Unik System Design A/S

Uafhængig revisors ISAE 3000-erklæring om kontrolforanstaltninger i henhold til standarddatabehandleraftale
pr. 30. november 2020

Building a better working world

Indhold

1 Ledelsens udtalelse

Unik System Design A/S (Unik) behandler personoplysninger på vegne af Uniks kunder i henhold til softwareløsningerne 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 sektion 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 fungerer effektivt. 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 fungerer effektivt sammen med relaterede kontroller hos Unik. Beskrivelsen omfatter ikke kontrolaktiviteter udført af Uniks kunder.

Unik bekræfter, at:

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

   (I) Redegør for, hvordan aktiviteter og kontroller var udformet 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) 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 udformet pr. 30. november 2020, hvis relevante kontroller hos underleverandører fungerer effektivt, og hvis kunder har udført de komplementerende kontroller, som forudsættes i designet af Uniks kontroller pr. 30. november 2020. 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.

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 22. december 2020

Unik System Design A/S

Jens Find
Adm. direktør

2 Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og tekniske foranstaltninger i henhold til databehandleraftale med Unik System Design A/S' kunder.

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

Omfang

Vi har fået som opgave at afgive erklæring om Unik System Designs (herefter Unik) beskrivelse af Unik Advosys og Unik Bolig i sektion 3 i henhold til behandling af personoplysninger og om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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 fungerer effektivt sammen med relaterede kontroller hos Unik. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Uniks kunder, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos Uniks kunder.

Unik anvender Sentia, som varetager driften af den underliggende infrastruktur til Unik Advosys og Unik Bolig. Beskrivelsen i sektion 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 underleverandørers kontroller, der forudsættes i designet af Uniks kontroller, er passende designet og fungerer effektivt 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 sektion 5 er præsenteret af ledelsen af Unik med henblik på at give supplerende oplysninger og er ikke omfattet af Uniks beskrivelse. Information om Uniks Ledelseskommentarer til afvigelser i erklæringen pr. 30 november 2020 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 sektion 1, 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 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 IESBA's etiske regler, som er baseret på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Uniks beskrivelse samt om udformningen 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 udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse i sektion 3 samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. 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 sektion 1.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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, 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.

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 i afsnit 3 af Unik Advosys og Unik Bolig, således som denne var udformet og implementeret pr. 30. november 2020, 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 pr. 30. november 2020, hvis relevante kontroller hos underleverandører fungerer effektivt, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Uniks kontroller pr. 30. november 2020.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Uniks ydelser, 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.

Aarhus, 22. december 2020
EY Godkendt Revisionspartnerselskab
CVR-nr.: 30 70 02 28

Per Højmark
statsaut. revisor
mne9230

Karsten Hybel
Senior manager, CISA

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 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 Hosting-aftale 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 Hosting vil der derudover være behandlinger, der har karakter af opbevaring og drift for den dataansvarlige.

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, medlemstatus for ansøgere (ind- og udmeldelsesdato, husstandens størrelse, ansøgertype, opnoteringer osv.), oplysninger om lejemål og bi-lejemål og lejemålshistorik, herunder diverse kommunikation med lejer.
- Andre personlige oplysninger, herunder CPR-numre.

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 fortrinsvist den Dataansvarliges ansatte, jobansøgere, praktikanter, klienter, sagsparter, sagsmodparter (tredjemand), vidner, kreditorer og debitorer, arvinger, leverandører og samarbejdspartnere.
- For Unik Bolig:
  - Kredsen af registrerede udgør fortrinsvist 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 tager 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 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 risikorating. 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 én årlig formel awareness-kampagne og 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 (Kontrolaktivitet D.3).

Minimum én gang årligt kontrolleres det, at alle adgange for alle fratrådte medarbejdere er nedlagt korrekt og rettidigt. Der foretages tillige prøvekontrol af, om nuværende medarbejdere har de korrekte adgangsrettigheder (Kontrolaktivitet D.2).

