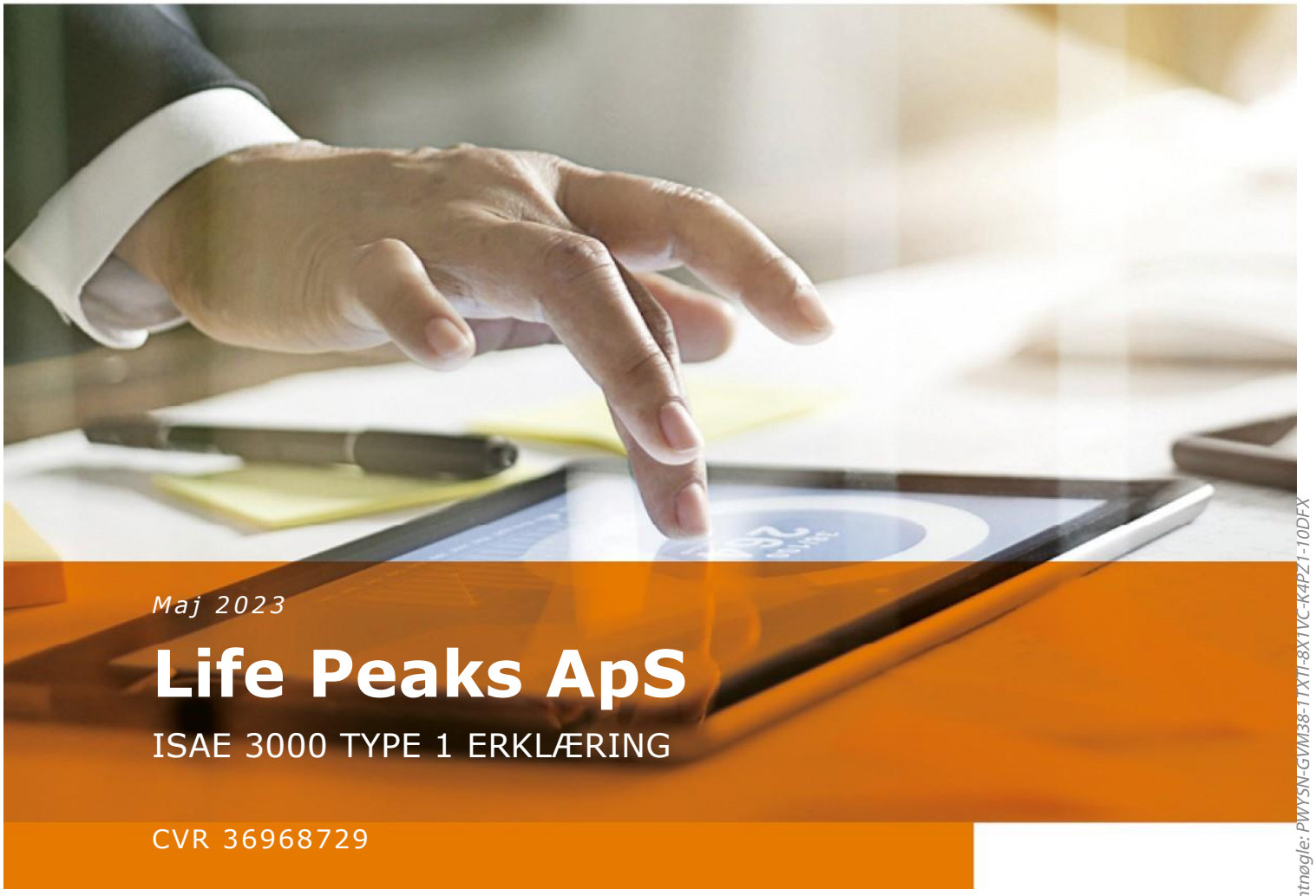
BEIERHOLM
VI SKABER BALANCE



Maj 2023

Life Peaks ApS

ISAE 3000 TYPE 1 ERKLÆRING

CVR 36968729

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med dataansvarlige.

Beierholm
Statsautoriseret Revisionspartnerselskab
Tangen 9
8200 Aarhus N
CVR 32 89 54 68
Tlf +45 87 32 57 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Life Peaks ApS' kunder.

Kapitel 3:
Beskrivelse af behandling.

Kapitel 4:
Kontrolmål, kontrolaktivitet, test og resultat heraf.

KAPITEL 1:

Ledelseserklæring

Life Peaks ApS behandler personoplysninger på vegne af kunder, i henhold til databehandleraftale for Life Peaks ApS' platform til udstedelse og administration af gavekort mv.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Life Peaks ApS' platform til udstedelse og administration af gavekort, som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Erklæringen omfatter ikke kontroller og forhold hos serviceleverandører og underdatabehandlere.

