Unik System Design A/S

CVR-nr. 17512692

Uafhængig revisors ISAE 3000 type 1 erklæring om kontrolforanstaltninger i henhold til standarddatabehandleraftale pr. 28. februar 2024

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Building a better working world

Indhold

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

1 Ledelsens udtalelse

Unik System Design A/S (Unik) behandler personoplysninger på vegne af Uniks kunder i henhold til standarddatabehandleraftale.

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 for Unik Hosting samt GlobalConnect til off-site opbevaring af backup. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos Unik og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Sentia og GlobalConnect. 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 er 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 sektion 3 giver en retvisende beskrivelse af Unik Advosys og Unik Bolig, der har behandlet personoplysninger for Uniks kunder pr. d. 28. februar 2024 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 behandlingen 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.

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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 designet og operationelt effektive pr. d. 28. februar 2024, hvis relevante kontroller hos underleverandører var hensigtsmæssigt designet og implementeret, og de dataansvarlige har designet og implementeret de komplementerende kontroller, som forudsættes i designet af Uniks kontroller pr. d. 28. februar 2024. 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 15. marts 2024
Unik System Design A/S

Jens Find
Adm. direktør

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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 Design A/S' (Unik) beskrivelse i sektion 3 af kontrolforanstaltninger i henhold til Unik's standarddatabehandleraftale pr. 28. februar 2024 (beskrivelsen) og om designet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende den operationelle effektivitet 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 kunderne, der forudsættes i designet af Uniks kontroller, er passende designet og implementeret sammen med relaterede kontroller hos Unik. Vores handlinger har ikke omfattet kontrolaktiviteter udført af kunderne, og vi har ikke vurderet egnetheden af design eller implementeringen af kontrolaktiviteter hos kunderne.

Unik anvender Sentia som varetager driften af den underliggende infrastruktur til Unik Hosting samt GlobalConnect til off-site opbevaring af backup. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos Unik og medtager således ikke kontrolmål og relaterede kontroller hos Sentia og GlobalConnect. 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 implementeret sammen med de relaterede kontroller hos Unik. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Sentia og GlobalConnect, og vi har ikke vurderet egnetheden af design eller implementeringen af kontrolaktiviteter hos underleverandører.

Oplysningerne medtaget i afsnit 5, Ledelseskommentarer til afvigelser i ISAE 3000-erklæring pr. 28. februar 2024, 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-erklæring pr. 28. februar 2024 har ikke været omfattet af vores handlinger om Uniks beskrivelse, og vi har ikke vurderet egnetheden af design eller implementeringen af kontrolaktiviteter, og udtrykker derfor ingen konklusion herom.

Uniks ansvar

Unik er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 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 designe, 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 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.

EY Godkendt Revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Uniks beskrivelse samt om design af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og designet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes design. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet.

En erklæringsopgave med sikkerhed af denne type omfatter desuden vurdering af den samlede præsentationen af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål og hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i sektion 1.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet 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.

Begrænsning i kontroller hos en databehandler

Uniks beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold.

Endvidere vil kontroller hos en databehandler, som følge af deres art, muligvis ikke forhindre eller opdage alle brud på 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 sektion 1. Det er vores opfattelse:

(a) at beskrivelsen af kontrolforanstaltningerne, således som disse var designet og implementeret pr. 28. februar 2024, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, der knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet pr. 28. februar, hvis kontroller hos underleverandører og komplementerende kontroller hos kunder var hensigtsmæssigt designet og implementeret pr. 28. februar 2024 som forudsat i designet af Uniks kontroller.

Beskrivelse af test af kontroller

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

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4, er udelukkende tiltænkt de kunder, der har anvendt Uniks systemer Unik Advosys og Unik Bolig i Unik Hosting, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundens egne kontroller, ved opnåelsen af en forståelse af kundernes informationssystemer, der er relevante for regnskabsaflæggelsen.

