Dansk Revision Århus
godkendt revisionsaktieselskab
Tomsagervej 2
DK-8230 Åbyhøj
aarhus@danskrevision.dk
www.danskrevision.dk
Telefon: +45 89 36 12 12
Telefax: +45 89 36 12 00
CVR: DK 26 71 76 71
Bank: 6181 0007769555

DIGIREHAB A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med DigiRehab A/S´ kunder.

Indholdsfortegnelse

1. Ledelsens udtalelse

DigiRehab A/S behandler personoplysninger på vegne af kunder (dataansvarlige) i henhold til indgåede databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt DigiRehabs ydelser, 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. DigiRehab A/S bekræfter, at:

a) Den medfølgende beskrivelse giver en retvisende beskrivelse af DigiRehabs ydelser, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 20. november 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan ydelserne 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 med henvisning til DigiRehabs ydelsers afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - 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) Indeholder relevante oplysninger om ændringer ved databehandlerens ydelser til behandling af personoplysninger foretaget pr. 20. november 2023.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved behandlingen, 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 hensigtsmæssigt udformet pr. 20. november 2023. 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.

Viborg, 5. december 2023

Niels Heuer
adm. direktør

DigiRehab A/S
Brovej 20 A, st.
8800 Viborg

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med DigiRehab A/S´ kunder relateret til ydelsen.

Til: DigiRehab A/S og DigiRehab A/S´ kunder relateret til ydelsen

Omfang

Vi har fået som opgave at afgive erklæring om DigiRehab A/S' beskrivelse af ydelser i relation til behandling af personoplysninger på vegne af dataansvarlige i henhold til databehandleraftale med DigiRehab A/S´ kunder pr. 20. november 2023. om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

DigiRehab A/S' ansvar

DigiRehab A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse på side 3-4, 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.

Dansk Revision Århus 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 DigiRehab A/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. 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 funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af DigiRehabs ydelser 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.

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

Begrænsninger i kontroller hos en dataansvarlig

DigiRehab A/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 DigiRehab's ydelser, 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 behandling af personoplysninger, således som denne var udformet og implementeret pr. 20. november 2023. 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. 20. november 2023.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt DigiRehab A/S' ydelser, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Åbyhøj, 5. december 2023

Dansk Revision Århus
godkendt revisionsaktieselskab, CVR-nr. 26717671

Claus Guldborg Nyvold
registreret revisor

3. Beskrivelse af behandling

DigiRehab A/S er leverandør af en SaaS (Software as a Service), og ved hjælp af den kan kommuner og private leverandører udføre fysisk træning med borgere, der kræver hjælp. DigiRehab A/S er derfor ansvarlig for at have procedurer og kontroller for at sikre opretholdelsen af de aftaler, der etableres med kunden. Dette omhandler både sikring af kundens data, daglig drift og vedligehold samt en videre udvikling af løsningen.

DigiRehab A/S er selv ansvarlig for implementering, support og drift af DigiRehab SaaS løsning, mens hosting og backup ivaretages af underleverandør.

DigiRehab blev grundlagt i 2014. DigiRehab A/S er specialister i fysisk rehabilitering af ældre borgere, og ved udviklingen af den web- baserede løsning DigiRehab, er det blevet muligt for kommuner og private aktører, der tilbyder hjemmepleje, at udnytte denne kompetence. Med DigiRehab løsning tilgængelig fra kundens IT-udstyr (primært tablets), kan personalet der udfører hjemmehjælp, nu også give borgere et tilbud om et individuelt tilpasset rehabiliteringsforløb.

DigiRehab A/S lægger stort fokus på videreudvikling af løsningen, efter kundens, slutbrugeren og samfundets behov, og har derfor følgende vision og mission:

Vores vision er at sikre livskvalitet og selvstændighed for så mange ældre som muligt på trods af eventuel nedsat funktionsevne. Vi sikrer dette ved at tilbyde et højkvalitets træningsværktøj, som vi med dyb indsigt udbreder med evidens for resultaterne.