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 D.4 og F.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, hvortil der skal anvendes individuelle nøglebrikker samt systemnøgle (Kontrolaktivitet B.3 og B.4). Det inkluderer ligeledes passende indbrudsalarmer, som serviceres regelmæssigt (Kontrolaktivitet 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 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 D.4og 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 behøver at få 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 passende backup af både Uniks egne servere og også kundeservere i Hosting. Sidstnævnte overvåger Unik gennem daglige rapporter fra Hosting- leverandør (Kontrolaktivitet J.2 og J.3).

Der foretages en årlig penetrationstest på enten det interne miljø eller det outsourcede hostingmiljø. Ekstern, uvildig part har i 2020 gennemført intern penetrationstest on premise hos Unik (Kontrolaktivitet G.4).

Hosting

Unik har defineret reglerne for firewallen i Hosting-miljøet, 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 Hosting-leverandøren. De forskellige kundesystemer er adskilt af VLAN-opdeling, og denne segmentering bliver periodisk testet af en 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 forsat 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 udformning og implementering 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 af implementering har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev nået pr. 30. november 2020.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers udformning og implementering 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.

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	Det kontrolleres, at alle medarbejdere underskriver en fortrolighedsaftale som et led i ansættelsen.	Forespurgt til procedure i forbindelse med ansættelse af nye medarbejdere. Inspiceret eksempel på, at en nyansat medarbejder har underskrevet en fortrolighedsaftale.	Ingen afvigelser konstateret.
A.2	Der gennemføres en eller flere awareness-kampagner i årets løb med emner, der relaterer sig til GDPR og it-sikkerhed	Forespurgt, om databehandleren udbyder awareness-træning til medarbejderne omfattende GDPR og generel it-sikkerhed. Inspiceret eksempler på statistikker over medarbejdernes gennemførelse af kontrolspørgsmål i forbindelse med awareness-træning vedrørende GDPR og generel it-sikkerhed.	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 begrænset til medarbejdere med arbejdsmæssigt behov. Adgang til Uniks lokale datacenter er sikret ved nøglebrik eller systemnøgle.	Inspiceret, at adgang til Uniks lokale datacenter er sikret via nøglebrik. Inspiceret oversigter over personer med nøglebrik og systemnøgle, der giver adgang til Uniks lokale datacenter.	Enkelte it-medarbejdere samt den administrerende direktør har adgang til Uniks lokale datacenter 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.	Ingen 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.	Ingen afvigelser konstateret.
B.4	Fysiske nøgler 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.	Ingen afvigelser konstateret.
B.5	Loggen over adgang til datacenter gennemgås og kontrolleres halvårligt.	Inspiceret, at adgang til datacenter logges og gennemgås halvårligt.	Ingen afvigelser konstateret.
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.	Forespurgt, om der foretages serviceeftersyn og test af alarmer i datacentret. Inspiceret aftale om etablering af serviceaftale omfattende UPS og køleanlæg.	Ingen 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. Inspiceret aftale om etablering af serviceaftale omfattende UPS og køleanlæg.	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 kvalitetspasswords.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
C.1	Håndbog for IT og Persondata foreskriver, at medarbejdernes password er personlige og fortrolige.	Inspiceret Håndbog for IT og Persondata vedrørende beskyttelse af brugernes password.	Ingen afvigelser konstateret.
C.2	Unik har fastsat kvalitetskrav til password og implementeret disse i Active Directory på det interne netværk.	Inspiceret password indstillinger i Active Directory på det interne netværk.	Ingen afvigelser konstateret.
C.3	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger fra et eksternt netværk, er omfattet af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger via eksternt netværk.	Ingen afvigelser konstateret.