København, den 15. marts 2024
EY Godkendt Revisionspartnerselskab
CVR- nr. 30 70 02 28

Jesper Due Sørensen
Partner

Nils B. Christiansen
statsaut. revisor
mne34106

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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 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 i Unik Hosting. 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 med 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 onlineforbindelse 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.

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 eller udvalgte sager.

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, medlemsstats for ansøgere (ind- og udmeldelsesdato, husstandens størrelse, ansøgertype, op-noteringer 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 fortrinsvist den Dataansvarliges ansatte, jobansøgere, praktikanter, klienter, sagsparter, sagsmodparter (tredjemand), vidner, kreditorer og debitorer, arvinger, leverandører og samarbejdspartnere.

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

- 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, 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, 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 on-boarding-processen og gennem løbende awareness-træning bliver medarbejderne trænet i behandlingen af persondata (Kontrolaktivitet A.2 og A.3).

Adgang til persondata gives, efter nedskrevet procedure (kontrolaktivitet D.1). 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.2).

Privilegerede brugeradgang tildeles og styres efter nedskrevet procedure. Dernæst skal der være et arbejdsbetinget behov for den privilegerede adgang og adgange gives kun i en tidsbegrænset periode (kontrolaktivitet D.3 og C.2).

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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).

Særlige adgange

I de tilfælde, hvor en kunde specifikt instruerer, at deres database skal behandles internt i Uniks systemer, følges en nedskreven proces (Kontrolaktivitet E.1). 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 til kunders databaser der behandles in-house hos Unik, kontrolleres halvårligt (Kontrolaktivitet E.2).

Ingen normale brugerkonti har privilegerede rettigheder i systemerne. Der er oprettet særskilte brugerkonti med privilegerede rettigheder. Det kontrolleres årligt, at der kun findes privilegerede brugere tilgængelige for medarbejdere, der har et arbejdsbetinget behov for det (Kontrolaktivitet D.3).

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.1-B.2). Det inkluderer ligeledes passende alarmer (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.3 og B.4). Her er desuden etableret alarmering for indbrud samt forhøjet temperatur og fugtighed, som serviceres regelmæssigt (Kontrolaktivitet B.5 og B.6).

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

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

Teknisk sikkerhed

Der er opsat passende tekniske foranstaltninger for at beskytte mod udefrakommende angreb på både servere og klienter (Kontrolaktivitet F.1-F.4).

Der er etableret formel patch management-procedurer for egne systemer og kundesystemer, som Unik driftsafvikler (Kontrolaktivitet F.2). Al tilgang til kundesystemer bliver logget, og loggen monitoreres løbende (Kontrolaktivitet F.4).

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

Unik foretager løbende sårbarhedsscanninger af både det interne miljø og det outsourcede Hosting-miljø (Kontrolaktivitet F.3).

Fjernadgang for medarbejdere er beskyttet af VPN-forbindelse og Multifaktor-authentication (Kontrolaktivitet C.3).

Ved endt kundeophør foretager Unik sletning af Kundens data, som Unik ikke længere er berettiget til at behandle (kontrolaktivitet E.3 og E.4)

Hosting

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 ekstern, uvildig part. Erklæringen omfatter ikke aktiviteter og kontroller hos serviceleverandører.

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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 I.1).

Kryptering

Der er etableret tekniske foranstaltninger, der sikrer kryptering af mailkorrespondance efter Datatilsynets retningslinjer på området. Alle udgående e-mails fra Unik er krypteret med TLS 1.2 eller højere. (Kontrolaktivitet H.1)

Unik stiller en sikker FTP-server til rådighed for Uniks kunder i de tilfælde, hvor der er behov for at sende kundedatabaser til Unik (kontrolaktivitet H.2)

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.
- sikre indholdet af fritekstfelterne ligger indenfor rammerne af databehandleraftalen.
- 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 vedrører
- samt, at benytte den af Unik etablerede FTP-server, når de sender data til Unik.

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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 implementering har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår nedenfor. Eventuelle andre kontrolmål, tilknyttede kontroller og komplementære 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. 28. februar 2024.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design 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.