Life Peaks ApS bekræfter, at:

- Den medfølgende beskrivelse, afsnit 3, giver en retvisende beskrivelse af Life Peaks ApS, der har behandlet personoplysninger for dataansvarlige som er omfattet af databeskyttelsesforordningen pr. 16. maj 2023.
  Kriterierne der er anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

  a) Redegør for, hvordan behandling af data var udformet og implementeret, herunder redegør for:

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

     ii) de processer i både it- 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 persondata under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

     viii) kontroller, som vi med henvisning til Life Peaks ApS' platform til udstedelse og administration af gavekorts udformning, 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.

ix) andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

b) 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 behandling og berigelse af data, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

- De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 16. maj 2023.
  Kriterierne som er anvendt for at give denne udtalelse var, at:

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

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

  iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse pr. 16. maj 2023.

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.

Brabrand, 31. maj 2023

Life Peaks ApS

David Balsgaard
Direktør

KAPITEL 2:

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Life Peaks ApS' kunder

Til Life Peaks ApS og relevante dataansvarlige

Omfang

Vi har fået som opgave at afgive erklæring om Life Peaks ApS' beskrivelse jf. kapitel 3 i henhold til databehandleraftale med Life Peaks ApS' kunder, pr. 16. maj 2023 og om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen omfatter ikke forhold og kontroller hos serviceleverandører og underdatabehandlere og vi udtrykker ingen konklusion herom.

Life Peaks ApS' ansvar

Life Peaks ApS' er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse jf. kapitel 3, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Beierholm er underlagt international standard om kvalitetsstyring, ISQM 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

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

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

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

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i kapitel 3.

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

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

Begrænsninger i kontroller hos Life Peaks ApS

Life Peaks ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved databehandlingen, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af Life Peaks ApS' behandling, således som denne var udformet og implementeret pr. 16. maj 2023, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i pr. 16. maj 2023.

Beskrivelse af test kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Life Peaks ApS' platform til udstedelse og administration af gavekort, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Aarhus, 31. maj 2023

Beierholm
Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Jens Theodor Saugbjerg
IT-auditor

KAPITEL 3:

Beskrivelse af behandling

Databehandleren stiller – på Software-as-a-Service (SaaS) vilkår – en teknisk løsning til rådighed for den dataansvarlige, gennem hvilken den dataansvarlige kan udstede gavekort og billetter til events. Løsningen indeholder endvidere et administrationsmodul, hvor den dataansvarlige kan tilgå oplysninger om udstedte gavekort mv., herunder oplysninger om gavekortenes udløbsdato samt hvorvidt de enkelte gavekort er helt eller delvist brugt.

I forbindelse med driften af den tekniske løsning behandler databehandleren implicit personoplysninger på vegne af den dataansvarlige.

Løsningen kan integreres i websider, således at den dataansvarlige kan tilbyde kunder at tilgå relevante dele af løsningen direkte og købe gavekort på "selvbetjenings-basis". I den forbindelse kan designet af den brugergrænseflade, den dataansvarliges kunder præsenteres for, tilpasses, således at den overfor den dataansvarliges kunder fremstår med logo, farver og skrifttyper efter den dataansvarliges valg – typisk med henblik på at få siden til at passe til den dataansvarliges visuelle identitet.

Der er dog alene mulighed for at tilpasse præsentationslaget, og den underliggende teknik og dermed behandlingen af personoplysninger er således identisk for alle dataansvarlige, der benytter løsningen.

I tillæg til den tekniske løsning leverer databehandleren en service bestående i print og forsendelse af fysiske gavekort, i hvilken forbindelse der ligeledes behandles personoplysninger på vegne af den dataansvarlige med henblik på at kunne producere det fysiske gavekort og fremsende dette til rette modtager.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er reguleret ved en aftale, der dels fastsætter de kommercielle vilkår, og dels indeholder en databehandleraftale, der pålægger databehandleren de forpligtelser, der følger af forordning (EU) 2016/679 (databeskyttelsesforordningen), artikel 28, stk. 3 og beskriver de nærmere rammer for opfyldelsen af disse forpligtelser.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige, drejer sig primært om teknisk drift af den løsning, den dataansvarlige benytter til udstedelse og administration af gavekort, samt supplerende serviceydelser i form af produktion og forsendelse af fysiske gavekort.

Personoplysninger

Behandlingen omfatter alene oplysninger, der kan betegnes som "almindelige personoplysninger" i den forstand, at de ikke er omfattet af databeskyttelsesforordningens artikler 9, 10 eller 87 og således kan behandles af den dataansvarlige alene på grundlag af databeskyttelsesforordningens artikel 6.

Nærmere bestemt omfatter behandlingen følgende kategorier af personer og personoplysninger:

- Om købere af gavekort: Navn, e-mailadresse og telefonnummer, samt oplysninger om det købte gavekort (udstedelsesdato, gyldighedsperiode, pålydende beløb og angivelse af hvor gavekortet kan anvendes) samt betalingsform

- Om (den senere) indehaver af gavekort købt via løsningen: Navn, e-mailadresse, telefonnummer og eventuelt fysisk adresse (hvor køberen ønsker fysisk gavekort fremsendt til modtageren), samt oplysninger om brug af gavekortet (sted, tidspunkt og beløb), restbeløb på gavekortet og gavekortets gyldighedsperiode.

