DELTAPLAN APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 30. OKTOBER 2020 OM BESKRIVELSEN AF DELTAPLAN-SYSTEMET OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING 2

2. DELTAPLAN APS' UDTALELSE 4

3. DELTAPLAN APS' BESKRIVELSE 6

DELTAPLAN ApS 6

DELTAPLAN online vagtplan og behandling af personoplysninger 6

Styring af persondatasikkerhed 6

Risikovurdering 7

Tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller 7

Kundens egne kontroller og ansvar 11

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST 12

Artikel 28, stk. 1: Databehandlerens garantier 14

Artikel 28, stk. 3: Databehandleraftale 15

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger 17

Artikel 28, stk. 2 og 4: Underdatabehandlere 18

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt 20

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger 21

Artikel 25: Databeskyttelse gennem design og standardindstillinger 28

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger 30

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige 31

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter 32

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden 33

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 30. OKTOBER 2020 OM BESKRIVELSEN AF DELTAPLAN-SYSTEMET OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Deltaplan ApS
Deltaplan ApS' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Deltaplan ApS (databehandleren) pr. 30. oktober 2020 udarbejdede beskrivelse i sektion 3 af DELTAPLAN-systemet og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige 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.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme og implementere kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i overensstemmelse med de internationale etiske regler for revisorer (IESBA's Etiske regler), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vi er underlagt den internationale standard om kvalitetsstyring ISQC 1, og vi anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

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

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

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 samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens

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 kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

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.

Begrænsninger i kontroller hos en databehandler

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af Deltaplan-systemet, som hver enkelt dataansvarlig 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 databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af DELTAPLAN-systemet og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 30. oktober 2020, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 30. oktober 2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens Deltaplan-systemet, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 13. januar 2021

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. DELTAPLAN APS' UDTALELSE

DELTAPLAN ApS varetager behandling af personoplysninger i forbindelse med DELTAPLAN online vagtplan for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt DELTAPLAN online vagtplan, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller), som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

DELTAPLAN ApS anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

DELTAPLAN ApS bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af DELTAPLAN online vagtplan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger (kontroller) pr. den 30. oktober 2019. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for DELTAPLAN-systemet, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - De processer der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
    - De processer der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
    - De processer der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger 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.
    - De kontroller, som med henvisning til afgrænsningen af DELTAPLAN online vagtplan har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.
2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af DELTAPLAN online vagtplan og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov

hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved DELTAPLAN online vagtplan, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

Deltaplan ApS bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 30. oktober 2020. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. 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.

DELTAPLAN ApS bekræfter, at der er implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Aarhus, den 13. januar 2021

DELTAPLAN ApS

Jørn Korsgård Nielsen
FFA

3. DELTAPLAN APS' BESKRIVELSE

Beskrivelse af DELTAPLAN ApS & DELTAPLAN online vagtplan

DELTAPLAN APS

DELTAPLAN ApS (herefter DELTAPLAN) er en 100% danskejet virksomhed, som udvikler og driver onlinesystemet DELTAPLAN online vagtplan. DELTAPLAN har til huse i Århus og har fastansatte medarbejdere, som arbejder specialiseret indenfor henholdsvis ledelse/salg/markedsføring/sikkerhed, it-udvikling og support/service.

DELTAPLANs ledelse varetager virksomhedens persondatasikkerhed, herunder indgåelse af databehandleraftaler, besvarelse af henvendelser fra dataansvarlige, underretning om brud på sikkerheden, efterlevelse af interne politikker, procedurer og lignende.

DELTAPLAN ONLINE VAGTPLAN OG BEHANDLING AF PERSONOPLYSNINGER

DELTAPLAN online vagtplan er en SaaS løsning til private og offentlige arbejdspladser og består af en web-applikation samt en mobil-applikation (iPhone & Android).

DELTAPLAN online vagtplan er udviklet af DELTAPLAN og afvikles fra hostingcenter i Danmark.

Formålet med DELTAPLAN online vagtplan er vagtplanlægning, kommunikation og afregning til løn.

Der benyttes underdatabehandlere til infrastruktur hosting samt sms & e-mail gateway. DELTAPLAN har indgået databehandleraftaler med alle underdatabehandlere.

DELTAPLAN behandler personoplysninger på vegne af DELTAPLANs kunder, der er dataansvarlige, når disse anvender DELTAPLAN online vagtplan. DELTAPLAN har indgået databehandleraftaler med de dataansvarlige om denne behandling.

DELTAPLAN behandler følgende personoplysninger - Navn, adresse, telefon, e-mail, cpr.nr, bankoplysninger, billede og lønoplysninger.

STYRING AF PERSONDATASIKKERHED

DELTAPLAN har etableret sikkerhedsforanstaltninger samt system til kontrol af disse.

Dette har til hensigt at beskytte de registreredes personoplysninger og derved sikre overholdelsen af databeskyttelsesforordningen og databeskyttelsesloven.

Kontrollen af sikkerhedsforanstaltningerne er opdelt i:
- Tilfældige kontroller
- Månedlige kontroller
- Årlige kontroller

Sikkerhedsforanstaltningerne og kontrollen af disse er etableret på baggrund af en risikovurdering, jf. nedenfor.