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

4.3 Resultater af test.

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

Kontrolmål A Der efterleves procedurer og kontroller, der sikrer, at databehandleren har implementeret passende organisatoriske foranstaltninger til sikring af relevant behandlings-sikkerhed.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
A.1	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til relevante procedurer vedrørende informationssikkerhed og databehandling. Informationssikkerhedsansvar for medarbejdere i Unik er specificeret i ansættelsesvilkårene. Ansættelsesvilkår omfatter en fortrolighedsklausul. Ansættelsesvilkår underskrives som en del af ansættelseskontrakten.	Forespurgt til procedure i forbindelse med ansættelse af nye medarbejdere. Inspiceret eksempel på ansættelsesaftale og påset, at ansættelsesaftalen indeholder afsnit vedrørende fortrolighedsaftale.	Ingen afvigelser konstateret.
A.2	Der afholdes månedlige awareness-kurser i GDPR og informationssikkerhed bortset fra juli. Det er et krav at alle medarbejdere i Unik gennemfører den planlagte træning.	Inspiceret dokumentation for at medarbejderne er inviteret til awareness-kursus i januar 2024. Inspiceret procedure for periodisk kontrol af, at medarbejdere gennemfører den planlagte awareness-træning.	Ingen afvigelser konstateret.
A.3	Der foretages kvartalsvis opfølgning på at medarbejderne har gennemført den planlagte træning.	Inspiceret procedure for periodisk kontrol af, at medarbejdere gennemfører den planlagte awareness-træning. 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.
A.4	Der foreligger skriftlige procedurer for håndtering af brud på persondatassikkerheden, herunder ansvarsfordeling, vurdering og rapportering.	Inspiceret Uniks Informationssikkerhedspolitik samt procedure for håndtering af brud på persondatasikkerheden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

