Stella Care ApS

Cvr 34472416

Kalkbrænderiløbskaj 6A, 2100 København Ø

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale 1.0 August 2021

1 Ledelsens udtalelse

Stella Care ApS behandler i forbindelse med Stella Cares løsning til lokalisering af demensramte personer personoplysninger på vegne af vore 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 de dataansvarlige, der har anvendt Stella Cares løsning, og 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.

Stella Care ApS bekræfter, at den medfølgende beskrivelse side 6 - 14 pr. 23.11.2022 giver en retvisende beskrivelse af Stella Cares løsning, hvori der er behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen.

Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan Stella Cares løsning var udformet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
- 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
- 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 underrettelse til de registrerede
- De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

- Kontroller, som vi 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
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne løsning til 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 løsningen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt udformet og effektivt implementeret pr. 23.11.2022. Kriterierne 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

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.

København, d. 30. november 2022

Stella Care ApS

Rasmus Hansen

Adm. Direktør

2 Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale version 1.0 August 2021

Til: Stella Care ApS og dataansvarlige der har databehandleraftale version 1.0 August 2021.

Omfang
Vi har fået som opgave at afgive erklæring om Stellas Care's beskrivelse på side 6 - 14 af løsningen til lokalisering af demensramte personer i henhold til databehandleraftalen version 1.0 August 2021 pr. dato 23. november 2022 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Stella Care Aps ansvar
Stella Care ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse på side 2-3, 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.

Revisors 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.

TimeVision Godkendt Revisionpartnerselskab er underlagt international standard om kvalitetsstyring, ISQC 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 Stella Care's beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.
Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på, at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af Stella Care's løsning til lokalisering af demensramte personer samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet på side 2-3.

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

Stella Care's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Stella Care's løsning til lokalisering af demensramte personer, 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 Stella Care's løsning til lokalisering af demensramte personer, således som denne var udformet og implementeret pr. dato 23. november 2022, i alle væsentlige henseender er retvisende, og
b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. dato 23. november 2022, og
c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt pr. dato 23. november 2022.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår på side 15-31.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 15-31 er udelukkende tiltænkt dataansvarlige, der har anvendt Stella Care's løsning til lokalisering af demensramte personer, 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.

Brøndby, den 30. november 2022

TimeVision
Godkendt Revisionspartnerselskab
CVR-nr.: 38267132

Lone Køhn Bundgaard
Registreret revisor
mne15966

3 Stella Cares beskrivelse af løsningen

3.1 Om Stella Care

Stella Care ApS er en privatejet dansk virksomhed med base i København, der udvikler og driver en løsning til lokalisering af demensramte personer. Siden 2012 har det været Stella Cares mål at skabe tryghed for mennesker med demens, deres pårørende samt plejepersonale.

Stella Cares løsning består af forskellige typer af personbårne GPS-enheder, en brugervenlig mobilapplikation ("Care Tracker") og et administrationssystem, der tilsammen skaber mulighed for, at pårørende og plejepersonale kan foretage geografisk lokalisering af demensramte personer. GPS-enhederne bæres af den demensramte, fx i form af et armbåndsur, og den tilhørende mobilapplikation samt administrationssystemet benyttes af pårørende eller personale.

Gennem løsningen skabes et grundlag for, at den demensramte opnår en høj grad af beskyttelse samtidigt med, at den individuelle frihed til at færdes frit bibeholdes. Derudover kan pårørende og plejepersonale være betryggede i, at de til enhver tid hurtigt kan lokalisere forsvundne demensramte personer.

Hovedparten af Stella Cares kunder er kommunale omsorgsmyndigheder, der anvender løsningen på plejecentre o.l. Blandt andre af Stella Cares kunder finder man også pårørende til demensramte personer, som rent privat har købt adgang til løsningen.

Stella Cares løsning kan defineres som tryghedsskabende velfærdsteknologi, jf. Bekendtgørelse om tryghedsskabende velfærdsteknologiske løsninger (BEK nr. 13 af 06/01/2022).