Sikkerhedsforanstaltningerne er dels manuelle, dels automatiseret, hvor dette er muligt.

Der er indlagt en dynamisk vedligeholdelse/udvikling af sikkerhedsforanstaltningerne samt kontrollen af disse, som sikrer, at disse løbende ændres i overensstemmelse med, at DELTAPLAN online vagtplan, lovgivningen samt verden i sin helhed ændrer sig.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter:

ARTIKEL	OMRÅDE
Artikel 28, stk. 1	Databehandlerens garantier
Artikel 28, stk. 3	Databehandleraftale
Artikel 28, stk. 3, litra a og h, og stk. 10 Artikel 29 Artikel 32, stk. 4	Instruks for behandling af personoplysninger
Artikel 28, stk. 2 og 4	Underdatabehandlere
Artikel 28. stk. 3, litra b	Fortrolighed og lovbestemt tavshedspligt
Artikel 28, stk. 3, litra c	Tekniske og organisatoriske sikkerhedsforanstaltninger
Artikel 25	Databeskyttelse gennem design og standardindstillinger.
Artikel 28, stk. 3, litra g	Sletning og tilbagelevering af personoplysninger
Artikel 28, stk. 3, litra e, f og h	Bistand til den dataansvarlige
Artikel 30, stk. 2, 3 og 4	Fortegnelse over kategorier af behandlingsaktiviteter
Artikel 33, stk. 2	Underretning om brud på persondatasikkerheden.

RISIKOVURDERING

DELTAPLAN udfører en årlig risikoanalyse med henblik på at klarlægge risici i forbindelse med databehandlingen.

I forhold til de registrerede personoplysningers hændelige eller ulovlige tilintetgørelse, tab, ændring eller uautoriseret videregivelse kategoriseres de fundne risici i forhold til, hvor sandsynlige disse ér, samt hvor alvorlige konsekvenser det vil have, hvis risikoen ikke længere er en risiko, men en realitet!

Ud fra dette etableres passende tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af de registreredes data.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

Databehandlerens garantier

DELTAPLAN har indført politikker og procedurer, der sikrer, at der kan gennemføres passende tekniske og organisatoriske sikkerhedsforanstaltninger således at behandling af data opfylder kravene for beskyttelse af de registreredes data, samt at lov og forordning overholdes.

DELTAPLAN har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik og databeskyttelsespolitik, der løbende gennemgås og opdateres.

Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for uddannelse og instruktion af medarbejdere, der behandler personoplysninger, herunder gennemførelse af løbende oplysning til medarbejderne.

Databehandleraftale

DELTAPLAN har indført automatik for indgåelse af en generel databehandleraftale i forbindelse med oprettelse af nye abonnementer på DELTAPLAN online vagtplan til kunder/dataansvarlige. DELTAPLANs generelle databehandleraftale angiver betingelserne for behandling af personoplysninger på vegne af den dataansvarlige samt brugen af underdatabehandlere. Databehandleraftalerne underskrives digitalt. Dokumentation for dette opbevares ligeledes digitalt.

Instruks for behandling af personoplysninger

DELTAPLAN har indført politikker og procedurer, der sikrer, at DELTAPLAN handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske, herunder hvem der hos den dataansvarlige kan give bindende instruks til DELTAPLAN. Proceduren sikrer desuden, at DELTAPLAN informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

DELTAPLANs medarbejdere er instrueret i, at det er den dataansvarlige og kun den dataansvarlige der må indtaste, ændre og slette persondata.

Underdatabehandlere

DELTAPLAN har indgået databehandleraftaler med alle underleverandører, som sikrer, at underdatabehandlerne er pålagt de samme databeskyttelsesforpligtelser som anført i databehandleraftalen mellem dataansvarlige og DELTAPLAN. DELTAPLAN har procedurer for årligt tilsyn med underdatabehandlere.

Fortrolighed og lovbestemt tavshedspligt

Alle medarbejdere i DELTAPLAN har forpligtet sig til fortrolighed. Dette sker ved underskrift dels af ansættelseskontrakt, dels af DELTAPLANs interne IT- & Databeskyttelsespolitik.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering

DELTAPLAN har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici målt i forhold til sandsynlighed, konsekvens og vægtet risiko.

Beredskabsplan

DELTAPLAN har etableret en detaljeret beredskabsplan i tilfælde af brud (eller formodet brud) på datasikkerheden. Beredskabsplanen ligger fysisk tilgængelig for personalet.

DELTAPLAN har desuden etableret en detaljeret beredskabsplan i tilfælde af fuld eller delvis gendannelse af data fra backup.

Håndtering af inddata- og uddatamaterialer

DELTAPLANs medarbejdere er instrueret i forsvarlig håndtering af ind- og uddata - både digitale data og printede data.

Opbevaring af personoplysninger

DELTAPLAN har indført procedurer, der sikrer, at opbevaring af personoplysninger alene foretages i overensstemmelse med DELTAPLANs generelle forretningsbetingelser samt listen over lokationer i den tilhørende databehandleraftale.