- Om medarbejdere hos den dataansvarlige: Navn, bruger-id og password samt oplysninger om brug af løsningen (i form af logfiler).

Praktiske tiltag

Life Peaks ApS leverer en standardiseret ydelse til et stort antal kunder.

Selv om der er mulighed for, at de enkelte kunder kan få tilpasset den grafiske brugergrænseflade, således at den fremstår som en integreret del af kundens website med samme farver, skrifttyper og andre kendetegn, sker behandlingen i det samme bagvedliggende system. Tilpasning af brugergrænsefladen påvirker ikke de dele af systemet, hvor den reelle behandling af personoplysninger finder sted, herunder den funktionalitet, der benyttes til at indsamle oplysninger fra kunderne. Behandlingen af personoplysninger i den tekniske løsning er således identisk for alle kunder.

De tillægsydelser, der indebærer et aspekt af manuel behandling – produktion og forsendelse af fysiske gavekort – indebærer ikke anden behandling af personoplysninger end print af gavekort og adresselabels. Denne proces er i praksis også i høj grad standardiseret.

Tilsvarende er de dele af kundeaftaler med tilhørende databehandleraftaler, der beskriver ydelserne og Life Peaks' behandling af personoplysninger i forbindelse hermed, også identiske.

Skulle en kunde have særlige ønsker eller behov, som Life Peaks ApS vælger at imødekomme, vil dette typisk ske ved en generel tilpasning af løsningen, således at ændringen får effekt for alle kunder, og dermed er risikoen for, at enkeltkunder har givet afvigende instruks for behandlingen i praksis ikke eksisterende.

Den tekniske løsning hostes i Amazon Web Services (AWS), som dermed forestår driften af den tekniske infrastruktur, herunder varetagelsen af tekniske og organisatoriske foranstaltninger, der er relevante for at sikre en stabil, velfungerende og sikker infrastruktur.

Ledelsen i Life Peaks ApS har – under hensyntagen til de ovenfor omtalte karakteristika ved den udbudte løsning, samt de muligheder og begrænsninger, der følger af et begrænset antal medarbejdere i virksomheden – tilrettelagt tekniske og organisatoriske foranstaltninger med henblik på at sikre, at Life Peaks overholder sine forpligtelser i henhold til databehandleraftalen.

Life Peaks ApS har ved tilrettelæggelsen af passende foranstaltninger lagt vægt på, i videst muligt omfang, at automatisere behandlingen, således at risikoen for manuelle fejl minimeres.

Life Peaks ApS benytter i den forbindelse en række af de værktøjer, der stilles til rådighed af AWS til at etablere en yderligere sikkerhed indenfor rammerne af den sikkerhed, AWS tilbyder som standard. Disse yderligere sikkerhedsforanstaltninger er såvel forebyggende i form af bl.a. adgangsbegrænsninger, som opklarende i form af forskellige logs og andre værktøjer til overvågning af driftsmiljøet.

Derudover har Life Peaks ApS etableret formelle procedurer for at sikre

- at beskrivelserne i databehandleraftalen til stadighed er en korrekt og fyldestgørende afspejling af de behandlingsaktiviteter, Life Peaks ApS udfører for selskabets kunder,
- at der føres et tilsyn med underdatabehandlere, der er tilpasset den iboende risiko i de dele af behandlingen, de respektive underdatabehandlere varetager eller bidrager til,
- at såvel automatiserede som manuelle procedurer for behandlingen af personoplysninger til stadighed fungerer som tilsigtet,
- at hændelser, som kan true sikkerheden i løsningen eller Life Peaks ApS' evne til at opfylde sine forpligtelser i henhold til databehandleraftalen, opdages og håndteres uden unødig forsinkelse.

Risikovurdering

Som databehandler, har Life Peaks ApS alene ansvar for at foretage risikovurdering i forhold til fastlæggelse af passende foranstaltninger for at sikre en tilstrækkelig behandlingssikkerhed, jf. databeskyttelsesforordningens artikel 32.

Ved vurdering af sikkerheden har Life Peaks ApS lagt vægt på

- at behandlingen er ensartet og standardiseret
- at der alene behandles en begrænset mængde personoplysninger om den enkelte registrerede, og
- at der alene er tale om almindelige oplysninger som navn, e-mailadresse, telefonnummer og – i visse tilfælde – fysisk adresse, samt oplysninger om de købte gavekort, samt
- at de enkelte sjældent har en pålydende værdi på mere end nogle få tusinde kroner, hvorfor den økonomiske risiko for de registrerede er begrænset, om end det ikke kan afvises, at fejl i eller manglende tilgængelighed af oplysninger om gavekortets værdi kan medføre hændelser, der kan føre til et vist ubehag for den registrerede, afhængigt af, hvordan den dataansvarlige håndterer situationen.

