AMU-FYN

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 31. JULI 2022 OM BESKRIVELSEN AF TOTALLØSNINGEN OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 31. JULI 2022 OM BESKRIVELSEN AF TOTALLØSNINGEN OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i AMU-Fyn
AMU-Fyns kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af AMU-Fyn (databehandleren) pr. 31. juli 2022 udarbejdede beskrivelse i sektion 3 af Totalløsningen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

Databehandlerens ansvar

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

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

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

Revisors ansvar

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

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Begrænsninger i kontroller hos en databehandler

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af Totalløsningen, som hver enkelt dataansvarlig måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af Totalløsningen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 31. juli 2022, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 31. juli 2022.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

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

København, den 6. september 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Brian Bomholdt
Partner, CISA, CISM, CISSP

2. AMU-FYNS UDTALELSE

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

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

AMU-Fyn bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af Totalløsningen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 31. juli 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for Totalløsningen, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange, der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at 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 underretning til de registrerede.
    - De processer, der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.
2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af Totalløsningen og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved Totalløsningen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

AMU-Fyn bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 31. juli 2022. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

AMU-Fyn bekræfter, at der er implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller – bortset fra kontroller i forbindelse med Artikel 25 Databeskyttelse gennem design og standardindstillinger - med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Odense, den 6. september 2022

AMU-Fyn

Jimmy Andersen
Udviklingschef

3. AMU-FYNS BESKRIVELSE AF TOTALLØSNINGEN

Beskrivelse af AMU-Fyn

AMU-Fyn er en offentlig selvejet institution, hvis primære formål er at medvirke til at skabe et velfungerende arbejdsmarked. AMU blev skabt i 1960, med det formål, at ufaglærte både ledige og beskæftigede, skulle tilbydes korte erhvervsrettede kurser. I 1966 blev opgaven udvidet til også at omfatte efteruddannelse af faglærte.

AMU-Fyn beskæftiger ca. 110 medarbejdere hver med sit speciale organiseret i ledelse, undervisning, administration og supportfunktioner.

GDPR-udvalget på AMU-Fyn styrer personsikkerheden i forhold til den behandling af Totalløsningen, som AMU-Fyn varetager på vegne af totalløsningskunder, herunder indgåelse af databehandleraftaler, besvarelser fra den dataansvarlige, underretning om brud på datasikkerheden, efterlevelse af interne politikker og procedurer og lignende.

AMU-Fyn og behandling af personoplysninger

AMU-Fyn leverer en totalløsning af kursusadministration til sine kunder. For at indgå i et totalløsningssamarbejde er der indgået en samarbejds- og databehandleraftale mellem hver enkelt kunde og AMU-Fyn.

Formålet med totalløsningen er at overtage den administrative tunge byrde fra firmaerne ved at administrere tilmelding og indkaldelse af virksomhedernes personale til efteruddannelse, administrere VEU godtgørelser samt befordringsbidrag.

AMU-Fyn behandler følgende oplysninger: navn, personnummer, kontaktdata, dato for ansættelsesforholdets begyndelse og afslutning, uddannelsesoplysninger, lønoplysninger, herunder ansættelsesform og timetal, kontaktoplysninger på kontaktperson i virksomheden.

AMU-Fyn bruger ikke underdatabehandlere i forbindelse med Totalløsningen.

Styring af persondatasikkerhed

AMU-Fyn har etableret sikkerhedsforanstaltninger samt system til kontrol af disses efterlevelse af databeskyttelseslovgivning. De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet ud fra en risikovurdering af fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang teknisk understøttet af it-systemer. Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter, som auditeres hvert andet år af ekstern revision:

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

Risikovurdering

Ledelsen på AMU-Fyn er ansvarlig for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som AMU-Fyn og totalløsningen til enhver tid står over for, således at indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til mindst muligt niveau.

Der foretages en løbende vurdering af, hvilket sikkerhedsniveau der er passende. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, opbevaret eller på anden måde behandlet.

