørgsler om portåbninger. I eventuelle tvivlstilfælde vil forespørgslen blive eskaleret til ledelsen i it-afdelingen.

PENNEO

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

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

Jens Jensen Find
Client Signer
På vegne af: Unik System Design A/S
Serienummer: PID:9208-2002-2-569893874189
IP: 194.19.xxx.xxx
2022-02-28 13:10:41 UTC
NEM ID

Per Højmark Dahl
EY Signer
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: PID:9208-2002-2-718537888884
IP: 145.62.xxx.xxx
2022-02-28 15:21:25 UTC
NEM ID

Jesper Due Sørensen
EY Signer
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: PID:9208-2002-2-421950499915
IP: 145.62.xxx.xxx
2022-02-28 15:41:34 UTC
NEM ID