C.4	Password til system- og servicekonti opbevares i et system, hvortil adgang er begrænset til udvalgte medarbejdere.	Forespurgt til procedure for tildeling af adgang af password til system- og servicekonti.	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	It-sikkerhedspolitikken foreskriver, at adgangsrettigheder skal begrænses til den enkelte medarbejders henholdsvis den eksterne konsulents arbejdsmæssige behov. Adgangsrettigheder skal godkendes af medarbejderens leder før tildeling.	Inspiceret it-sikkerhedspolitikken vedrørende tildeling af adgangsrettigheder til medarbejdere og eksterne konsulenter. Forespurgt til procedure for tildeling af adgangsrettigheder.	Vi har konstateret, at der på tidspunktet for test ikke foreligger en formel beskrivelse af Uniks håndtering af roller og rettigheder, som håndteres via Active Directory-sikkerhedsgrupper. Ingen yderligere 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.	Ingen 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 af nærmeste leder. Tildeling og vedligeholdelse af rettigheder sker via en manuel proces 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.	Ingen afvigelser konstateret.
D.4	Privilegerede rettigheder er begrænset til medarbejdere i it-afdelingen samt eksterne konsulenter med arbejdsmæssigt behov.	Stikprøvevist inspiceret, at privilegerede adgangsrettigheder er tildelt medarbejdere og eksterne konsulenter med et arbejdsmæssigt behov.	Vi har konstateret, at enkelte medarbejdere, som ikke varetager systemadministrative funktioner, er tildelt systemadministrative rettigheder på det interne netværk. 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.	Inspiceret Uniks Persondatapolitik. Forespurgt til procedurer, der sikrer, behandling af personoplysninger altid gennemføres efter skriftlig instruks.	Ingen afvigelser konstateret.
F.2	Nærværende leder gennemgår liste over medarbejdere, der har adgang til in-house kundedatabaser, og sikrer, at det alene er medarbejdere med arbejdsbetinget behov.	Forespurgt, om der foretages regelmæssig vurdering og godkendelse af tildelte brugeradgange.	Unik har oplyst, at der ikke foretages periodisk opfølgning på brugere og deres rettigheder. Ingen yderligere 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 er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der er installeret antivirussoftware på klienter, der anvendes ved behandling af personoplysninger, samt om antivirussoftware på klienterne er opdateret.	Ingen afvigelser konstateret.
G.2	Patches til systemer og databaser følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer, herunder sikkerhedspatches.	Forespurgt, om der foreligger formaliserede procedurer for håndtering af patches til systemer og databaser. Inspiceret, at systemer og databaser er opdateret med seneste patches.	Ingen afvigelser konstateret.
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 firewallen.	Der er på nuværende tidspunkt ikke etableret en formel proces for administration og ændring af firewallen. Ingen yderligere afvigelser konstateret.
G.4	Der foretages penetrationstest én gang årligt, enten på det outsourcede Hosting-miljø eller på det interne netværk.	Forespurgt, om der foretages årlig penetrationstests. Inspiceret dokumentation for senest gennemførte penetrationstest i juni 2020. Forespurgt, om eventuelle svagheder konstateret i forbindelse med de gennemførte penetrationstest er eller vil blive afhjulpet.	Ingen afvigelser konstateret.
G.5	Der er opsat logning af al tilgang til kundesystemer, der ligger i kundens eget miljø eller i Unik Hosting-miljø, 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 på det Hostede miljø samt på SQL-servere.	Ingen afvigelser konstateret.
G.6	Der er etableret funktionsadskillelse mellem udviklings- og driftsmiljø. Dette er implementeret i en change management-procedure for udvikling samt begrænsning i adgangen til at foretage deployment.	Forespurgt til procedure for test, godkendelse og deployment af ændringer til Advosys og Bolig4. Inspiceret, at der foreligger funktionsadskillelse mellem de forskellige miljøer i forbindelse med udvikling.	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. Inspiceret eksempel på, at det ikke er muligt at sende personfølsomme data via en ikke-krypteret forbindelse.	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.	Ingen afvigelser konstateret.