Stella Care har i de seneste år haft et stort fokus på beskyttelse af de registreredes personoplysninger, rettigheder og frihedsrettigheder. Ledelsen har derfor tilrettelagt sine processer, systemdesign, behandlingssikkerhed m.v. på en måde, der sikrer efterlevelse af gældende databehandleraftaler og databeskyttelsesforordningen.

3.2 Beskrivelse af behandlingen af personoplysninger

Stella Care fungerer i rollen som databehandler for sine kunder, der i rollen som dataansvarlige er overordnet ansvarlige for behandlingen af personoplysninger i løsningen.

Formålet med Stella Cares behandling af personoplysninger på de dataansvarliges vegne er at kunne levere de aftalte ydelser som aftalt mellem parterne, herunder at kunne levere fysiske GPS-enheder, at kunne stille mobilapplikationen og administrationssystemet til rådighed for den dataansvarlige og dennes brugere samt at yde support som aftalt i databehandleraftalen og salgsaftalen mellem parterne.

3.2.1 Karakteren af behandlingen

Behandlingen omfatter følgende:

- Stella Care behandler personoplysninger om demensramte personer, der er udstyret med en GPS-enhed. Behandlingen omfatter indsamling og brug af lokationsdata samt registrering af navn og personnumre med henblik på administration, support og drift af løsningen. Idet løsningen henvender sig til demensramte personer, vil der indirekte også ske behandling af helbredsoplysninger, om end disse oplysninger ikke registreres i Stella Cares systemer.
- Stella Care behandler personoplysninger om brugere (pårørende og plejepersonale), der anvender Care Tracker mobilapplikation og administrationsystemet. Behandlingen omfatter registrering af navn, kontaktoplysninger, arbejdsgiver, evt. stilling samt tekniske oplysninger om brugerens anvendte device.

3.2.2 Kategorier af registrerede personer og typer af personoplysninger

Følgende er omfattet af databehandleraftalen mellem parterne:

Kategorier af registrerede personer	Typer af personoplysninger
Demensramte personer	Navn Lokations data Personnummer Helbredsoplysninger
Brugere af mobilapplikation og administrationssystemet (pårørende og plejepersonale)	Navn Kontaktoplysninger (telefonnummer og mailadresse) Arbejdsgiver Evt. stilling Tekniske oplysninger om brugerens device ifm. brug af Care Tracker-applikationen.

3.2.3 Praktiske tiltag

Stella Cares fokus på på beskyttelse af de registreredes personoplysninger, rettigheder og frihedsrettigheder betyder, at organisationen løbende gennemfører praktiske tiltag i form af tekniske og organisatoriske sikkerhedsforanstaltninger, der sikrer vedvarende efterlevelse af gældende databehandleraftaler og databeskyttelsesforordningen.

Stella Care har dermed opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed. Dette sikrer blandt andet, at tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger, og at disse implementeres tilstrækkeligt med henblik på at sikre personoplysninger mod tab af fortrolighed, tab af integritet og tab af tilgængelighed.

Herunder gives der en struktureret oversigt over praktiske tiltag i form af tekniske og organisatoriske sikkerhedsforanstaltninger samt tilhørende kontroller:

Kontrolmål	Sikkerhedsforanstaltninger og kontroller	Henvisning til databeskyttelsesforordningen
Kontrolmål A Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.	• Sikring af gyldige databehandleraftaler med de dataansvarlige • Sikring af gyldig og dokumenteret instruks for behandling af personoplysninger • Efterlevelse af instruks for behandling af personoplysninger • Procedurer for underretning af den dataansvarlige ved ulovlig instruks	• Artikel 28 • Artikel 29 • Artikel 32
Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Risikovurderinger af behandlingsaktiviteter • Malwarebeskyttelse • Firewall • Netværkssegmentering • Brugeradgangsstyring • Systemovervågning og alarmering ved uregelmæssigheder • Kryptering • Hændelseslogning • Retningslinjer for test- og udviklingsmiljøer • Sårbarhedsscanninger og penetrationstests • Opdatering og patching af systemer, databaser og netværk • Passwordbeskyttelse • Tofaktorautentifikation • Fysisk adgangssikkerhed • Sikkerhedskopiering	• Artikel 5 • Artikel 25 • Artikel 28 • Artikel 32
Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Politikker for informationssikkerhed og databeskyttelse • Retningslinjer for rekruttering af personale • Retningslinjer for efterprøvning af personale gennem indhentelse af straffeattester • Retningslinjer for offboarding af personale ved fratrædelser • Instruktion af medarbejdere • Awarenesstræning • Sikring af opretholdelse af fortrolighed og tavshedspligt • Brugeradgangsstyring	• Artikel 5 • Artikel 25 • Artikel 28 • Artikel 30 • Artikel 32