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller udføres der en gang årligt en risikovurdering. Risikovurderingen belyser sandsynligheden for og konsekvenserne af hændelser, der kan true persondatasikkerheden og dermed personers rettigheder, herunder tilfældige, forsætlige og uforsætlige hændelser. Risikovurderingen tager hensyn til det aktuelle tekniske niveau og implementeringsomkostningerne. I risikoanalysen indgår evt. svigt eller tab af en kritisk ressource, samt nødvendige forhold/foranstaltninger for at undgå dette.

Tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller

Databehandlerens garantier
AMU-Fyn har indført politikker og procedurer, der sikrer, at AMU-Fyn kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. AMU-Fyn har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres.

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

Databehandleraftaler og instruks
AMU-Fyn har indført procedure for indgåelse af databehandlingsaftaler, der angiver betingelserne for behandling af personoplysninger på vegne af den dataansvarlige. AMU-Fyn anvender en skabelon for databehandleraftaler i overensstemmelse med de tjenester, der leveres. Databehandleraftalerne underskrives af begge parter og opbevares elektronisk.

Fortrolighed og lovbestemt tavshedspligt
Som databehandler sikrer AMU-Fyn, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne lukkes derfor straks ned, hvis autorisationen fratages. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser over for den dataansvarlige. Som databehandler sikrer AMU-Fyn, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende tavshedspligt. Som databehandler kan AMU-Fyn efter anmodning fra den dataansvarlige påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering
AMU-Fyn har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom.

Beredskabsplaner
AMU-Fyn har etableret beredskabsplan, således at man rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. Beredskabsplanen ligger fysisk tilgængelig for personalet.

Opbevaring af personoplysninger
AMU-Fyn har indført procedurer, der sikrer, at opbevaring af personoplysninger alene foretages i overensstemmelse med AMU-Fyns persondatapolitik. Adgang til personoplysninger tildeles på baggrund af arbejds betinget behov/need-to-know principper.

Fysisk adgangskontrol
AMU-Fyn har indført procedurer, der sikrer, at lokaler og pc'er beskyttet mod uautoriseret adgang.

Logisk adgangssikkerhed
AMU-Fyn har etableret kontroller, der sikrer, at adgang til systemer og data er beskyttet mod uautoriseret adgang til personoplysninger. En bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Fjernarbejdspladser og fjernadgang til systemer og data
AMU-Fyn har implementeret procedurer, der sikrer, at adgang fra arbejdspladser uden for AMU-Fyns lokaler og fjernadgang til servere og data sker via sikre forbindelser. AMU-Fyn har implementeret procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med kryptering.

Netværk sikkerhed
AMU-Fyn har indført procedurer, der sikrer netværk i forhold til anvendelse og sikkerhed. AMU-Fyn netværk er opdelt i et administrativt- og et undervisningsnetværk. Sikkerheden sker igennem central router og dedikeret IP adressering.

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

Sikkerhedskopiering og reetablering af data
AMU-Fyn har indført procedure, der sikrer, at systemer og data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation.

Patch Management
AMU-Fyn har indført procedure, der sikrer, at systemer og systemsoftware på infrastrukturen opdateres med sikkerhedsopdateringer i overensstemmelse med leverandørernes anvisninger.

Logning af anvendelse af personoplysninger
AMU-Fyn har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret.

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

Bortskaffelse af IT-udstyr
Lagringsmedier, der skal destrueres, kan afleveres til den IT-sikkerhedsansvarlige, der skal sørge for en effektiv og permanent destruktion af mediet eller data derpå.

Databeskyttelse gennem design og standardindstillinger
AMU-Fyn udvikler og vedligeholder Totalløsningen efter behov. Ved ønsker til ændringer vurderes disse, herunder også eventuelle konsekvenser i relation til persondataforordningen. Udvikling af nye funktioner sker med ud fra behov og ønsker samt under hensyntagen til beskyttelser af de registrerede kursister ud fra en risikovurdering. Ændringer vurderes og testes forinden disse implementeres i Totalløsningen.