Fysisk adgangskontrol

DELTAPLAN har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne. Gæster ledsages.

Logisk adgangssikkerhed

DELTAPLAN har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Brugere oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder sker ud fra et arbejdsbetinget behov.

Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger "Best practice" for en sikker logisk adgangskontrol.

Fjernarbejdspladser og fjernadgang til systemer og data
I tilfælde hvor DELTAPLANs medarbejdere anvender fjernarbejdspladser, er der indført procedure, som sikrer, at der altid arbejdes gennem VPN ved kontakt til eksterne netværk (inkl. internet) og computere.

Eksterne kommunikationsforbindelser
DELTAPLAN har indført procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med stærk kryptering, og at e-mail anvender TLS.

Kryptering af personoplysninger
DELTAPLAN har indført procedurer, der sikrer, at data, som indeholder personoplysninger, og som opbevares på databaser, er krypteret, hvis dette er påkrævet. Den kryptering, der anvendes, vurderes løbende i forhold til det aktuelle trusselsniveau.

Firewall
DELTAPLAN har indført procedurer, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Netværkssikkerhed
DELTAPLAN har indført procedurer, der sikrer, at netværket er opdelt i internt- og gæstenetværk, der ikke har forbindelse med hinanden. Det kræver således special autorisation at få adgang til DELTAPLANs interne netværk.

Antivirusprogram
DELTAPLAN har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware, samt at beskyttelsen løbende kontrolleres og opdateres.

Sårbarhedsscanning og penetrationstest
DELTAPLAN har indført procedurer, der sikrer, at applikationer, infrastruktur og systemer testes for sårbarheder.

Backup og opbevaring
DELTAPLAN har indført procedure, der sikrer, at systemer og data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation. Sikkerhedskopier er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde, eller at sikkerhedskopier ødelægges ved brand, vand, hærværk eller hændelig skade.

Vedligeholdelse af systemsoftware
DELTAPLAN har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og software installeret på servere og arbejdsstationer.

Logning i systemer, databaser og netværk
DELTAPLAN har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau.

Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret mod tab og sletning.

Overvågning
DELTAPLAN har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Reparation og service samt bortskaffelse af it-udstyr
DELTAPLAN har indført procedurer, der sikrer, at udstyr, som udleveres til tredjemand for service, reparation eller bortskaffelse, udleveres uden datadiske, og at brugte og kasserede datamedier og diske registreres og destrueres, så data ikke kan gendannes.

Databeskyttelse gennem design og standardindstillinger
DELTAPLAN har indført politikker og procedurer for udvikling og vedligeholdelse af DELTAPLAN online vagtplan, hvor der anvendes Change Management systemer, hvilket sikrer en styret udviklingsproces.

Udviklings-, test- og produktionsmiljø er adskilt, og der er funktionsadskillelse mellem medarbejdere i udviklingsafdelingen og i drifts- og supportafdelingen. Enhver udviklings- og ændringsopgave gennemløber et testforløb, og der anvendes anonymiserede produktionsdata som testdata. Der er indført procedurer for versionskontrol, logning og sikkerhedskopiering, så det er muligt - ved fejlbehæftede udgivelser - at lave en roll-back til sidste duelige version.

Sletning og tilbagelevering af personoplysninger
DELTAPLAN har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Bistand til den dataansvarlige
DELTAPLAN har indført politikker og procedurer, der sikrer, at DELTAPLAN kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

DELTAPLAN har indført politikker og procedurer, der sikrer, at DELTAPLAN kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 34-36 om konsekvensanalyser.

DELTAPLAN har indført politikker og procedurer, der sikrer, at DELTAPLAN kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige. DELTAPLAN giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

Underretning om brud på persondatasikkerheden
DELTAPLAN har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at DELTAPLAN er blevet opmærksom på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at vurdere, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

Fortegnelse over kategorier af behandlingsaktiviteter

DELTAPLAN har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden på anmodning.

KUNDENS EGNE KONTROLLER OG ANSVAR

Den dataansvarlige er forpligtet til at sikre følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed opfylde databeskyttelseslovgivningen:

- Den dataansvarlige er ansvarlig for at sikre, at personoplysninger, som de registrerer i DELTAPLAN online vagtplan, er ajourførte.
- Den dataansvarlige er ansvarlig for at sikre, at den instruks, der er givet til DELTAPLAN, er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering.
- Den dataansvarlige er ansvarlig for at sikre, at der ikke sker registrering af følgende særlige kategorier af personoplysninger, herunder
  - Oplysninger om race eller etnisk oprindelse
  - Politisk, religiøs eller filosofisk
  - Fagforeningsmæssigt tilhørsforhold
  - Helbredsoplysninger
  - Oplysninger om seksuelle forhold og orientering
  - Oplysninger om strafbare forhold
  - Generiske og biometriske forhold
- Den dataansvarlige er ansvarlig for at sikre, at instruksen givet til DELTAPLAN er hensigtsmæssig set i forhold til databehandleraftalen og hovedydelsen.
- Den dataansvarlige er ansvarlig for at sikre, at den dataansvarliges brugere i DELTAPLAN online vagtplan er ajourførte.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i DELTAPLAN ApS beskrivelse af DELTAPLAN-systemet samt for udformningen af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

BDO's test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af DELTAPLAN ApS, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 30. oktober 2020.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion og observation.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.