På den baggrund er det Life Peaks ApS' vurdering,

- at det er tilstrækkeligt at foretage en overordnet risikovurdering af kravene til beskyttelse af personoplysningernes fortrolighed, troværdighed og tilgængelighed, og
- at hensynet til de registreredes rettigheder og frihedsrettigheder, herunder særligt de forventede meget begrænsede konsekvenser for de registrerede ved en kompromittering af datas fortrolighed, troværdighed eller tilgængelighed, tilsiger, at et sikkerhedsniveau i overensstemmelse med almindelig god praksis er tilstrækkeligt.

Det er i den forbindelse ligeledes Life Peaks ApS' vurdering, at netop datas troværdighed og tilgængelighed vil være af stor betydning for de dataansvarlige, da rettidig adgang til korrekt information er afgørende for de dataansvarliges mulighed for at betjene kunder, der ønsker at indløse gavekort.

Life Peaks ApS har derfor valgt at benytte en teknisk infrastruktur, som erfaringsmæssigt sikrer en høj oppetid, og at begrænse adgangen til at foretage ændringer af programmer og data til få personer og sikre, at en repræsentant fra selskabets ledelse altid er involveret ved godkendelse og driftssætning af ny eller ændret kode.

For så vidt angår beskyttelsen af de registreredes rettigheder og frihedsrettigheder i øvrigt, herunder eksempelvis vurdering af behovet for udarbejdelse af en konsekvensanalyse eller opfyldelse af oplysningspligten overfor de registrerede, påhviler ansvaret herfor de dataansvarlige.

Life Peaks vil bistå de dataansvarlige i det omfang, det er nødvendigt for at de dataansvarlige kan foretage de relevante risikovurderinger. Life Peaks bemærker i den forbindelse, at behandlingsaktiviteten i forbindelse med udstedelse og administration af gavekort mv. ikke har de egenskaber, der i henhold til databeskyttelsesforordningens betragtning 89 og Datatilsynets "liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse jf. databeskyttelsesforordningens artikel 35, stk. 4" indikerer, at en behandlingsaktivitet skulle indebære høj risiko.

Kontrolforanstaltninger

Efterlevelse af instruks (Kontrolmål A)

Life Peaks ApS har ansvaret for drift af den tekniske løsning, hvori behandlingen af personoplysninger finder sted. Denne behandling er standardiseret, og der anvendes tilsvarende en standardiseret instruks i databehandleraftalen. Der gælder således samme instruks for alle kunder.

Instruksen gennemgås regelmæssigt og mindst en gang om året for at sikre, at der er overensstemmelse mellem instruksen og den faktiske behandling af personoplysninger.

Derudover er aktiviteter, der er nødvendige for at efterleve krav i instruksen, i videst muligt omfang automatiseret (f.eks. sletning/anonymisering af data), således at risikoen for menneskelige fejl er minimeret.

Life Peaks ApS overvåger løbende, at systemet og de automatiserede aktiviteter udføres som tilsigtet.

Implementering af tekniske foranstaltninger til sikring af passende behandlingssikkerhed (Kontrolmål B)

Life Peaks ApS har vurderet, at et sikkerhedsniveau i overensstemmelse med almindelig god praksis er tilstrækkeligt.

Driften af den tekniske infrastruktur varetages af Amazon Web Services (AWS), og Life Peaks ApS har tilrettelagt behandlingen sådan, at der ikke opbevares data lokalt hos Life Peaks ApS. Life Peaks ApS gennemfører periodisk – en gang om året – tilsyn med AWS og andre underdatabehandlere og påser i den forbindelse

- at underdatabehandleren har implementeret de sikkerhedsforanstaltninger, der efter Life Peaks ApS' opfattelse er nødvendige for at opnå et passende sikkerhedsniveau, og
- at de implementerede sikkerhedsforanstaltninger med en betryggende grad af sikkerhed har fungeret som tilsigtet og samlet set har opfyldt de relevante kontrolmål

Derudover benytter Life Peaks ApS de værktøjer, der stilles til rådighed af AWS til etablering af supplerende sikkerhedsforanstaltninger i AWS' miljø. Dette inkluderer