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

Bistand til den dataansvarlige
AMU-Fyn har indført politikker og procedurer, der sikrer, at AMU-Fyn kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.
AMU-Fyn indført politikker og procedurer, der sikrer, at AMU-Fyn kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige.
AMU-Fyn giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

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

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

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

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

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

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

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 31. juli 2022.

Udførte testhandlinger

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

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

Resultat af test

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

En afvigelse foreligger, når:

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

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Informationssikkerhedspolitik ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedspolitik. Vi har observeret at denne senest er opdateret i maj 2021. Vi har via forespørgsel fået oplyst, at medarbejdede som arbejder med Totalløsningen er bekendt med informationssikkerhedspolitikken indhold og krav.	Ingen afvigelser konstateret
Organisering af informationssikkerhedspolitik ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af Informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens informationssikkerhedspolitik og årshjul for efterprøvelse af Informationssikkerhed og persondataforordningen. Vi har stikprøvevis inspiceret styregruppereferater for vurdering og gennemførelse af ledelsesstyring i relation til Informationssikkerhed og persondataforordningen.	Ingen afvigelser konstateret
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for ansættelse af medarbejdere. Vi har observeret, at der stilles krav til erfaring og kompetencer ved ansættelser af medarbejdere til Totalløsningen.	Ingen afvigelser konstateret

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Der er ikke været nyansættelser i adskillige år, hvorfor det ikke er muligt at inspicere dokumentation for udført screening af ny medarbejdere.	
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for off-boarding af medarbejdere. Vi har observeret, at der stilles krav om fortsat fortrolighed af informationer efter fratrædelsen. Der er ikke været fratrædelser i adskillige gå, hvorfor det ikke er muligt at inspicerer dokumentation off-boarding af medarbejdere.	Ingen afvigelser konstateret
Uddannelse og instruktion af nye medarbejdere, der behandler personoplysninger ▶ Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og Informationssikkerhed, i forlængelse af ansættelsen. ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret personalepolitikken og observeret, at der stilles krav om introduktion og regelmæssigt træning i Informationssikkerhed og Persondataforordningen. Vi har inspiceret gældende årshjul for uddannelse. Der er ikke været nyansættelser i adskillige gå, hvorfor det ikke er muligt at inspicerer dokumentation for gennemført uddannelse og instruktion nye medarbejdere.	Ingen afvigelser konstateret

Awareness og oplysningskampagner generelt for medarbejdere ▶ Databehandleren udfører oplysningskampagner for medarbejdere om databeskyttelse og Informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret gældende årshjul for awareness træning. Vi har stikprøvevis inspiceret gennemført awareness træning.	Ingen afvigelser konstateret

Artikel 28, stk. 3: Databehandleraftale		
Kontrolmål ▶ *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Indgåelse af databehandleraftale med den dataansvarlige ▶ Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ▶ Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. ▶ Ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, anvender databehandleren en tjekliste, som fastlægger hvad databehandleren kan leve op til. ▶ Databehandleraftaler underskrives og opbevares elektronisk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for indgåelse af databehandleraftaler og observeret, at roller og ansvar er defineret og der stilles krav om opbevaring. Vi har inspiceret skabelon for indgåelse af databehandleraftaler i relation til Totalløsningen og observeret, at denne indeholder de forventede afsnit samt en instruks på behandling af persondata. Vi har stikprøvevis inspiceret underskrevet databehandleraftale og observeret, at den følger den fastsatte skabelon. Vi har stikprøvevis inspiceret alle databehandleraftaler foreligger elektronisk og er underskrevet.	Ingen afvigelser konstateret