For de ydelser, som team.blue Denmark A/S (tidligere Zitcom A/S) leverer inden for hosting af infrastruktur har vi fra uafhængig revisor modtaget en ISAE 3402 type 2-erklæring om generelle it-kontroller relateret til hostingydelser for perioden fra 1. januar til 31. december 2019.

For de ydelser, som Peytz & Co leverer inden for e-mail-services, har vi ikke modtaget dokumentation for deres efterlevelse af den indgåede databehandleraftale.

For de ydelser, som Compaya A/S leverer inden for SMS-services, har vi modtaget en ISAE 3000 erklæring pr. 30. april 2020 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i DELTAPLAN ApS' beskrivelse af kontrolmiljøet. Vi har således alene vurderet erklæringer og udtalelse og testet de kontroller hos DELTAPLAN ApS, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlernes opfyldelse af den mellem den pågældende underdatabehandler og DELTAPLAN ApS indgåede databehandleraftale samt opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

Resultatet af de udførte test af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet eller implementeret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Informationssikkerhedspolitik ▶ DELTAPLAN ApS har udarbejdet og implementeret en informationssikkerhedspolitik samt tilhørende procedurebilag, der er godkendt af ledelsen. ▶ DELTAPLAN ApS har udarbejdet og implementeret en databeskyttelsespolitik. ▶ DELTAPLAN ApS politikker bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret databehandlerens IT- og databeskyttelsespolitik, som alle medarbejdere er forpligtet til at underskrive. Vi har inspiceret og observeret, at den senest er blevet gennemgået, opdateret og godkendt i 5. maj 2020.	Ingen afvigelser konstateret.
Rekruttering af medarbejdere ▶ DELTAPLAN ApS har en styret proces ved ansættelse af medarbejdere, der sikrer, at medarbejdere har de nødvendige kvalifikationer inden ansættelse.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har observeret, at den administrerende direktør ansætter og afskediger personligt alle medarbejdere, og at ansættelse sker ud fra kvalifikationer. Vi har foretaget inspektion af ansættelseskontrakt. Vi har observeret, at medarbejdere skal erklære sig ustraffede, og at indhentelse af straffeattest sker i tvivlstilfælde.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere ▶ DELTAPLAN ApS har procedurer, der skal sikre vedligeholdelse af medarbejdernes kendskab til regler for behandling af personoplysninger og it-sikkerhed.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af DELTAPLAN ApS' IT- og databeskyttelsespolitik, hvoraf fremgår, at nye medarbejdere gøres bekendt med interne retningslinjer og behandling af personoplysninger. VI har observeret, at medarbejdere, efter ændringer i politikkerne, skal genbekræfte kendskabet.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier

Kontrolmål

- *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af underskrevne IT- og databeskyttelsespolitik, informationer på intranet og mødereferat fra statusmøde.	

Artikel 28, stk. 3: Databehandleraftale

Kontrolmål

- *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige - DELTAPLAN ApS har udarbejdet en databehandleraftaleskabelon for indgåelse af databehandleraftaler. - Databehandleraftale skal indgås inden databehandlingen kan igangsættes. - DELTAPLAN ApS vedligeholder en oversigt over indhold af databehandleraftale, herunder hvorvidt der er indgået individuelle databehandleraftaler. - DELTAPLAN ApS ajourfører den dataansvarlige, hvis der anvendes, eller sker ændringer i anvendelsen af, underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af DELTAPLAN ApS' skabelon for databehandleraftale og forretningsbetingelser. Vi har observeret, at skabelon for databehandleraftale og forretningsbetingelserne opfylder kravene til indholdet af en databehandleraftale i henhold til databeskyttelsesforordningens artikel 28, stk. 3. Vi har foretaget inspektion af DELTAPLAN ApS oversigt over indgåede databehandleraftaler med dataansvarlige. Vi har observeret: • at databehandleraftalerne følger skabelon for databehandleraftale. • at databehandlingen ikke kan igangsættes, før databehandleraftalen er accepteret af den dataansvarlige. • at DELTAPLAN ApS anvender en oversigt over indhold af databehandleraftale.	Ingen afvigelser konstateret.

Artikel 28, stk. 3: Databehandleraftale		
Kontrolmål ▶ *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	• at databehandleraftalerne er underskrevet af begge parter og opbevares elektronisk. • at databehandleraftalerne indeholder en instruks fra den dataansvarlige om, at DELTAPLAN ApS skal ajourføre den dataansvarlige ved anvendelse af, eller ændringer i anvendelsen af, underdatabehandlere.	