Kontrolmål	Sikkerhedsforanstaltninger og kontroller	Henvisning til databeskyttelsesforordningen
Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.	• Procedurebeskrivelser for sletning af personoplysninger • Procedurebeskrivelse for sletning af genetablerede personoplysninger fra sikkerhedskopi	• Artikel 5 • Artikel 28
Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	• Procedurebeskrivelse for opbevaring af personoplysninger • Oversigt over geografiske lokationer for behandlingen af personoplysninger	• Artikel 28
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.	• Sikring af gyldige databehandleraftaler med underdatabehandlere • Sikring af gyldig og dokumenteret instruks for behandling af personoplysninger • Procedurer for den dataansvarliges godkendelse for ændring i brugen af underdatabehandlere • Procedurer for tilsyn med underdatabehandlere • Procedurer for notifikation af dataansvarnlige i forbindelse med tilsyn med underdatabehandlere • Risikovurderinger af databehandlere	• Artikel 28 • Artikel 29
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.	• Retningslinjer, der sikrer, at personoplysninger ikke overføres til modtagere udenfor EU/EØS uden den dataansvarliges instruks • Retningslinjer for overførsel af personoplysninger til modtagere udenfor EU/EØS • Sikring af fornødent overførselsgrundlag ved overførsler til modtagere udenfor EU/EØS	• Artikel 44 • Artikel 45 • Artikel 46

Kontrolmål	Sikkerhedsforanstaltninger og kontroller	Henvisning til databeskyttelsesforordningen
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.	• Retningslinjer for bistand til dataansvarlige	• Artikel 28
Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.	• Retningslinjer for håndtering af databrud • Awarenesstræning af personale • Opfølgning på uregelmæssigheder identificeret i logs, overvågning m.v. • Sikring af dokumentation af databrud • Fastlagte metoder for underretning af de dataansvarlige i tilfælde af databrud • Procedurer for bistand til dataansvarlige i tilfælde af databrud.	• Artikel 28 • Artikel 33

3.2.4 Risikovurdering

Stella Care foretager risikovurderinger af alle behandlingsaktiviteter, som omfatter behandling af personoplysninger.

Ledelsen i Stella Care har truffet beslutning om, at alle risikovurderinger, der vedrører behandlinger af personoplysninger, foretages ved hjælp af ENISAs[1] metoder og rammeværk. Derved sikres det, at risikovurderingerne tager udgangspunkt i behandlingens mulige konsekvenser for de registrerede, samt at forhold om trusler og sårbarheder kan identificeres tilstrækkeligt. ENISAs metoder og rammeværk for risikovurderinger inddrager desuden kontroller som omfattet af ISO/IEC 27001:2013.

Gennem ENISAs metode og rammeværk for risikovurderinger vurderes sårbarheder og trusler ud fra følgende temaer:

- Netværk og tekniske ressourcer
- Processer og procedurer relateret til behandlingen
- Involverede personer og parter
- Branchesektor og omfang af behandlingen.