Vores mission er at skabe velfærdsteknologiske produkter, der optimerer ressourceanvendelsen i den kommunale rehabilitering og samtidig øger ældres livskvalitet og selvhjulpenhed.

Karakteren af behandlingen

Databehandler leverer og supporterer og implementerer onlineløsningen. Data der lægges ind i systemet af den dataansvarlige bliver hostet ved databehandlerens brug af underdatabehandler.

Den typiske proces forløber således:

Borgeren bliver udvalgt på baggrund af faglig vurdering af rehabiliteringspotentialet. Herefter oprettes borgeren i DigiRehab med stamdata indeholdende navn og cpr./identifikationsnummer.

Borgeren screenes ift. fysiske formåen og behov for hjælp vha. en faglig vurdering og fysiske tests. Denne information lagres i www.digirehab.dk.

Systemet danner et træningsprogram baseret på ovenstående informationer. Herefter pågår træningen ca. 2 gange om ugen. Efter hver træning logges informationer om træningstidspunkt, borgerens oplevelse (fx ved smerter) og medarbejderen vurderer træningen på en skala.

Systemet adviserer relevant personale (fx visitationen) om udviklingen i træningsindsatsen og denne information bruges til at vurdere det videre forløb.

Intensiv træning ophører typisk efter 12 uger, hvorefter vedligeholdende træning opstartes. Herefter gemmes data på borgere i op til 5 år eller til hovedaftalens ophør.

Databehandler behandler denne data samt data om borgerens visiterede ydelser og udviklingen i disse på den dataansvarliges vegne. Sidstnævnte data kommer fra den dataansvarlige og anvendes til at vurdere det økonomiske potentiale ved anvendelsen af systemet.

Databehandler udarbejder løbende rapporter om dette i anonymiseret form.

Personoplysninger

Almindelige personoplysninger: Navn, adresse, træningstidspunkter, screeninginformation af borgerens behov for hjælp, screeningsinformation af borgerens fysiske formåen, visiterede ydelser.

Følsomme personoplysninger: Helbredsoplysninger.

Fortrolig oplysning: Cpr. nummer.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Borgere tilknyttet Sundheds- og omsorgsområdet, udvalgt baseret på en faglig vurdering af rehabiliteringspotentiale
- Medarbejdere i kommunen

Praktiske tiltag

Der er implementeret passende tekniske og organisatoriske foranstaltninger til at sikre behandling af personoplysninger. Disse foranstaltninger er implementeret på baggrund af anerkendte branchestandarder og retningslinjer fra databeskyttelsesforordningen og tilsynsmyndigheden.

Håndtering af informationssikkerhed og behandling af personoplysninger

Gennem den centrale informationssikkerhedspolitik og interne persondatapolitik har ledelsen beskrevet DigiRehab A/S' struktur for informationssikkerhed og behandling af personoplysninger. Politikkerne skal som minimum revideres én gang årligt.

DigiRehab A/S' overordnede målsætning er at levere en stabil og sikker SaaS løsning til kunderne. Til at understøtte dette er indført politikker og procedurer, der sikrer, at leverancer er ensartede og gennemsigtige.

DigiRehab A/S' interne retningslinjer for informationssikkerhed og behandling af personoplysninger er gældende for alle medarbejdere og for alle leverancer.

Alle servere og netværksenheder behandles af hosting leverandøren, som auditeres af ekstern revision minimum 1 gang om året.

De interne retningslinjer er udarbejdet, så DigiRehab A/S har ét fælles regelsæt. Dermed opnås et stabilt driftsmiljø, et højt sikkerhedsniveau og krav i databehandleraftaler der er indgået med kunder imødekommes.

Medarbejdere og uddannelse

Ledelsen har til opgave at sikre, at kompetencer vedligeholdes, og selskabets retningslinjer efterleves. DigiRehab A/S følger normale retningslinjer for håndtering af personale. Ledelsens kræver, at alle medarbejdere og underleverandører opretholder informationssikkerhed i overensstemmelse med DigiRehab A/S' politikker og procedurer.