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* ▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelon for indgåelse af databehandleraftaler i relation til Totalløsningen og observeret, at denne indeholder instruks på behandling af persondata. Ved forespørgsel er det oplyst, at databehandleren kun har databehandleraftaler efter egen standard. Vi har stikprøvevis inspiceret underskrevet databehandleraftale og observeret, at den følger den fastsatte skabelon.	Ingen afvigelser konstateret
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig. ▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for administration af Totalløsningen og tilhørende tekniske beskrivelser og observeret, at krav til beskyttelse af personoplysninger varetages. Vi har inspiceret årshjul for kontrol med persondataforordningen. Vi har stikprøvevis inspiceret egenkontrol for opfølgning på efterlevelse af persondataforordningen.	Ingen afvigelser konstateret
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig, i tilfælde hvor den dataansvarliges instruks, strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for underretning af dataansvarlige.	Ingen afvigelser konstateret

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* ▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Der har ifølge det oplyste ikke været registreret ulovlig databehandling i relation til den anførte instruks.	

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt		
Kontrolmål ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Lovbestemt tavshedspligt ▶ Alle medarbejdere tilknyttet Totalløsningen er underlagt lovbestemt tavshedspligt efter straffelovens bestemmelser.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har via forespørgsel fået oplyst, at Databehandleren er underlagt forvaltningslovens bestemmelser om tavshedspligt som offentlige uddannelsesinstitution.	Ingen afvigelser konstateret
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet en tavsheds- og fortrolighedsaftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for ansættelser og observeret, at der stilles krav om underskrevet tavshed- og fortrolighedsaftale som en del af afsættelsen af medarbejdere, som skal arbejde med Totalløsningen. Vi har stikprøvevis inspiceret, at underskrevet tavsheds- og fortrolighedsaftale foreligger på medarbejdere, som arbejder med Totalløsningen.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af Totalløsningen baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret årshjul for persondataforordningen og observeret, at der er fastsat krav om minimum årlig risikovurdering af Totalløsningen. Vi har inspiceret beskrivelse af tekniske sikringsforanstaltninger og observeret, at disse løbende revurderes ud fra identificerede trusler og i relevant omfang ajourføres. Vi har inspiceret procedurer for risikovurdering, samt den gennemførte risikovurdering af Totalløsningen.	Ingen afvigelser konstateret
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, beredskabsplanerne er tidssvarende og effektive i kritiske situationer. ▶ Beredskabstest dokumenteres og evalueres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beskrivelse af etablerede tekniske foranstaltninger og observeret, at der foreligger en beredskabsplan. Vi har inspiceret årshjul for it-drift og observeret, at der er fastsat krav test af beredskabet. Seneste test er gennemført i marts 2021.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Opbevaring af personoplysninger ▶ Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper. ▶ Fysiske materialer indeholdende personoplysninger opbevares aflåst.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beskrivelse af etablerede tekniske foranstaltninger og observeret, at der er defineret krav til adgangsbeskyttelse ud fra et arbejdsbetinget behov. Vi har inspiceret adgang til Totalløsningen og fået bekræftelse på, at alle medarbejdere med adgang har et arbejdsbetinget behov for adgang. Det er via forespørgsel oplyst, at der ikke opbevares personoplysninger fysisk form i relation til Totalløsningen.	Ingen afvigelser konstateret
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang. ▶ Alle udleverede nøgler registreres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Det er via forespørgsel oplyst, at kontorlokaler, hvor medarbejdere der arbejder med Totalløsningen sidder, er aflåst, når der ikke er personer til stede. Vi har inspiceret referater fra gennemført kontrol med udleverede nøgler.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter		
Fysisk sikkerhed ▶ Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. Den fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret etablerede fysiske sikringsforanstaltninger på serverrum, herunder foranstaltninger til beskyttelse mod eksterne og miljømæssige trusler.	Ingen afvigelser konstateret
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. ▶ Der foretages årligt gennemgang af brugere og brugerrettigheder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beskrivelse af tekniske sikringsforanstaltninger og observeret, at der er fastsat krav for tildeling af adgang og rettigheder til Totalløsningen. Vi har udtrukket brugere med adgang til Totalløsningen og stikprøvevist observeret, at tildelte adgang og rettigheder er sket ud fra et arbejdsbetinget behov. Vi har udtrukket privilegerede og stikprøvevist observeret, at tildelt adgang alene er sket ud fra et arbejdsbetinget behov.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret årshjul og observeret, at der minimum foretages en årlig gennemgang af brugere og brugerrettigheder.	