Kontrolmål J Der efterleves procedurer og kontrollerer, der sikrer, at databehandleren har implementeret passende sikkerhedsforanstaltninger for kundedata i det outsourcede Hosting-miljø.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
J.1	Én gang årligt gennemgås revisorerklæringer fra Sentia vedrørende generelle it-kontroller (ISAE 3402) samt overholdelse af GDPR (ISAE 3000).	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).	Ingen afvigelser konstateret.
J.2	Der tages daglig sikkerhedskopiering af al væsentlig data i henhold til de indgåede kundeaftaler og interne retningslinjer.	Inspiceret proceduren for backup af systemer og data, herunder opsætningen. Inspiceret daglig backuprapport for at sikre, at kundedata er inkluderet i den backup. Inspiceret, at der gennemføres opfølgning på fejlede backupjobs.	Ingen afvigelser konstateret.
J.3	Reetablering af backup testes halvårligt eller efter særlig aftale med kunden.	Inspiceret, at der er gennemført restore-test af backup.	Ingen afvigelser konstateret.

5 Ledelseskommentarer til afvigelser i ISAE 3000-erklæring pr. 30 november 2020

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 og implementeret den 30. november 2020. 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 begrænset til medarbejdere med arbejdsmæssigt behov. Adgang til Uniks lokale datacenter er sikret ved nøglebrik eller systemnøgle.	Enkelte it-medarbejdere samt den administrerende direktør har adgang til Uniks lokale datacenter uden at have et permanent arbejdsmæssigt behov. Ingen yderligere afvigelser konstateret	Unik opbevarer ikke kundedata i eget datacenter, medmindre der er indgået særlig og specifik aftale om brug af anonymiseret data til brug for test og debug. I Uniks eget datacenter er Uniks eget setup, og Unik finder det derfor arbejdsbetinget, at såvel den administrerende direktør som it-medarbejdere har adgang i forbindelse med beredskab, opdateringer, servicevinduer og lignende.
D.1	It-sikkerhedspolitikken foreskriver, at adgangsrettigheder skal begrænses til den enkelte medarbejders henholdsvis den eksterne konsulents arbejdsmæssige behov. Adgangsrettigheder skal godkendes af medarbejderens leder før tildeling.	Vi har konstateret, at der på tidspunktet for test ikke foreligger en formel beskrivelse af Uniks håndtering af roller og rettigheder, som håndteres via Active Directory-sikkerhedsgrupper. Ingen yderligere afvigelser konstateret.	Unik er i gang med et projekt, der skal forbedre den eksisterende tildeling af rettigheder i Uniks it-infrastruktur, udbygge de formelle retningslinjer herfor og sikre, at ingen medarbejdere har adgange udover, hvad der er nødvendigt for, at de kan varetage deres pågældende funktion.
D.4	Privilegerede rettigheder er begrænset til medarbejdere i it-afdelingen samt eksterne konsulenter med arbejdsmæssigt behov.	Enkelte medarbejdere, som ikke varetager systemadministrative funktioner, er tildelt systemadministrative rettigheder på det interne netværk. Ingen yderligere afvigelser konstateret.	I forbindelse med revisionen har Unik fået forelagt en liste over medarbejdere, der har haft privilegeret adgang til de SQL-servere, som revisor har. De pågældende medarbejdere har alene haft privilegerede rettigheder til in-house SQL-servere, og dermed ikke SQL-servere i Unik Hosting. In-house SQL-servere indeholder alene kundedata efter særlig og specifik aftale med kunder og oftest i anonymiseret form. Medarbejdere, der varetager systemudvikling, har efter revisionen fået fjernet privilegerede rettigheder på in-house SQL-servere.

Kontrolref.	Kontroltekst	Resultat af test	Ledelsens svar
F.2	Nærværende leder gennemgår liste over medarbejdere, der har adgang til in-house kundedatabaser, og sikrer, at det alene er medarbejdere med arbejdsbetinget behov.	Unik har oplyst, at der ikke foretages periodisk opfølgning på brugere og deres rettigheder. Ingen yderligere afvigelser konstateret.	Unik har allerede inden revisionen været i gang med et projekt vedrørende dette. Projektet er næsten færdigt, da Unik har implementeret en ændring i det system, der håndterer oversigten over in-house kundedatabaser. Sidste fase er, at nærværende leder får udtræk over medarbejdere, der har adgang til kundedatabaser. Dette forventes gennemført januar 2021.
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 firewallen. Ingen yderligere afvigelser konstateret.	Uniks it-medarbejderne, 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 litafdelingen.