Alle medarbejdere og relevante samarbejdspartnere bliver løbende informeret og gjort bevidste om DigiRehab A/S' retningslinjer for informationssikkerhed og behandling af personoplysninger. Retningslinjerne, som også gælder efter ansættelsens ophør eller ændring, er defineret og kommunikeret til medarbejderen/leverandøren og håndhæves af virksomheden.

Fysisk sikkerhed og miljøsikring

DigiRehab's A/S kontorfaciliteter er sikret med alarm udenfor kontorets åbningstider. Alarmen er tilknyttet bemandet alarmcentral med udrykning. Udenfor kontorets åbningstider er det kun autoriseret personale, der har adgang til faciliteterne. Yderligere er adgang til fortroligt materiale, der opbevares fysisk, sikret i skab med lås, og adgangen hertil er begrænset til udvalgte medarbejdere.

Netværkssikkerhed

Virksomheden opbevarer ikke driftsdata i kontorets faciliteter, da driftsdata opbevares ved hosting- partner. Internet ind til kontorfaciliteterne er fibernet, og serveren er beskyttet med firewall.

Driftsmiljø

DigiRehab A/S' driftsmiljø er placeret i underleverandørs datacenter, hvor denne er ansvarlig for at varetage sikkerheden, jf. kontrakt.

Underleverandøren har stor erfaring i opbygning og drift af datacenter, og er ansvarlig for den fysiske sikring, brand-, og vandskadedetektion og -bekæmpelse, strøm og køling.

Brugerstyring/ adgangssikkerhed

Ledelsen har fastsat retningslinjer for administration af adgang til både det interne driftsmiljø samt i forhold til produktionsmiljøet, herunder tildeling af rettigheder, således at en passende adskillelse af uforenelige funktioner er etableret. Adgangen til de forskellige it-miljøer sker gennem angivelse af unikke bruger-id og tilhørende password.

Kildekode

Adgang til kildekode administreres af underleverandør iht. instruks fra DigiRehab A/S. Det er kun udvalgte medarbejdere, med kompetencer og behov for adgang til kildekode, der bliver autoriseret til at have adgang. Adgang til kildekode sker via personlig brugerkonto og adgangskode. Systemet logger, hvilke medarbejdere der har været logget ind til kildekoden.

PC

Alle medarbejdere følger procedurer for adgangskode og pauseskærm.

Kunder, der benytter sig af DigiRehab, anvender en loginprocedure via eget ADFS, hvor de selv administrerer brugeradgang og password-krav. Loginforsøg logføres. Ved mislykket forsøg kan DigiRehab administrator se årsag hertil, og underrette kundens tekniske afdeling, der kan tilknytte brugeren de rigtige ADFS-grupper. Loggen slettes automatisk efter 6 måneder.

I forbindelse med brugeroprettelser eller nulstilling af adgangskoder (hvor kunden ikke benytter ADFS), skal brugerne have en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter indledende brug. Den midlertidige adgangskode skal være unik og følge best practice.

Antivirus/ Malwarebeskyttelse

Ledelsen har fastlagt retningslinjer for beskyttelse af PC mod malware og virus.

Itpilot A/S er ansvarlig for og administrerer antivirus og malwarebeskyttelse på DigiRehab A/S' servere, jf. kontrakt.

Overvågning

Itpilot A/S er ansvarlig for og administrerer overvågning af DigiRehab A/S' servere, datastorage, net- værksenheder mv.

Backup

Itpilot A/S er ansvarlig for og administrerer backup af DigiRehab A/S' driftsmiljø, jf. kontrakt.

Patch Management

Itpilot A/S er ansvarlig for og administrerer patches på DigiRehab A/S' driftsmiljø, jf. kontrakt.