Fjernarbejdspladser og fjernadgang til systemer og data - Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. - Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse ([SHA-2 & 256 bit]) - Fjernadgang skal foregå via to-faktor autentifikation ([SMS Passcode])	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beskrivelse af tekniske sikringsforanstaltninger og observeret, at der er fastsat sikkerhedskrav til fjernadgang til Totalløsningen. Fjernadgang tildeles alene gennem en RDP-forbindelse – og ingen services på Totalløsningen er direkte udstillet på internettet. Vi har inspiceret personer med adgang til at kunne etablere RDP-forbindelser, herunder hvilke personer som så efterfølgende internt har adgang til Totalløsningen.	Ingen afvigelser konstateret
Eksterne kommunikationsforbindelser - Eksterne kommunikationsforbindelser er krypteret.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beskrivelse af tekniske sikringsforanstaltninger og observeret, at der er fastsat krav om kryptering eller tilsvarende for eksterne kommunikationsforbindelser.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret, at kommunikation mellem databehandlerens lokationer sker i et segmenteret MPLS-netværk. Vi har inspiceret, at fjernadgang til systemer og data sker gennem RDG gateway som fjernskrivebord.	
Netværkssikkerhed - Netværks topologien er struktureret efter best-practice principper, hvilket betyder at servere som driver applikationer ikke kan nås direkte fra internettet. - Databehandler netværk er segmenteret så interne services/servere ikke kan kommunikere direkte med internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at Databehandlerens netværk er segmenteret, således at administrativt netværk er adskilt fra det øvrige netværk. Vi har inspiceret at Totalløsningen er placeret på det administrative netværk. Vi har inspiceret, at databasen til Totalløsningen ikke kommunikerer direkte med internettet, men at dette sker gennem front-end applikation.	Ingen afvigelser konstateret
Antivirusprogram - Der er installeret antivirus-software på alle servere og arbejdsstationer. - Antivirus-software opdateres løbende og er opdateret med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beskrivelse af tekniske sikringsforanstaltninger og observeret, at der er fastsat krav til anvendelse af antivirusprogram.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har stikprøvevis inspiceret arbejdsstationer, som anvendes til Totalløsningen, og observeret, at antivirus er konfigureret og opdateret.	
Sikkerhedskopiering og retablering af data - Der foretages dagligt backup af systemer og data.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret beskrivelse af tekniske sikringsforanstaltninger og observeret, at der er fastsat krav til sikkerhedskopiering. Vi har inspiceret dokumentation for, at totalløsningen sikkerhedskopieres på daglig bases.	Ingen afvigelser konstateret
Vedligeholdelse af systemsoftware - Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed. - Databehandleren følger op på at systemsoftware opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har via forespørgsel fået oplyst, at opdatering af systemsoftware foretages manuelt ud fra en risiko- og konsekvens-vurdering af softwareopdateringer, når disse frigives fra leverandørerne. Vi har inspiceret at databaseserveren for Totalløsningen er opdateret med seneste sikkerhedsopdatering.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger samt overvågning ▶ Alle succesfulde og mislykkede adgangsforsøg til Totalløsningen og data logges. ▶ Alle brugerændringer i Totalløsningen og databaser logges. ▶ Loggen slettes efter den fastsatte retentionsperiode ▶ Databehandler monitorerer og logger netværkstrafik ▶ Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har via forespørgsel fået oplyst, at databehandleren ikke formelt har defineret krav til logning og overvågning på Totalløsningen. Standard AD event logning gennemføres, men der er ikke etableret en systematisk gennemgang og stillingstages til log. Logs gennemgås alene på ad hoc basis når der opstår et behov.	Vi konstaterer, at der ikke er formaliseret krav til opsætning af logning og overvågning på Totalløsningen, ud fra en risikobaseret tilgang til beskyttelse af persondata. Vi konstaterer desuden, at etableret logning på systemniveau ikke systematisk gennemgås, men anvendes til ad hoc baserede undersøgelser. Ingen yderligere afvigelser konstateret.
Reparation og service samt bortskaffelse af it-udstyr ▶ Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for håndtering af it-udstyr ved reparation og service og observeret, at medier og udstyr indeholdende særligt følsomme data ved endt brug vil blive destrueret fysisk. Der er har ikke de seneste år været medier med data fra Totalløsningen, som er blevet udfaset, hvorfor det ikke er muligt at inspicere dokumentation for udført destruktion.	Ingen afvigelser konstateret