- AWS Shield til beskyttelse mod Distributed Denial of Service (DDoS)-angreb
- AWS WAF (Web Application Firewall) for at beskytte vores webapplikationer mod almindelige webeksploits og ondsindede angreb.
- Amazon Virtual Private Cloud (VPC), som isolerer Life Peaks' ressourcer og skaber et sikkert virtuelt netværk, som Life Peaks ApS har fuld kontrol over. VPC konfigureres med sikkerhedsgrupper og netværks Access Control Lists (ACL) for at styre ind- og udgående trafik til Life Peaks ApS' systemer og databaser
- AWS Direct Connect eller AWS VPN til at oprette sikre forbindelser mellem Life Peaks ApS' on-premise netværk og Life Peaks ApS' AWS-miljø. Dette sikrer, at den eksterne adgang til systemer og databaser sker gennem en krypteret og sikker tunnel.
- AWS Config, Amazon CloudWatch, AWS GuardDuty, Amazon S3 Access Logs, AWS CloudTrail og AWS Security Hub benyttes til at overvåge drift og sikkerhed og afhjælpe eventuelle sikkerhedsproblemer. Overvågningen er til dels baseret på alarmer, der sikrer at Life Peaks ApS straks bliver underrettet, hvis visse foruddefinerede hændelser indtræffer.

Alle data er krypteret både under transmission og "i hvile".

Endelig får Life Peaks ApS i forbindelse med større opdateringer, sikkerhedstestet applikationen med hjælp fra et eksternt sikkerhedsfirma for at sikre, at applikationen er robust overfor tekniske angreb.

Implementering af organisatoriske foranstaltninger til sikring af passende behandlingssikkerhed (Kontrolmål C)

Life Peaks ApS har udarbejdet en overordnet informationssikkerhedspolitik, som fastsætter de overordnede målsætninger og rammer for informationssikkerheden. Informationssikkerhedspolitikken er godkendt af selskabets ledelse.

Informationssikkerhedspolitikken er suppleret af kortfattede procedurer og checklister for de væsentligste sikkerheds- og kontrolopgaver, såsom risikovurdering samt sletning/anonymisering og kontrol af heraf.

Derudover understøttes sikkerhedsarbejdet af, at Life Peaks ApS kun har et meget begrænset antal medarbejdere, hvorfor der er en tæt og daglig dialog mellem ledelse og alle medarbejdere i organisationen. Der er udarbejdet vejledning til medarbejderne om, hvordan de kan understøtte informationssikkerheden, og den tætte dialog giver et godt grundlag for en hurtig og effektiv håndtering af sikkerhedsmæssige problemer eller spørgsmål. Organisationens begrænsede størrelse og ledelsens meget direkte involvering i den daglige drift medvirker derudover til at sikre, at alle er bekendt med fratrædelser eller ændring af arbejdsopgaver, således at adgange til systemer og data kan deaktiveres eller tilpasses rettidigt.

Endelig har Life Peaks ApS etableret en procedure for godkendelse og driftssætning af ny eller ændret funktionalitet. Denne procedure sikrer blandt andet, at der altid er en repræsentant for selskabets ledelse involveret i godkendelsen af ny eller ændret funktionalitet.

Sikring af sletning af oplysninger (Kontrolmål D og E)

Sletning eller anonymisering af oplysninger er primært tilrettelagt med udgangspunkt i relevant lovgivning og det enkelte gavekorts levetid, således at det sikres, at oplysningerne opbevares så længe dette er nødvendigt for at den dataansvarlige kan opfylde sine retlige forpligtelser, herunder bogføringslovens dokumentationsforpligtelser og ihændehaverens ret til at få udbetalt restværdien af gavekort – også i en periode efter de er udløbet.

Slettefristerne er dokumenteret i databehandleraftalen og dermed godkendt af den dataansvarlige.

Sletning/anonymisering er automatiseret, således at oplysninger automatisk slettes eller anonymiseres i overensstemmelse med de vedtagne sletteregler.

Sikring af at der alene anvendes godkendte underdatabehandlere (Kontrolmål F)

Databehandleren har de dataansvarliges generelle godkendelse til at anvende underdatabehandlere. Anvendelsen af nye underdatabehandlere varsles senest tre uger inden de pågældende underdatabehandlere påbegynder understøttelsen af driften.

Derudover gennemgår Life Peaks ApS en gang om året oplysninger hos deres underdatabehandlere for at sikre, at de oplysninger, der er videregivet til de dataansvarlige om underdatabehandlerne stadig er korrekte (f.eks. om en underdatabehandler har skiftet navn eller er blevet opkøbt).

Når Life Peaks ApS indgår aftale med en ny underdatabehandler, påser Life Peaks ApS, at aftalen med underdatabehandleren pålægger underdatabehandleren de samme forpligtelser, som Life Peaks ApS er underlagt i aftalerne med de dataansvarlige. Såfremt der er relevante krav, der ikke findes i aftalen med underdatabehandleren, og det ikke er muligt for Life Peaks ApS at få indarbejdet et sådant krav, vurderer Life Peaks ApS, hvorvidt kravet er relevant henset til den ydelse, underdatabehandleren skal levere.