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* ▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Instruks for behandling af personoplysninger ▶ DELTAPLAN ApS har udarbejdet en informationssikkerhedspolitik og databeskyttelsespolitik, som beskriver de krav, der stilles til DELTAPLAN ApS og dennes personale som databehandler. ▶ DELTAPLAN ApS' skabelon for databehandleraftale indeholder instruks for databehandlingen.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af DELTAPLAN ApS' IT- og databeskyttelsespolitik. Vi har observeret, at instruks fra databehandleraftaler med dataansvarlige er implementeret heri. Vi har foretaget inspektion af udvalgte databehandleraftaler og observeret, at databehandleraftalerne indeholder instruks fra dataansvarlige, som er implementeret i DELTAPLAN ApS' databeskyttelsespolitik.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ DELTAPLAN ApS indhenter og gennemgår instruks fra dataansvarlige i forbindelse med indgåelse af databehandleraftalen. ▶ DELTAPLAN ApS følger den indhentede instruks ved enhver behandling af personoplysninger på vegne af den data ansvarlige.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret udvalgte databehandleraftaler og observeret, at der foreligger en instruks i de indgåede databehandleraftaler. Vi har observeret, at DELTAPLAN ApS har udarbejdet procedurer for efterlevelse af instruks.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks ▶ DELTAPLAN ApS gennemgår instrukser fra den dataansvarlige og underretter denne, hvis instruksen er i strid med lovgivningen.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret standarddatabehandleraftalen. Vi har fået oplyst, at DELTAPLAN ApS underretter den dataansvarlige ved indhentelse af instruks i tilfælde af, at denne strider mod lovgivningen. Der er endnu ikke indhentet databehandleraftale med ulovlig instruks, hvorfor vi ikke har testet procedurens implementering.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ DELTAPLAN ApS har indgået databehandleraftaler med underdatabehandler. ▶ Underdatabehandleren pålægges de samme databeskyttelsesretlige forpligtelser, som DELTAPLAN ApS er pålagt af de dataansvarlige. ▶ Databehandleraftalen underskrives af begge parter og gemmes elektronisk.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret databehandleraftaler indgået med DELTAPLAN ApS' underdatabehandlere team.blue. Danmark A/S (Wannafind), Compaya A/S og Peytz & Co. Vi har observeret, at disse er underskrevet og er opbevaret elektronisk.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Underdatabehandlere skal fremgå af databehandleraftalerne og godkendes af dataansvarlige.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret proceduren for indgåelse af databehandleraftaler samt procedure for godkendelse af ændringer i forretningsbetingelser og databehandleraftale. Vi har inspiceret databehandleraftaler med DELTAPLAN ApS' kunder og har observeret, at underdatabehandlere er angivet.	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere ▶ Ændringer til databehandleraftaler skal godkendes af de dataansvarlige.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret proceduren for godkendelse af ændringer i forretningsbetingelser og databehandleraftale. Vi har observeret, at der foreligger godkendelse af anvendelsen af underdatabehandlere.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere		
Kontrolmål ▶ *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.* ▶ *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.* ▶ *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Oversigt over godkendte underdatabehandlere ▶ Underdatabehandleraftaler skal godkendes af DELTAPLAN ApS og dataansvarlige.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret proceduren for indgåelse af databehandleraftaler samt procedure for godkendelse af ændringer i forretningsbetingelser og databehandleraftale. Vi har observeret, at dataansvarlige skal godkende ændringer i databehandleraftalerne i DELTAPLAN online vagtplan.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ▶ DELTAPLAN ApS fører tilsyn med sine underdatabehandlere i form af indhentelse af erklæringer, fysisk besøg eller skriftligt tilsyn, baseret på en risikovurdering af databehandlerkonstruktionen.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af dokumentation for det førte tilsyn af underdatabehandlere. Vi har inspiceret ISAE 3402 revisorerklæring fra DELTAPLAN ApS' primære it-driftsleverandør Wannafind (tema.blue Denmark A/S) for perioden 2019. Vi har inspiceret ISAE 3000 revisionserklæring fra DELTAPLAN ApS' SMS serviceleverandør Compaya A/S. Der er ikke modtaget materiale i relation til Peytz & Co's e-mail-services.	Vi konstaterer, at der ikke for ydelser leveret af Wannafind samt Peytz & Co ikke foreligger en ISAE 3000 erklæringer eller tilsvarende dokumentation som kontrol på, at underdatabehandleres behandling af persondata sker betryggende og efter instruks fra DELTAPLAN. Ingen yderligere afvigelser konstateret.