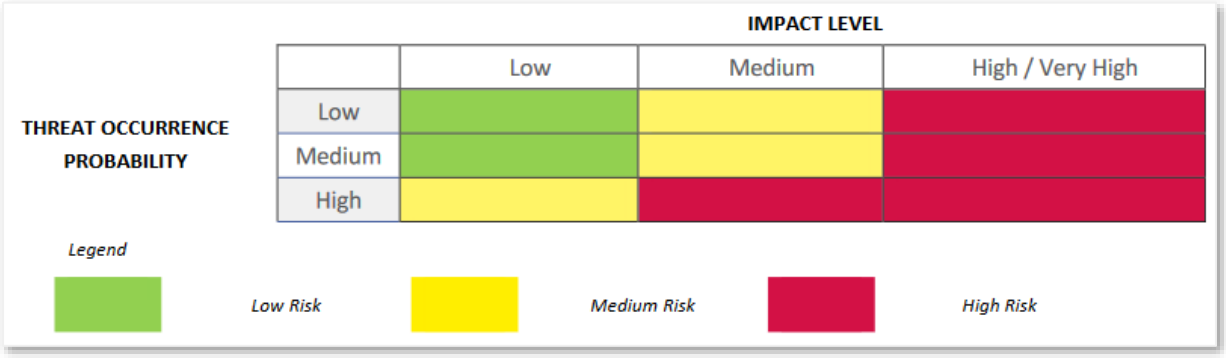
Baseret på underspørgsmål for hvert tema, har Stella Care identificeret et trusselsbillede, hvorved det har været muligt at identificere passende sikkerhedsforanstaltninger, der kan minimere forekomsten af brud på persondatasikkerheden og forbedre processer med henblik på beskyttelse af personoplysninger.

Udover ovenstående temaer tager ENISAs metoder og rammeværk for risikovurderinger udgangspunkt i følgende definitioner:

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Figur 1: Niveauer for vurdering af konsekvenser for de registrerede

[1] ENISA: European Union Agency for Network and Information Security (www.enisa.europa.eu)



Figur 2: Identifikation af trusselsbilledet

Stella Cares risikovurderinger tager udgangspunkt i følgende dataflows:

Figur 3: Dataflow – Stella Cares løsning til lokalisering af demensramte borgere

Det sikres til enhver tid, at alle implementerede sikkerhedsforanstaltninger lever op til de krav, der følger af databehandleraftalerne med de dataansvarlige.

Der følges op på alle risikovurderinger én gang årligt eller oftere, såfremt behovet opstår på grund af ændringer i processer, systemer m.v.

3.2.5 Kontrolforanstaltninger

Stella Care har implementeret kontroller vedrørende behandling af personoplysninger indenfor følgende områder:

Databehandleraftaler og instruks (kontrolmål A)

- Sikring af gyldige databehandleraftaler med de dataansvarlige
- Sikring af gyldig og dokumenteret instruks for behandling af personoplysninger
- Efterlevelse af instruks for behandling af personoplysninger
- Procedurer for underretning af den dataansvarlige ved ulovlig instruks

Tekniske sikringsforanstaltninger (kontrolmål B)

- Risikovurderinger af behandlingsaktiviteter
- Malwarebeskyttelse
- Firewall
- Netværkssegmentering
- Brugeradgangsstyring
- Systemovervågning og alarmering ved uregelmæssigheder
- Kryptering
- Hændelseslogning

- Retningslinjer for test- og udviklingsmiljøer
- Sårbarhedsscanninger og penetrationstests
- Opdatering og patching af systemer, databaser og netværk
- Passwordbeskyttelse
- Tofaktorautentifikation
- Fysisk adgangssikkerhed
- Sikkerhedskopiering

Organisatoriske foranstaltninger (kontrolmål C)

- Politikker for informationssikkerhed og databeskyttelse
- Retningslinjer for rekruttering af personale
- Retningslinjer for efterprøvning af personale gennem indhentelse af straffeattester
- Retningslinjer for offboarding af personale ved fratrædelser
- Instruktion af medarbejdere
- Awarenesstræning
- Sikring af opretholdelse af fortrolighed og tavshedspligt
- Brugeradgangsstyring

Sletning og tilbagelevering af personoplysninger (kontrolmål D)

- Procedurebeskrivelser for sletning af personoplysninger
- Procedurebeskrivelse for sletning af genetablerede personoplysninger fra sikkerhedskopi

Opbevaring af personoplysninger (kontrolmål E)

- Procedurebeskrivelse for opbevaring af personoplysninger
- Oversigt over geografiske lokationer for behandlingen af personoplysninger

Anvendelse af underdatabehandlere (kontrolmål F)

- Sikring af gyldige databehandleraftaler med underdatabehandlere
- Sikring af gyldig og dokumenteret instruks for behandling af personoplysninger
- Procedurer for den dataansvarliges godkendelse for ændring i brugen af underdatabehandlere
- Procedurer for tilsyn med underdatabehandlere
- Procedurer for notifikation af dataansvarnlige i forbindelse med tilsyn med underdatabehandlere
- Risikovurderinger af databehandlere

Bistand til den dataansvarlige (kontrolmål H)

- Retningslinjer for bistand til dataansvarlige

Håndtering af databrud (kontrolmål I).