Såfremt kravet ikke er relevant, dokumenteres dette. Er der derimod tale om et krav, der er relevant i forhold til den pågældende underdatabehandler, søger Life Peaks ApS på anden måde at sikre, at manglen ikke får betydning for de dataansvarlige, f.eks. ved at Life Peaks ApS implementerer supplerende foranstaltninger, der afhjælper risikoen ved at et givet krav ikke findes i aftalen med underdatabehandleren.

Sikring af at der kun sker overførsel til tredjelande, hvor der er instruks herom, der er tilvejebragt et overførselsgrundlag og om nødvendigt implementeret supplerende foranstaltninger (Kontrolmål G).

Databehandleraftalen indeholder en instruks, der berettiger Life Peaks ApS til at overføre personoplysninger til lande udenfor EU/EØS (tredjelande), hvis dette sker som konsekvens af brugen af en godkendt underdatabehandler.

I de tilfælde, hvor anvendelsen af en underdatabehandler medfører overførsel af personoplysninger til tredjelande, sikrer Life Peaks ApS at der etableres et overførselsgrundlag – typisk EU-Kommissionens standardkontrakter, og at der etableres supplerende foranstaltninger for at sikre de registrerede en tilstrækkelig beskyttelse, hvor dette må anses for nødvendigt på grund af oplysningernes karakter og/eller retstilstanden i modtagerlandet.

De etablerede foranstaltninger er beskrevet i databehandleraftalen. Det påhviler herefter den dataansvarlige selv at vurdere, om disse foranstaltninger er tilstrækkelige og – i afkræftende fald – at etablere sådanne yderligere foranstaltninger, som den dataansvarlige måtte anse for nødvendige.

Sikring af databehandlerens evne til at bistå den dataansvarlige med besvarelse af registreredes anmodning om udøvelse af deres rettigheder (Kontrolmål H)

Den tekniske løsning indeholder funktionalitet, der gør det muligt for den dataansvarlige selv at udtrække oplysninger om individuelle registrerede, således at det er muligt for den dataansvarlige at besvare en indsigtsanmodning for så vidt angår de oplysninger, der behandles af databehandleren.

Det er af sikkerhedshensyn som udgangspunkt ikke muligt at slette eller ændre oplysninger i systemet, da dette vil medføre, at den dataansvarlige ikke længere vil kunne opfylde sine dokumentationsforpligtelser i henhold til gældende lov, særligt bogføringsloven.

Skulle der alligevel blive behov for at slette eller ændre oplysninger, vil databehandleren bistå hermed på ad hoc basis.

Sikring af at den dataansvarlige underrettes rettidigt om sikkerhedsbrud (Kontrolmål I)

Databehandleren har etableret en procedure, der sikrer, at den dataansvarlige underrettes om sikkerhedsbristen uden ugrundet ophold og om muligt indenfor 48 timer.

Kravene til indholdet af sådanne underretninger er fastsat i databehandleraftalens punkt 10.3.

Underretningen sendes til den e-mailadresse, der er oplyst af den dataansvarlige i den tekniske løsning.

---oOo---

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige har følgende forpligtelser af hensyn til den samlede sikkerhed i systemet:

- At sikre at den dataansvarliges medarbejderes adgang til løsningen til enhver tid er korrekt konfigureret, herunder at personer, der ikke længere skal have adgang til løsningen, deaktiveres i løsningen
- At sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering
- At vurdere behovet for yderligere supplerende foranstaltninger i forbindelse med eventuelle tredjelandsoverførsel samt etablering af sådanne nødvendige foranstaltninger.

KAPITEL 4:

Kontrolmål, kontrolaktivitet, test og resultater heraf

KONTROLMÅL A:

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

Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
A.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering. Vi har inspiceret, at procedurer er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
A.2 Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har forespurgt ledelsen om, hvordan det tilsikres, at behandling af personoplysninger alene foregår i henhold til instruks, og vurderet hensigtsmæssigheden heraf. Vi har inspiceret, at platformen kun kræver indtastning af de personoplysninger der er indeholdt i instruks fra dataansvarlig og at behandling af disse foregår i overensstemmelse med instruks.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
A.3 Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandleren mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har forespurgt ledelsen om, hvorledes der foretages vurderinger af om en instruks er i strid med gældende forordninger eller anden lovgivning.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL B:

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

Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
B.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen om, hvordan det tilsikres at der de aftalte krav i aftalen med den dataansvarlige. Vi har inspiceret en oversigt over skriftlige procedurer, og vurderet om hvorvidt denne forekommer opdateret og tilstrækkelig i forhold til aftalte sikringsforanstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.2 Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har forespurgt ledelsen om, hvorvidt risikovurderingen er tilrettelagt og gennemført, med den hensyn til konsekvenser for den behandlede. Vi har forespurgt ledelsen om, hvilke tekniske foranstaltninger der er implementeret, og hvordan disse sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Vi har inspiceret, at der foreligger en formaliseret politik, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Vi har inspiceret at, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.3 Der er implementeret sikringsforanstaltninger mod afvikling af ondsindet kode og virus på de systemer og databaser, der anvendes til behandling af personoplysninger og, at sikringsforanstaltningerne løbende opdateres.	Vi har forespurgt ledelsen, om der er valgt leverandører der har implementeret sikkerhedsforanstaltninger mod afvikling af ondsindet kode på relevante systemer og databaser. Vi har inspiceret, at sikkerhedsforanstaltninger mod afvikling af ondsindet kode, er indeholdt i leverandørens leverancer. Vi har inspiceret, via stikprøve, at leverandører har revisionserklæringer hvori der fremgår at der er implementeret foranstaltninger mod afvikling af ondsindet kode.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