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt		
Kontrolmål ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Lovbestemt tavshedspligt ▶ Som databehandler for offentlige myndigheder er DELTAPLAN ApS underlagt lovbestemt tavshedspligt.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af databehandleraftaler og har observeret, at der er oplyst om lovbestemt tavshedspligt.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle nuværende medarbejdere skal have underskrevet en tavsheds- eller fortrolighedsaftale.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af fortrolighedsaftaler og har observeret, at alle medarbejdere har underskrevet denne.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▸ DELTAPLAN ApS har udarbejdet risikovurderinger, der indenfor tilgængelighed, integritet og fortrolighed omfatter vurdering af risici, konsekvens og foranstaltninger i forhold til de registreredes rettigheder. ▸ Risikovurderingerne omfatter alle it- og databehandlingsaktiviteter.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret DELTAPLAN ApS' risikovurderinger og har observeret, at disse omfatter stillingtagen til tilgængelighed, integritet og fortrolighed samt konsekvenser herfor i forhold til de registreredes rettigheder Vi har observeret, at risikovurderingerne omfatter DELTAPLAN ApS' it- og databehandlingsaktiviteter.	Ingen afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▸ DELTAPLAN ApS har en beredskabsplan i tilfælde af brud på datasikkerheden, som er fysisk tilgængelig for medarbejderne. ▸ DELTAPLAN ApS har en beredskabsplan for gendannelse af data fra backup.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret DELTAPLAN ApS' beredskabsplan og har observeret, at der er taget stilling til foranstaltninger, og at den er tilgængelige for medarbejderne. Vi har inspiceret planen for sikkerhedskopiering og gendannelse. Vi har observeret, at DELTAPLAN ApS' backupdata er tilgængelige for gendannelse, og at en gendannelse er udført.	Ingen afvigelser konstateret.
Håndtering af inddata- og uddatamaterialer	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▸ DELTAPLAN ApS medarbejdere er instruerede i forsvarlig håndtering af ind- og uddata.	Vi har inspiceret databeskyttelsespolitikken, der omfatter retningslinjer for håndtering af persondataoplysninger.	
Opbevaring af personoplysninger ▸ Personoplysninger opbevares i henhold til databehandleraftalerne og de generelle forretningsbetingelser.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret udvalgte databaser og har observeret, at der ikke er andre personhenførbare data end angivet i databehandleraftalerne og de generelle forretningsbetingelser.	Ingen afvigelser konstateret.
Fysisk adgangskontrol ▸ DELTAPLAN ApS' kontorer er aflåste og overvåget udenfor kontortid.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret DELTAPLAN ApS' kontorer og har observeret, at disse er aflåste udenfor kontortid, samt at videoovervågning er etableret hele døgnet.	Ingen afvigelser konstateret.
Logisk adgangskontrol ▸ Kun medarbejdere, der er autoriseret, har adgang til DELTAPLAN ApS' kundedata. ▸ Adgangskoder er påkrævet for alle systemer og skal følge "Best Practice".	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af adgang til kundedata og har observeret, at kun autoriserede supportmedarbejdere har adgang til kundedata, og at adgangen logges. Vi har foretaget inspektion af adgangskoder til netværk, system og data og har observeret, at disse følger "Best Practice".	
Fjernarbejdspladser og fjernadgang til systemer og data - Kun medarbejdere, der er tildelt fjernadgang til serveradministration, har adgang til produktionsdata - Fjernadgang sker gennem en krypteret VPN-forbindelse.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret adgang til administrationsmodulerne og har observeret, at der skal anvendes VPN-adgang, og at der skal anvendes personlig adgangskode.	Ingen afvigelser konstateret.
Eksterne kommunikationsforbindelser - Adgang til DELTAPLAN online vagtplan sker over sikre, krypterede forbindelser. - E-mail skal anvende krypterede forbindelser.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret adgangen til DELTAPLAN online vagtplan, og vi har observeret, at dette sker over sikre, krypterede forbindelser. Vi har inspiceret aftalen med DELTAPLAN ApS udbyder af e-mailservice. Vi har observeret at e-mail forbindelserne er sikret med kryptering.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Kryptering af personoplysninger ▶ DELTAPLAN ApS krypterer data i databaser, som indeholder personoplysninger, hvor dette er påkrævet.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret udtræk fra databaser og observeret, at bankoplysninger og personnumre er krypteret i databasen.	Ingen afvigelser konstateret.
Firewall ▶ DELTAPLAN ApS' it-miljø er beskyttet af centrale samt personlige firewalls.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret driftsaftalen med DELTAPLAN ApS' it-serviceleverandør og vi har observeret, at firewall er omfattet af aftalen. Vi har ved udtræk inspiceret firewallopsætningen på DELTAPLAN ApS' lokale pc'er, og vi har observeret, at firewall er aktiveret.	Ingen afvigelser konstateret.
Netværkssikkerhed ▶ DELTAPLAN ApS netværk er opdelt i internt netværk og gæstenetværk.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har ved inspiceret gæstenetværket og ved efterprøvning observeret, at netværket er adskilt fra det interne netværk.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Antivirusprogram ▶ DELTAPLAN ApS har anti-malware og antivirusprogrammer installeret på alle pc'er, og at disse systemer opdateres løbende.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har ved udtræk inspiceret antimalware og antivirusprogrammer på medarbejdernes pc'er, og vi har observeret, at de er opdaterede.	Ingen afvigelser konstateret.
Sårbarhedsscanning og penetrationstests ▶ DELTAPLAN ApS har procedurer for sårbarheds- og penetrationstests, der sikrer identifikation af sårbarheder i applikationer og infrastruktur.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har observeret, at der ikke er formaliseret procedure for sårbarheds- og penetrationstests, ligesom der ikke foreligger dokumentation for at DELTAPLAN-systemet er testet.	Vi konstaterer, at der ikke er udarbejdet formaliseret procedurer for regelmæssig sårbarheds- og penetrationstests samt dokumentation herfor. Ingen yderligere afvigelser konstateret.
Sikkerhedskopiering og retablering af data ▶ DELTAPLAN ApS sikrer, at systemer og data sikkerhedskopieres. ▶ DELTAPLAN har implementeret en procedure for gendannelse af data, der sikrer, at data kan genskabes fra backup.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret procedure for sikkerhedskopiering, herunder logmateriale. Vi har inspiceret proceduren for gendannelse, herunder adgangen til gendannelse. Vi har observeret, at data kan gendannes ud fra backupkopier.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Vedligeholdelse af systemsoftware ▶ Operativsystemer skal være ajourført med sikkerhedsopdateringer.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret medarbejdernes pc'er, hvorvidt disse er ajourført med seneste sikkerhedsopdateringer. Vi har inspiceret driftsaftalen med DELTAPLAN ApS it-serviceleverandør om denne er omfattet af sikkerhedsopdatering af centralt udstyr.	Ingen afvigelser konstateret.
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ DELTAPLAN ApS har implementeret sikkerhedslogning ved adgang til DELTAPLAN online vagtplan.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har ved udtræk inspiceret adgangslog ved supporteres adgang til kundedata. Vi har observeret, at log indeholder oplysninger om adgang til data.	Ingen afvigelser konstateret.
Overvågning ▶ Systemfejl overvåges, logges og registreres i supportsystemet.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har ved udtræk inspiceret logning af systemfejl. Vi har observeret, at systemfejl registreres i DELTAPLAN ApS' supportsystem.	
Reparation og service samt bortskaffelse af it-udstyr ▸ DELTAPLAN ApS har procedurer for bortskaffelse af centralt it-udstyr, der sikrer, at it-udstyr bortskaffes på forsvarlig vis.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret driftsaftalen med DELTAPLAN ApS' it-serviceleverandør, der varetager korrekt bortskaffelse af centralt it-udstyr. Vi har på forespørgsel fået oplyst, at der på tidspunktet for vores erklæringsafgivelse ikke har været bortskaffelse, reparation og service. Vi har derfor ikke kunnet teste, at proceduren har været implementeret.	Ingen afvigelser konstateret.
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▸ Alle sikkerhedsdokumenter, herunder de detaljerede sikkerhedsforanstaltninger, revurderes ved væsentlige ændringer.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret udvalgte sikkerhedsdokumenter og har observeret, at disse er ajourførte i henhold til risikovurderingerne.	Ingen afvigelser konstateret.