A.5	Unik fører en fortegnelse over af behandlingsaktiviteter, som Unik foretager sig. Der foretages løbende – og mindst en gang årligt – vurdering af, om fortegnelsen skal opdateres.	Inspiceret fortegnelse over behandlingsaktiviteter. Inspiceret dokumentation for at fortegnelsen over behandlingsaktiviteter er opdateret i august 2023.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, der sikrer, at databehandleren har implementeret passende fysisk sikkerhed på lokaliteter, hvor der behandles personoplysninger.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
B.1	Al fysisk adgang til Uniks kontorer, lokaler og faciliteter kan kun ske med en unik nøglebrik eller systemnøgle. Uden for normal åbningstid skal der anvendes pinkode sammen med nøglebrikken.	Forespurgt til procedure for tildeling af fysisk adgang til Uniks lokaler. Inspiceret, at adgang til Uniks domicil i Vejle samt til det lokale datacenter i Vejle kun kan opnås ved anvendelse af nøglebrik eller systemnøgle.	Ingen afvigelser konstateret.
B.2	Systemnøgle anvendes til at kunne få adgang til lokationer og aflåste rum på lokationerne i tilfælde af, at alarmsystemer ikke er funktionelle. Systemnøgler tildeles kun relevante medarbejdere. Disse medarbejdere underskriver en fuldmagt ved levering af systemnøglen.	Forespurgt til procedure for tildeling af fysisk adgang til Uniks lokaler. Inspiceret oversigter over udleverede systemnøgler.	Ingen afvigelser konstateret.
B.3	Der er etableret fysisk adgangssikkerhed, så kun autoriserede personer kan opnå fysisk adgang til serverum, hvori der opbevares og behandles personoplysninger. Adgang til datacentrene kontrolleres kvartalsvist.	Forespurgt til procedure for tildeling af fysisk adgang til Uniks datacentre i Vejle og i Aalborg. Inspiceret oversigter over personer med fysisk adgang til Uniks datacentre i Vejle og i Aalborg. Inspiceret dokumentation for kvartalsvis kontrol af personer med fysisk adgang til Uniks datacentre i Vejle og i Aalborg.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Kontrolmål B Der efterleves procedurer og kontroller, der sikrer, at databehandleren har implementeret passende fysisk sikkerhed på lokaliteter, hvor der behandles personoplysninger.			
B.4	Log over medarbejdere med adgang til serverum gennemgås og kontrolleres halvårligt.	Forespurgt til procedure for halvårlig kontrol af log over adgang til serverrum. Inspiceret dokumentation for kontrol af log over adgang til serverrum i november 2023.	Ingen afvigelser konstateret.
B.5	Der er etableret alarm ved forhøjet temperatur samt ved fugt og oversvømmelse i serverrummene.	Inspiceret dokumentation for opsatte temperatur- og fugtalarmer i og ved serverrummene. Inspiceret eksempler på monitorering af temperatur og fugtighed i serverrummene.	Ingen afvigelser konstateret.
B.6	Der er etableret aftale om eftersyn af nødstrømsanlæg (UPS) og køleanlæg i serverrummene.	Inspiceret rapport for serviceeftersyn af nødstrømsanlæg (UPS) og køleanlæg i serverrummet i Vejle dateret 24/10-2023. Inspiceret rapport for serviceeftersyn af køleanlæg i serverrummet i Aalborg dateret 5/9-2023. Inspiceret dokumentation for test af nødstrømsanlæg (UPS) i Aalborg, dateret 4/12-2023.	Ingen afvigelser konstateret.
B.7	Der er etableret indbrudsalarm på Uniks lokationer samt aftale om, at der foretages serviceeftersyn heraf.	Inspiceret dokumentation for etableret indbrudsalarm samt at der er indgået aftale om serviceeftersyn og udrykning ved alarm.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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	Der foreligger skriftlige procedurer som indeholder krav til password for at sikre at alle medarbejdere følger Uniks praksis. Medarbejdere instrueres i at password er personlige og fortrolige.	Inspiceret politik og procedure for anvendelse af password. Stikprøvevist inspiceret systemparametre af betydning for brugernes anvendelse af password.	Ingen afvigelser konstateret.
C.2	Fjernadgang til tredjeparter tildeles af Unik ud fra et arbejdsbetinget behov. Adgangen tildeles i en tidsbegrænset periode. Det kontrolleres kvartalsvis om adgangen har en udløbsdato.	Inspiceret procedure for kontrol af eksterne konsulenter. Inspiceret eksempel på tildeling af tidsbegrænset adgang til en ekstern konsulent. Inspiceret dokumentation for kvartalsvis kontrol af at eksterne konsulenters adgang er tidsbegrænset.	Ingen afvigelser konstateret.
C.3	Fjernadgang for Uniks medarbejdere er beskyttet af VPN-forbindelse og MFA (multifaktor-authentication).	Forespurgt til procedure for opnåelse af ekstern adgang til Uniks systemer. Inspiceret dokumentation for konfiguration af firewall'en, RADIUS serveren samt Azure for så vidt angår VPN og MFA.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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	Der foreligger en skriftlig politik for adgangsstyrring, som indeholder krav til styring af adgangsrettigheder. Der foreligger skriftlige procedurer for registrering og afmelding af brugere for at sikre passende tildeling af adgangsrettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om politikken skal opdateres.	Inspiceret politikker og procedurer for administration af brugere og brugerrettigheder. Inspiceret dokumentation for, at *"Informationssikkerhedspolitikken"* er reviewet og ajourført i august 2023.	Ingen afvigelser konstateret.
D.2	Brugernes placering i organisatoriske grupper i Active Directory revurderes kvartalsvis til sikring af, at de tildelte adgangsrettigheder er arbejdsbetinget.	Inspiceret dokumentation for kvartalsvis kontrol i Vejle, af at brugernes adgangsrettigheder er arbejdsbetinget. Inspiceret dokumentation for kvartalsvis kontrol i Aalborg, af at brugernes adgangsrettigheder er arbejdsbetinget.	Ingen afvigelser konstateret.
D.3	Privilegerede rettigheder er begrænset til medarbejdere samt til eksterne konsulenter med arbejdsmæssige behov. Brugeres privilegerede adgangsrettigheder revurderes kvartalsvis, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret dokumentation for kvartalsvis kontrol i Vejle, af at privilegerede brugeres adgangsrettigheder er arbejdsbetinget. Inspiceret dokumentation for kvartalsvis kontrol i Aalborg, af at privilegerede brugeres adgangsrettigheder er arbejdsbetinget.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Kontrolmål E