B.4 Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.5 Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har forespurgt ledelsen, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Vi har inspiceret, at lokale netværk der anvendes til print af persondata, ikke er internetvendte og at der anvendes fysisk kabling ved print af gavekort og adressemærkater.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.6 Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har forespurgt, om det tilsikres at medarbejdere kun har adgang til persondata hvis de har et arbejdsbetinget behov herfor. Vi har inspiceret, at Life Peaks ApS' brugeres adgang til systemer og personoplysninger er begrænset til medarbejdernes arbejdsbetingende behov. Vi har inspiceret, at de implementerede tekniske foranstaltninger understøtter, at dataansvarlig er i stand til at opdele egne brugere efter arbejdsbetinget behov for adgang.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.7 Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Systemovervågning • Netværkstrafik. • Fejlkørsler • Autoskalering	Vi har inspiceret, at der er adgang til kontinuerlig monitorering af systemer. Vi har inspiceret, at der modtages alarmer i tilfælde af væsentlige hændelser, inkl. hvad leverandøren har foretaget sig, for at afhjælpe hændelsen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

B.8 Der anvendes effektiv kryptering ved transmission og opbevaring af personoplysninger via internettet og e-mail.	Vi har forespurgt ledelsen, om det tilsikres at der implementeret effektiv kryptering ved anvendelse af cloudløsning hvor der kan ske overførsel til tredjeland uden for EU. Vi har inspiceret, at data der opbevares i platformen, er krypteret med AES-256 kryptering. Vi har inspiceret, at nøglemateriale opbevares på fysisk hardware inden for EU. Vi har inspiceret, at data der transmitteres til platformen, er krypteret med RSA 2048 kryptering. Vi har inspiceret, at kvitteringsmails der udsendes via platformen, understøtter TLS-kryptering.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.9 Der er etableret logning i systemet, således at alle brugeraktiviteter i platformen registreres.	Vi har inspiceret, at alle handlinger der foretages af en bruger i platformen registreres og logges i systemet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.10 Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har forespurgt om hvorvidt der anvendes personoplysninger til test. Det oplyses at der ikke anvendes persondata, hverken i klar tekst eller anonymiseret, til test og udvikling.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.11 De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har inspiceret, at der er foretaget penetrationstest af platformen. Vi har inspiceret, at erkendte sårbarheder er gennemgået af ledelsen, og at der planlægges på opfølgning.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.12 Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har forespurgt ledelsen, om hvorvidt der følges faste procedurer for ændringer til platformen. Vi har forespurgt ledelsen, om hvorvidt denne godkender ændringer til platformen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
B.13 Der er forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger.	Vi har forespurgt ledelsen, hvorledes brugeradgangen til personoplysninger inspiceres. Vi har inspiceret medarbejderes adgange til systemer og databaser, og kontrolleret at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

B.14 Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og data centre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret, at der anvendes datacenter der kan dokumentere fysisk adgangssikkerhed via SOC2 erklæring. Vi har inspiceret, at alt behandling og opbevaring af persondata i fysisk form, foregår i aflåste lokaler. Vi har forespurgt ledelsen, om det tilsikres at der ikke opbevares persondata i fysisk form uden for almindelige arbejdstid.	Vi har ikke ved vores test konstateret yderligere afvigelser.

KONTROLMÅL C:

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

Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
C.1 Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. IT-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om IT-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.2 Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har forespurgt ledelsen, om hvorvidt den løbende sikrer at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler. Vi har inspiceret databehandleraftalen, og påset, at informationssikkerhedspolitikken ikke er i modstrid med den indgåede aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.3 Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser	Vi har forespurgt ledelsen, om hvorvidt der indhentes referencer i forbindelse med ansættelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.4 Ved ansættelse underskriver medarbejdere ansættelsesaftale der omfatter tavshedspligt. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information, som eksempelvis instrukssystemet.	Vi har forespurgt ledelsen, om det tilsikres at nye medarbejdere er bekendt med informationssikkerhedspolitikken og relevante procedurer vedrørende databehandling. Vi har inspiceret, via stikprøve, at tavshedspligt indgår i de underskreven ansættelsesaftaler.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