Change Management

Formålet med change management er at sikre, at ændringer testes og afprøves, inden ændringer sættes i drift.

Proceduren for change management starter, når et behov for en ændring opstår. Ændringen registreres i opgavestyringssystemet DevOps. Når en ændring ønskes programmeret, videregives den som en op- gave til en programmør. Programmøren udfører ændringen på en lokal kopi af server. Når programmøren har udviklet/rettet, tester programmøren selv sin rettelse. Når programmøren er tilfreds med sit resultat, uploades løsningen til test-server, hvor funktionerne i ændringen gennemgås og evalueres.

Dette fortsætter som en iterativ proces, indtil ændringerne lever op til det ønskede resultat, og de efterfølgende er klar til at blive uploadet til drift-server og tilgængelige for DigiRehab A/S' kunder. Upload til drift-server sker periodisk og udenfor arbejdstid.

Styring af IT-sikkerhedshændelser

Alle medarbejdere i DigiRehab A/S er bekendt med procedurer og rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af DigiRehab A/S' drift. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til IT-administrator. IT-administrator har, sammen med ledelsen, ansvaret for at definere og koordinere en struktureret styrelsesproces, der sikrer en pas- sende reaktion på sikkerhedshændelser.

Beredskabsstyring

Formålet med beredskabsstyring hos DigiRehab A/S er at sikre forretningskontinuitet, samt give kunder en hurtig og valid reetablering i tilfælde af systemnedbrud.

DigiRehab's hosting-leverandør itpilot ApS, er ansvarlig for overvågning og drift af systemet. Fysisk og digitalt angreb på- og reetablering af systemet vil derfor følge hosting-leverandørs beredskabsplan.

Ved større nedbrud informeres kunder eller kundens DPO, der benytter de påvirkede services, via mail- liste. Denne besked indeholder en foreløbig status, fejlbeskrivelse, samt, hvis muligt, et estimat for hvornår fejlen er udbedret. Kunder holdes gennem mailliste løbende orienteret, indtil fejlen er udbed- ret.

Overensstemmelse med rollen som databehandler

DigiRehab A/S indgår databehandleraftaler med alle kunder, før kundens anvendelse af DigiRehab SaaS løsning går i gang.

DigiRehab A/S efterlever de sikkerhedskrav, som fremgår af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) og Databeskyttelsesloven.

DigiRehab A/S fører fortegnelser over behandlingen af personoplysninger samt fortegnelser over alle brud på persondatasikkerheden.

DigiRehabs A/S' behandling af personoplysninger på vegne af kunderne sker udelukkende efter dokumenteret instruks, medmindre - andet kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som DigiRehab A/S er underlagt; i så fald underretter DigiRehab A/S kunden om dette retlige krav in- den behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

DigiRehab A/S samt deres ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

DigiRehab A/S underretter straks kunden om ethvert brud på persondatasikkerheden.

Kunden træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt.

Alle medarbejdere er gjort bekendt med de retningslinjer og trænes løbende heri.

Risikovurdering

For hver behandlingsaktivitet er der foretaget en vurdering af sandsynligheden for at der sker tab af fortrolighed (uvedkommende får adgang til oplysningerne), integritet (oplysningerne er ikke korrekt) eller tilgængelighed (oplysninger mistes). I denne vurdering er der taget udgangspunkt i trusler og i de foranstaltninger der er implementeret for at beskytte oplysningernes fortrolighed, integritet og tilgængelighed.

Dernæst er konsekvensen for de registrerede blevet vurderet. Denne vurdering tager udgangspunkt i hvad konsekvensen for den registrerede er hvis der sker tab af fortrolige, integritet eller tilgængeligheden af oplysningerne. Vurdering er baseret på om oplysningerne er almindelige, fortrolige eller følsomme og de eventuelle indirekte konsekvenser med hensyn til typen af datasættet. Desto større sandsynlighed for at oplysningernes tab af fortrolighed, integritet eller tilgængelighed kan føre til materiel eller immateriel skade for den registrerede, desto større er konsekvensen.