Artikel 25: Databeskyttelse gennem design og standardindstillinger		
Kontrolmål ▶ *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Udvikling og vedligeholdelse af systemer ▶ DELTAPLAN ApS har procedurer for systemudvikling, test og idriftsættelse. ▶ Risikovurdering af systemændringer for at sikre databeskyttelse gennem design, jf. artikel 25, stk. 1. ▶ Enhver systemændring er testet, inden idriftsættelse. ▶ Alle systemændringer registreres i en ændringslog. ▶ Versionsstyring af systemændringer gør det muligt at ▶ tilbageføre ændringer ved fejl eller lignende (roll back).	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af procedurerne for driftsudvikling, test og idriftsættelse. Vi har inspiceret referater fra udviklermøde, der omfatter systemændringer og tests. Vi har inspiceret logs fra sikkerhedskopieringer samt gendannelse af data.	Ingen afvigelser konstateret.
Informationssikkerhed i udvikling og ændringer ▶ DELTAPLAN ApS indsamler kun oplysninger, der er relevante for systemets funktionalitet.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har foretaget inspektion af anvendelsen af informationsanalyse, herunder cookies. Vi har observeret, at der ikke indsamles data ud over nødvendige for systemets funktionalitet.	Ingen afvigelser konstateret.
Adskillelse af udviklings-, test og produktionsmiljø ▶ DELTAPLAN ApS anvender funktionsadskillelse mellem systemudvikling, test og produktion.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har ved inspektion observeret, at udviklere ikke har adgang til produktionsmiljøet.	Ingen afvigelser konstateret.
Personoplysninger i udviklings- og testmiljø ▶ DELTAPLAN ApS anvender ikke kundedata i test og udviklingsmiljøet.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret test- og udviklingsmiljø, der ikke indeholder personnumre.	Ingen afvigelser konstateret.