C.5 Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har forespurgt ledelsen, om det er en proces for at deaktivere brugerrettigheder og inddrage aktive ved en medarbejders fratrædelse. Vi har inspiceret, at der er implementeret en formel procedure for fratrædelse af medarbejdere. Vi har inspiceret, at tidligere ansatte ikke længere har aktive brugere i systemet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.6 Ved fratrædelse orienteres medarbejderen om, at tavshedspligten fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har inspiceret, at ansættelsesaftalen inkluderer en bestemmelse om at tavshedspligten er gældende efter fratrædelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
C.7 Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til IT-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har forespurgt ledelsen, om der gennemføres awareness-træning og uddannelse af medarbejde i IT-sikkerhed og behandlingssikkerhed. Vi har inspiceret, at der er adgang til uddannelse for medarbejdere indeholdende: • Grundlæggende IT-sikkerhed • Sikker adfærd online • Datahåndtering • Reaktion på databrud	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL D:

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.		
Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
D.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger. Vi har inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
D.2 Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Persondata slettes 12 måneder efter gavekorts udløb • Persondata slettes 36 måneder efter eventdata for billetter	Vi har inspiceret, via stikprøver, at data i platformen slettes/anonymiseres automatisk efter den prædefinerede sletningsdato.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
D.3 Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning	Vi har forespurgt ledelsen, om der er procedurer for tilbagelevering eller sletning af data ved ophør af behandling.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL E:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.		
Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
E.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen, om det tilsikres at der kun opbevares persondata i overensstemmelse med aftalen med dataansvarlige. Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
E.2 Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har forespurgt ledelsen, om de er bekendt med de lokationer hvor data behandles og opbevares. Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Vi har inspiceret, at der ikke fremgår behandlingslokationer der ikke er godkendt af den dataansvarlige i databehandleraftalen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL F:

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

Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
F.1 Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
F.2 Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har inspiceret at der ikke fremgår underdatabehandlere der ikke er generelt godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
F.3 Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren.	Vi har forespurgt ledelsen, om der er en procedure for at underrette den dataansvarlige rettidigt ved ændringer i anvendelsen af underdatabehandlere. Vi har inspiceret, at databehandleraftaler indeholder specifikke krav til rettidigt varsel af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
F.4 Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har forespurgt ledelsen, om den tilsikrer at underdatabehandlere som minimum er underlagt de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen. Vi har inspiceret at der er indgået databehandleraftaler med underdatabehandlere. Vi har inspiceret ved stikprøver på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

F.5 Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Vi har inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
F.6 Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende.	Vi har forespurgt ledelsen, om der foretages en risikovurdering af den enkelte underdatabehandler. Vi har inspiceret, at der løbende føres opfølgning med underdatabehandlere, herunder gennemgang af revisionserklæringer for udvalgte underdatabehandlere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL G:

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

Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
G.1 Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Vi har inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
G.2 Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har inspiceret, at der foreligger instruks fra dataansvarlige til overførsel af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
G.3 Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har forespurgt ledelsen, om den sikrer at et gyldigt overførselsgrundlag er til stede og kan dokumenteres. Vi har inspiceret, via stikprøver, at der foreligger gyldigt overførselsgrundlag samt dokumentation for supplerende sikringsforanstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL H:

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

Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
H.1 Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
H.2 Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har inspiceret, at der foreligger formaliserede procedurer for bistand til den dataansvarlige herunder: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsninger til behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har inspiceret, at platformen muliggør at dataansvarlig selv kan opfylde størstedelen af forpligtelserne over for den registrerede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL I:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.		
Life Peaks ApS' kontrolaktivitet	Revisors test af kontroller	Resultat af test
I.1 Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen, om der foreligger procedurer for håndtering af brud på persondatasikkerheden. Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
I.2 Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Orientering fra leverandører	Vi har forespurgt ledelsen, om hvorvidt der vil være muligt at identificere at muligt brud på persondatasikkerheden. Vi har inspiceret, at den udbudte awareness-træning indeholder reaktion på evt. databrud. Vi har inspiceret, at der er tilgang til overvågning af netværkstrafik. Vi har inspiceret, at overvågning mhp. identifikation af databrud, samt orientering til Life Peaks ApS, er indeholdt i leverandørens leverancer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
I.3 Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har forespurgt ledelsen, om der tidligere er konstateret nogen brud på persondatasikkerheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
I.4 Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

PENNEO

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

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

Jens Theodor Saugbjerg
IT-auditor
Serienummer: CVR:32895468-RID:82443788
IP: 212.98.xxx.xxx
2023-05-31 06:16:13 UTC
NEM ID

Kim Larsen
Statsautoriseret revisor
Serienummer: CVR:32895468-RID:34629841
IP: 212.98.xxx.xxx
2023-05-31 06:16:28 UTC
NEM ID

David Bram Balsgaard
Direktør
Serienummer: 4d1bd70e-85c8-4efd-9d4d-036b5bcd4561
IP: 185.187.xxx.xxx
2023-05-31 08:18:05 UTC
MitID