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

Komplementerende kontroller hos de dataansvarlige

Denne generelle beskrivelse er baseret på, at der ikke tages højde for den enkelte kundes aftale.

De fleste kunder tildeler adgang til DigiRehab ved integration til kundens ADFS-løsning. Det betyder, at kunden selv kontrollerer, hvilke medarbejdere der har adgang til kundens data i DigiRehab løsningen. Disse kunder bærer derfor selv det fulde ansvar for håndtering af denne adgang, da den giver adgang til evt. fortrolig information. Dette betyder, at DigiRehab A/S ikke er ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til DigiRehab. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Kunden bærer derfor selv ansvaret for, at deres medarbejdere har adgang til systemet, og at de beskytter de informationer, der er registreret.

Følgende er en beskrivelse af de kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i afsnit 4.

Den dataansvarlige har følgende forpligtelser:

- at sikre sig, at personoplysningerne er ajourførte
- at sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering
- at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen.
- at sikre sig, at den dataansvarliges brugere er ajourførte

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.	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 bemærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer 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.	Ingen bemærkninger.

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*
		Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	

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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen bemærkninger.

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.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	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 bemærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	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 bemærkninger.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Ingen bemærkninger.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i	Ingen bemærkninger.

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*
		brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret ved en stikprøve på 5 kunder, at brugeres adgange til data er begrænset til medarbejdernes arbejdsbetingede behov.	
B.7	• Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen bemærkninger.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	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. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Ingen bemærkninger.

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*
		Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	
B.9	Der er etableret logning i systemer og databaser af følgende forhold: • Logon og fejlede login forsøg • Åbning af borger og træningsprogrammer • Når en medarbejder eller administrator hos kunden giver sig selv adgang til et nyt område	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret, at logning af brugeraktiviteter i systemer og databaser, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved en stikprøve på XX udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret.	Ingen bemærkninger.

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*
		Inspiceret ved en stikprøve på XX udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger.	Ingen bemærkninger.
B.12	Ændringer til systemer og databaser følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer og databaser, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer og databaser er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.	Ingen bemærkninger.

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*
		Inspiceret ved en stikprøve på 5 kunder er det påset at det kun er medarbejdere med arbejdsbetinget behov der er tildelt adgang til kunden. Inspiceret ved en stikprøve på 4 fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen bemærkninger.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til datacentre, hvori der opbevares og behandles personoplysninger.	Ingen bemærkninger.

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.	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 bemærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret, at kravene i databehandleraftalen der indgås med kunderne, er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen bemærkninger.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Ingen bemærkninger.

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.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 8 nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale.	Ingen bemærkninger.
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 4 fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen bemærkninger.
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 XX fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen bemærkninger.

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.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.	Ingen bemærkninger.

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 bemærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.	Ingen bemærkninger.
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.	Ingen bemærkninger.

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*
		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.	

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.	Ingen bemærkninger.
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.	Ingen bemærkninger.

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 bemærkninger.
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 1 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 bemærkninger.
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 bemærkninger.

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.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 1 ud af 1 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen bemærkninger.
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 bemærkninger.
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.	Ingen bemærkninger.

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*
		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.	

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 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.	Der sker ikke overførsel af personoplysninger til usikre tredjelande.

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 skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
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 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 procedurer.	Ingen bemærkninger.

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 bemærkninger.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af it-miljøet • Logning af brugeraktiviteter i systemet.	Inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret, dokumentation for overvågning af it-miljøet. Inspiceret, dokumentation for logning af brugeraktiviteter i systemet.	Ingen bemærkninger.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest XX timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden	Ingen bemærkninger.

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*
		Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.	
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 bemærkninger.

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."

Niels Heuer
Adm. direktør
Serienummer: d5bdbff9-834a-4442-9665-1ddb5fac0d04
IP: 158.248.xxx.xxx
2023-12-07 08:33:19 UTC