Der efterleves procedurer og kontroller, 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
E.1	Unik foretager alene behandling af personoplysninger, når der foreligger en instruks fra dataansvarlig. Der foretages kvartalsvis kontrol af, at behandling af kundedata sker efter instruks fra dataansvarlig.	Stikprøvevist inspiceret databehandleraftaler mellem Unik og 7 udvalgte kunder. Inspiceret dokumentation for kvartalsvis kontrol af aftalegrundlag for kundedatabaser udført i februar 2024.	Ingen afvigelser konstateret.
E.2	Unik foretager kvartalsvis kontrol af at adgange til in-house kundedatabaser er tildelt medarbejdere med et arbejdsbetinget behov.	Inspiceret dokumentation for kvartalsvis kontrol af medarbejdere med adgang til in-house kundedatabaser udført i januar 2024.	Ingen afvigelser konstateret.
E.3	Unik foretager kvartalsvis kontrol af at in-house kundedatabaser slettes efter ophør af instruks.	Inspiceret dokumentation for kvartalsvis kontrol af at in-house kundedatabaser er slettet efter ophør af instruks.	Ingen afvigelser konstateret.
E.4	Unik sletter kundedata senest 90 dage efter databehandleraftalens ophør. For kunder hvis data er placeret i Unik Hosting, foretager Unik i Vejle kvartalsvis kontrol af at kundedata er slettet rettidigt. For kunder hvis data er placeret i Uniks datacenter i Aalborg foretager Unik i Aalborg halvårlig kontrol af at kundedata er slettet rettidigt.	Forespurgt til procedurer for håndtering af kundedata når en databehandleraftale ophører. Inspiceret dokumentation for kvartalsvis kontrol, udført den 11. oktober 2023, af at kundedata, der var placeret i Unik Hosting, er slettet rettidigt. Inspiceret dokumentation for halvårlig kontrol, udført 24. august 2023, af at kundedata, der var placeret i Uniks datacenter i Aalborg, er slettet rettidigt.	1 kundedatabase, der var placeret i Uniks datacenter i Aalborg, er slettet 67 dage for sent. 1 kundedatabase, der var placeret i Uniks datacenter i Aalborg, er slettet uden at det er registreret hvornår databasen er slettet. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Kontrolmål F

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
F.1	Der foretages kvartalsvis kontrol af at servere og klienter, der anvendes til behandling af personoplysninger, er beskyttet med antivirus system der løbende opdateres.	Inspiceret dokumentation for kvartalsvis kontrol af, at servere og klienter, der anvendes til behandling af personoplysninger, er beskyttet med antivirus system, der løbende opdateres.	Ingen afvigelser konstateret.
F.2	Microsoft patches frigives første tirsdag i måneden og installeres den første søndag i måneden i løbet af tre måneder. Det foretages månedlig kontrol af, at opdateringerne er gennemført planmæssigt.	Stikprøvevist inspiceret dokumentation for månedlig kontrol af patchning af servere i det hostede miljø.	Ingen afvigelser konstateret.
F.3	Der foretages ugentlige sårbarhedsscanninger af hosting-miljøet samt af Uniks interne netværk.	Stikprøvevist inspiceret dokumentation for sårbarhedsscanning af Uniks Hosting miljø, udført den 9. august 2023. Stikprøvevist inspiceret dokumentation for sårbarhedsscanning af Uniks interne netværk, udført den 16. august 2023.	Det er oplyst at der ikke er etableret en procedure for at følge op på eventuelle konstaterede sårbarheder. De testede sårbarhedsscanninger af Uniks interne netværk viste flere kritiske sårbarheder bl.a. på grund af systemer som havde overskredet end-of-life og ikke længere ville blive opdateret af leverandøren. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
F.4	Unik kontrollerer halvårligt at adgang til kundesystemer på Uniks lokation i Aalborg logges. Unik kontrollerer kvartalsvist at adgang via Remote Desktop Manager til kundernes eget miljø ligeledes bliver logget.	Forespurgt til procedure for logning af brugeraktiviteter i systemer, der anvendes til behandling af personoplysninger, herunder logning af adgang til kundernes eget miljø. Stikprøvevist inspiceret dokumentation for halvårlig kontrol af at adgang til kundesystemer på Uniks lokation i Aalborg logges. Stikprøvevist inspiceret dokumentation for halvårlig kontrol af at adgang til kundernes eget miljø ligeledes bliver logget.	Ingen afvigelser konstateret.