- Retningslinjer for håndtering af databrud
- Awarenesstræning af personale
- Opfølgning på uregelmæssigheder identificeret i logs, overvågning m.v.
- Sikring af dokumentation af databrud
- Fastlagte metoder for underretning af de dataansvarlige i tilfælde af databrud
- Procedurer for bistand til dataansvarlige i tilfælde af databrud.

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

Komplementerende kontroller hos de dataansvarlige

I forbindelse med den dataansvarliges brug af Stella Cares løsning til lokalisering af demensramte personer, har den dataansvarlige følgende forpligtelser (ikke udtømmende liste):

- Den dataansvarlige er ansvarlig for efterlevelse af databeskyttelsesforordningen, herunder forordningens principper som beskrevet i artikel 5.
- Den dataansvarlige skal give Stella Care besked om eventuelle ændringer i behandlingen af personoplysninger, som er nødvendig for at den dataansvarlige kan opfylde sine forpligtelser efter databeskyttelsesforordningen og databeskyttelsesloven.
- Den dataansvarlige – i det omfang det er muligt for den dataansvarlige – skal selv foretage fornødne ændringer i behandlingen af personoplysninger i det integrerede administrationssystem, fx i forbindelse med ajourføring af brugere.
- Den dataansvarlige skal sikre, at der er fornøden hjemmel til behandlingen af personoplysningerne.
- Den dataansvarlige skal sikre, at instruksen som givet i databehandleraftalen til Stella Care, er lovlig set i forhold til den enhver tid gældende lovgivning.
- Den dataansvarlige skal sikre sig overholdelse af oplysningspligten overfor de registrerede, jf. databeskyttelsesforordningens artikel 13 og 14.

4 Kontrolmål, kontrolaktivitet, test og resultat heraf

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på 1 behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har inspiceret proceduren for tildeling og afbrydelse af brugeradgange Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Det har ikke været muligt at teste implementeringen, da vi har fået oplyst, at der ikke har været tilfælde af behandling af personoplysninger, der er vurderet i strid med lovgivningen. Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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 Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Vi har Inspiceret, at procedurer er opdateret. Inspiceret ved en stikprøve på 2 databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Ingen afvigelser konstateret
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 Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Vi har Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Vi har Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Vi har Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Ingen afvigelser konstateret
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. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen afvigelser konstateret

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har forespurgt til proceduren for regelmæssig gennemgang af brugerne med adgang til personoplysninger. Vi har Inspiceret, at der afholdes statusmøder, hvor der foretages gennemgang af brugernes adgang.	Ingen afvigelser konstateret
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Fejlede forsøg på logon til systemer, databaser og netværk	Vi har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden.	Ingen afvigelser konstateret
B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: • Fejlede forsøg på log-on til systemer, databaser og netværk Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har forespurgt om procedure for hændelseslogning. Vi har Forespurgt om proceduren for beskyttelse af logning. Vi har Forespurgt om proceduren for logning af systemadministratorer m.v. Stikprøvevis inspiceret, at der er opsat logning af aktiviteter udført af systemadministratorer m.v. på servere.	Ingen afvigelser konstateret

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.10	Personoplysninger, der anvendes til udvikling, test eller lignede, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål, .	Vi har forespurgt om proceduren for sikring af testdata. Inspiceret informationssikkerhedspolitikken for sikring af testdata.	Ingen afvigelser konstateret
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har forespurgt om der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests.	Ingen afvigelser konstatere
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Vi har Inspiceret, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen afvigelser konstatere
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret proceduren for tildeling og afbrydelse af brugeradgange. Vi har inspiceret, at de aktive brugeradgange regelmæssigt vurderes på statusmøder med serviceleverandøren.	Ingen afvigelser konstatere
B.14	Der er etableret adgangssikkerhed, således at kun autoriserede personer har adgang til systemer og databaser, hvori der sker behandling af personoplysninger. .	Vi har inspiceret Datacenterbeskrivelsen, og at sikkerhedsregler indeholder procedure for fysisk adgangskontrol. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen afvigelser konstatere