Artikel 25: Databeskyttelse gennem design og standardindstillinger		
Kontrolmål ▶ *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Supportopgaver ▶ DELTAPLAN ApS supportmedarbejdere har adgang til kundedata, når der ydes support til de dataansvarlige.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret medarbejdernes adgang til supportsystemet og kundernes data. Vi har observeret, at kun supportmedarbejderne har adgang, og at adgangen til kundedata logges.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren kan slette og tilbagelevere personoplysninger, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning og tilbagelevering af personoplysninger ▶ DELTAPLAN ApS har en procedure for sletning af data, der sikrer, at data slettes eller tilbageleveres ved ophør af kontrakten med den dataansvarlige. ▶ Personoplysninger slettes efter 5 år plus indeværende år. ▶ Personoplysninger kan slettes tidligere efter anmodning fra den dataansvarlige. ▶ Personoplysninger kan tilbageleveres, når behandlingen af personoplysninger ophører.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret proceduren for sletning af data. Vi har observeret, at data ikke slettes, men gøres utilgængelige for de dataansvarlige i henhold til procedurens tidsfrist. Vi har på forespørgsel fået oplyst, at data kan slettes manuelt efter ønske fra den dataansvarlige, og at der ikke er eksempler på, at dataansvarlige har anmodet om dette. Vi har således ikke kunnet teste, om kontrollen er implementeret. Vi har på forespørgsel fået oplyst, at data kan tilbageleveres til den dataansvarlige ved ophør af databehandlingen, og at der ikke er eksempler på, at dataansvarlige har anmodet om dette. Vi har således ikke kunnet teste, om kontrollen er implementeret.	Vi konstaterer, at personoplysninger ikke slettes i henhold til tidsfristen, men gøres utilgængelige for den dataansvarlige. Data kan slettes manuelt efter ønske fra den dataansvarlige. Ingen yderligere afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige		
Kontrolmål ▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
De registreredes rettigheder ▶ DELTAPLAN ApS har procedurer, der skal sikre bistand til den dataansvarlige om de registreredes rettigheder	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret proceduren samt databehandleraftalen, der omfatter bistand til den dataansvarlige om de registreredes rettigheder. Vi har observeret, at DELTAPLAN ApS forpligter sig til at bistå den dataansvarlige.	Ingen afvigelser konstateret.
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser ▶ DELTAPLAN ApS har procedurer for bistand til den dataansvarlige om brud på persondatasikkerhed og konsekvensanalyse.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret proceduren samt databehandleraftalen, der omfatter bistand til den dataansvarlige i forbindelse med behandlingssikkerhed, brud på persondatasikkerhed og konsekvensanalyse. Vi har observeret, at DELTAPLAN ApS forpligter sig til at bistå den dataansvarlige.	Ingen afvigelser konstateret.
Revision og inspektion ▶ DELTAPLAN ApS har indført procedurer, der sikrer, at DELTAPLAN ApS kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige ved fysisk tilsyn eller inspektion.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret databehandleraftaler samt besvarelser på henvendelser fra dataansvarlige om databehandlingen. Vi har observeret, at DELTAPLAN ApS på anmodning har stillet alle relevante oplysninger til rådighed.	Ingen afvigelser konstateret.

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter		
Kontrolmål ▶ *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.* ▶ *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.* ▶ *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. Listen opdateres, når der foretages ændringer og kontrolleres under den årlige revision.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret DELTAPLAN ApS' fortegnelse over behandlingsaktiviteter. Vi har observeret, at fortegnelsen indeholder de oplysninger, som kræves efter databeskyttelsesforordningens artikel 30 stk.2.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ DELTAPLAN ApS vedligeholder en fortegnelse over behandlingsaktiviteter, der opbevares elektronisk.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret fortegnelsen over behandlingsaktiviteter og har observeret, at denne vedligeholdes i en central database.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Alle relevante aktuelle oplysninger i fortegnelsen kan stilles til rådighed for tilsynsmyndigheden.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har ved inspektion observeret, at der kan foretages udtræk fra fortegnelsen efter anmodning. Vi har på forespørgsel fået oplyst, at fortegnelsen vedligeholdes løbende, og at den efter anmodning stilles til rådighed for Datatilsynet.	Ingen afvigelser konstateret.

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden		
Kontrolmål ▶ *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.* ▶ *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underretning om brud på persondatasikkerheden ▶ DELTAPLAN ApS har en beredskabsplan, der sikrer at den dataansvarlige underrettes om brud på persondatasikkerhed.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret DELTAPLAN ApS' beredskabsplan. Vi har observeret, at denne omfatter underretning af den dataansvarlige.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ DELTAPLAN ApS har en beredskabsplan, der sikrer at brud på persondatasikkerheden identificeres.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret DELTAPLAN ApS' beredskabsplan og har observeret, at denne omfatter identifikation af brud på persondatasikkerheden.	Ingen afvigelser konstateret.
Registrering af brud på persondatasikkerheden ▶ DELTAPLAN ApS har implementeret et system til registrering håndtering af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos DELTAPLAN ApS. Vi har inspiceret DELTAPLAN ApS' beredskabsplan og har observeret, at denne omfatter registrering af brud på person-datasikkerheden. Vi har observeret, at DELTAPLAN ApS anvender et skema til registrering af brud på persondatasikkerheden. Vi har på forespørgsel fået oplyst, at DELTAPLAN ApS på tidspunktet for afgivelse af erklæringen ikke har haft brud på persondatasikkerheden, hvorfor implementering af kontrollen ikke har kunnet testes.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 80

PENNEO

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

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

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2021-01-14 08:22:47Z
NEM ID

Mikkel Jon Larssen
Underskriver
Serienummer: CVR:20222670-RID:52744874
IP: 77.243.xxx.xxx
2021-01-14 08:27:11Z
NEM ID