Kontrolmål G
Der efterleves procedurer og kontroller, der sikrer forsvarlig håndtering og afskaffelse af flytbare medier.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
G.1	Der foreligger skriftlige procedurer for bortskaffelse af IT-udstyr, der sikrer, at bortskaffelse sker på forsvarlig vis, og at data slettes og destrueres efter aftale.	Inspiceret procedure for håndtering af it-udstyr der enten skal skrottes eller videresælges. Stikprøvevist inspiceret dokumentation for kvartalsvis afstemning mellem Uniks egne registreringer af skrottet it-udstyr og liste over skrottet it-udstyr, skrottet af leverandøren Ping-IT.	Unik registrerer ikke databærende mobile enheder, der udleveres til Ping-IT med henblik på skrotning. Ingen yderligere afvigelser konstateret.

Kontrolmål H
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
H.1	E-mails, der afsendes fra Unik krypteres med TLS.	Inspiceret dokumentation for opsætning af kryptering.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Kontrolmål H 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**
	Det kontrolleres én gang årligt at alle udgående e-mails er krypteret med TLS 1.2 eller højere.	Inspiceret dokumentation for årlig kontrol af at udgående e-mails er krypteret med TLS 1.2 eller højere.	
H.2	Der stilles en sikker FTP-server til rådighed for den Dataansvarlige til overførsel af kundedatabaser til Unik. Det kontrolleres én gang årligt at FTP-serveren er konfigureret med krav om anvendelse af en sikker forbindelse.	Inspiceret dokumentation for, at FTP-serveren er konfigureret med krav om anvendelse af en sikker forbindelse.	Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, der sikrer, at databehandleren har implementeret passende sikkerhedsforanstaltninger for kundedata i det outsourcede hostingmiljø.			
Nr.	**Databehandlerens kontrolaktivitet**	**Revisors udførte test**	**Resultatet af revisors test**
I.1	På baggrund af en risikovurdering udføres der løbende – og mindst en gang årligt – en opfølgning på den enkelte leverandør i form af gennemgang af revisionserklæringer.	Inspiceret dokumentation for, at der er foretage gennemgang og vurdering af de seneste ISAE 3000 og ISAE 3402 revisorerklæringer fra Sentia samt GlobalConnect.	Ingen afvigelser konstateret.
I.2	Der tages daglig sikkerhedskopiering af al væsentligt data i henhold til de indgåede kundeaftaler og interne retningslinjer. Det kontrolleres dagligt, at backup er udført som planlagt.	Inspiceret proceduren for daglig kontrol af backup af systemer og data. Stikprøvevist inspiceret dokumentation for, at der er gennemført daglig opfølgning på fejlede backupjobs.	Ingen afvigelser konstateret.
I.3	Reetablering af backuptest testes regelmæssigt eller efter særskilt aftale med kunden.	Inspiceret dokumentation for, at der er gennemført en restore-test af backup.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Kontrolmål I