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Ingen afvigelser konstatere

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstatere
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på 2 databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstatere
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Straffeattest	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på 1 nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet: • Straffeattest	Ingen afvigelser konstatere

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret ved en stikprøve på 1 nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på 1 nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • Stella Cares håndbog om databeskyttelse. • Øvrige relevante retningslinjer for behandling af personoplysninger, som er gældende for den pågældende medarbejders funktion, herunder relevant awarenesstræning.	Ingen afvigelser konstatere
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på 0 fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Det har ikke været muligt at teste implementeringen, da der ikke har været fratrædelser i perioden. Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved en stikprøve på 0 fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Det har ikke været muligt at teste implementeringen, da der ikke har været fratrædelser i perioden. Ingen afvigelser konstateret.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen afvigelser konstatere

Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstatere
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Behandlingen af personoplysningerne ophører med opsigelsen af databehandleraftalen. • Sletning af oplysninger kan desuden ske efter skriftlig anmodning fra den dataansvarlige. • Særligt for lokationsdata: • Lokationsdata er et eller flere datasæt bestående af en GPS-position (koordinater) og et tilhørende tidsstempel for, hvornår GPS-positionen er registreret af en GPS-enhed. • Lokationsdata kan opdeles i a) historiske lokationsdata og b) seneste lokationsdata: • a) Historiske lokationsdata er alle GPS-positioner, der er ældre end den seneste GPS-position. Historisk lokationsdata for GPS-enheder opbevares i en periode på 14 dage. • b) Seneste lokationsdata består af ét datasæt med den seneste GPS-position for en GPS-enhed. Seneste lokationsdata opbevares så længe GPS-enheden er i den dataansvarliges besiddelse. • Særligt for oplysninger om inaktive brugere af Care Tracker mobil/web applikation: • Oplysninger i form af login-oplysninger om brugere af Care Tracker mobil/web applikation slettes efter 12 måneders inaktivitet."	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på 1 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på 0 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Det har ikke været muligt at teste implementeringen omkring sletning af data, da vi har fået oplyst, at der ikke har været henvendelser fra kunder i perioden angående sletning. Ingen afvigelser konstateret.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
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.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret ved en stikprøve på 0 ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Det har ikke været muligt at teste implementeringen omkring sletning/tilbagelevering af data, da der ikke har været ophørt nogle aftaler i perioden. Ingen afvigelser konstateret.

Kontrolmål E
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på 2 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen afvigelser konstatere
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Stikprøvevis inspiceret, at der er dokumentation for, at databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige	Ingen afvigelser konstatere

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.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstatere
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på 2 underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstatere
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. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser konstatere
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på 2 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstatere

F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstatere
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. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen afvigelser konstatere

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.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren ikke må 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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger ikke overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstatere

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.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.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.	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. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstatere
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.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen afvigelser konstatere

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen afvigelser konstatere
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik	Forespurgt, om der har været afholdt awarenesstræning i 2022. Inspiceret dokumentation for gennemført awarenesstræning i 2022 Inspiceret dokumentation for overvågning af netværkstrafik	Ingen afvigelser konstatere
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret beredskabsplanen for håndtering af brud på persondatasikkerheden. Forespurgt, om der er konstateret nogen brud på persondatasikkerheden i erklæringsperioden	Ingen afvigelser konstatere

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
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.	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. • Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden	Ingen afvigelser konstatere

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."

Rasmus Hansen
Direktør
På vegne af: Stella Care ApS
Serienummer: 3da45185-f999-4089-a493-1cf60330e0f7
IP: 80.62.xxx.xxx
2022-11-30 17:28:16 UTC
MitID

Lone Køhn Bundgaard
Registreret revisor
På vegne af: TimeVision Godkendt Revisionspartnersel…
Serienummer: CVR:38267132-RID:13823126
IP: 46.36.xxx.xxx
2022-12-01 06:44:52 UTC
NEM ID