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultatet af revisors test
I.4	Unik anvender kun underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige. Uniks standard-databehandleraftale opdateres når der foretages ændringer i forhold til underdatabehandlere.	Inspiceret at Uniks standard-databehandleraftale er opdateret i forhold til Vipre, der kan tilkøbes til at kryptere e-mails samt GlobalConnect, der anvendes til off-site storage af backup.	Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

5 Ledelseskommentarer til afvigelser i ISAE 3000-erklæring pr. 28. februar 2024

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 pr. 28. februar 2024. Således omfatter EY's konklusion ikke oplysningerne i afsnit 5.

Kontrolref.	Kontroltekst	Resultat af test	Ledelsens svar
C.1	Der foreligger skriftlige procedurer som indeholder krav til password for at sikre at alle medarbejdere følger Uniks praksis. Medarbejdere instrueres i at password er personlige og fortrolige.	Password politikkens krav til at brugernes password skal indeholde store og små bogstaver er ikke implementeret i Active Directory for PC-desktop og Windows domæne brugere. Ingen yderligere afvigelser konstateret.	Det lokale Active Directory er synkroniseret med Azure Active Directory, hvor der er enforced både en generel og en specifik liste over "banned passwords" samt krav om passwords med små og store bogstaver.
E.4	Unik sletter kundedata senest 90 dage efter databehandleraftalens ophør. For kunder hvis data er placeret i Unik Hosting, foretager Unik i Vejle kvartalsvis kontrol af at kundedata er slettet rettidigt. For kunder hvis data er placeret i Uniks datacenter i Aalborg foretager Unik i Aalborg halvårlig kontrol af at kundedata er slettet rettidigt.	1 kundedatabase, der var placeret i Uniks datacenter i Aalborg, er slettet 67 dage for sent. 1 kundedatabase, der var placeret i Uniks datacenter i Aalborg, er slettet uden at det er registreret hvornår databasen er slettet. Ingen yderligere afvigelser konstateret.	Sletteprocesser er indskærpet for relevante medarbejdere.
F.3	Der foretages ugentlige sårbarhedsscanninger af hosting-miljøet samt af Uniks interne netværk.	Det er oplyst at der ikke er etableret en procedure for at følge op på eventuelle konstaterede sårbarheder. De testede sårbarhedsscanninger af Uniks interne netværk viste flere kritiske sårbarheder bl.a. på grund af systemer som havde overskredet end-of-life og ikke længere ville blive opdateret af leverandøren. Ingen yderligere afvigelser konstateret.	Der er ikke etableret formelle procedurer for opfølgning på konstaterede sårbarheder. De konstaterede kritiske sårbarheder i systemer med overskredet end-of-life drejer sig alene om testsystemer.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Kontrolref.	Kontroltekst	Resultat af test	Ledelsens svar
G.1	Der foreligger skriftlige procedurer for bortskaffelse af IT-udstyr, der sikrer, at bortskaffelse sker på forsvarlig vis, og at data slettes og destrueres efter aftale.	Unik registrerer ikke databærende mobile enheder, der udleveres til Ping-IT med henblik på skrotning. Ingen yderligere afvigelser konstateret.	Mobiltelefoner og USB-enheder slettes i alle tilfælde internt inden udlevering til skrotning.

Penneo dokumentnøgle: K50XV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

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
Adm. direktør
På vegne af: Unik System Design A/S
Serienummer: d91ee1b4-c5d4-4873-ac07-b3d53dcce46e
IP: 194.192.xxx.xxx
2024-03-18 08:30:41 UTC

Jesper Due Sørensen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3
IP: 80.208.xxx.xxx
2024-03-18 08:43:30 UTC

Nils Bonde Christiansen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1
IP: 165.225.xxx.xxx
2024-03-18 09:23:59 UTC

Penneo dokumentnøgle: K5OXV-0T3AU-KLLES-LFXA3-BB5WK-CI2IH

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>.** Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**