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurdere og evaluerer effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret årshjul for kontrol med it-sikkerhed og GDPR-forhold. Vi har inspiceret referater fra afprøvning/vurdering af sikringsforanstaltninger.	Ingen afvigelser konstateret

Artikel 25: Databeskyttelse gennem design og standardindstillinger		
Kontrolmål ▶ *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Udvikling og vedligeholdelse af systemer ▶ Databehandleren arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelses opgaver. ▶ Risikovurdering af systemændringer er udført for, at sikre databeskyttelse gennem design og standardindstillinger. ▶ Der er indført funktionsadskillelse mellem udvikling og drift.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for databeskyttelse gennem design og standardindstillinger og teknisk flow for ændringer. Det er oplyst, at der sker meget få ændringer i systemet og ved ændringer vurderes konsekvenserne for de registrerede, inden ændringer gennemføres.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren kan slette og tilbagelevere personoplysninger, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af samarbejdet og/eller når en registreret ophører ansættelsesforholdet hos den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelon til databehandleraftale og konstateret, at databehandler er forpligtet til at slette data efter den dataansvarliges instruks. Vi har inspiceret henvendelse fra en dataansvarlig omkring sletning af en registreret. Vi har inspiceret procedurer for sletning af en kursist samt teknisk dokumentation for gennemført sletning.	Ingen afvigelser konstateret
Tilbagelevering af personoplysninger ▶ Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen. ▶ Dataansvarlig og databehandler har aftalt i hvilket format, overførelse og medie data skal tilbageleveres, når det anmodes af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelon til databehandleraftale og konstateret, at databehandler er forpligtet til at tilbagelevere data efter den dataansvarliges instruks. Der er har ikke de seneste år været henvendelse på tilbagelevering af persondata, hvorfor det ikke er muligt at inspicere dokumentation for udført tilbagelevering.	Ingen afvigelser konstateret

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige		
Kontrolmål ▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
De registreredes rettigheder ▶ Databehandler har udarbejdet en procedure for bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder. ▶ Det er muligt at give indsigt i alle oplysninger, der er registreret i Totalløsningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for bistand til de dataansvarlige. Vi har inspiceret indgåede databehandler aftaler. Det er observeret, at databehandleren er forpligtet til at yde bistand til den dataansvarlige i relation til de registreredes rettigheder. Der er har ikke de seneste år været henvendelse om bistand til den dataansvarlige hvorfor det ikke er muligt at inspicere dokumentation for udført bistand.	Ingen afvigelser konstateret
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret informationssikkerhedspolitikken samt procedurer for bistand til den dataansvarlige og observeret, at der er fastsat retningslinjer for bistand til de dataansvarlige. Der er har ikke de seneste år været henvendelse fra de dataansvarlige med ønsker om bistand, hvorfor det ikke er muligt at inspicere dokumentation for udført bistand.	Ingen afvigelser konstateret

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter		
Kontrolmål ▶ *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.* ▶ *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.* ▶ *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Databehandlerens fortegnelse er skriftlig og opbevares elektronisk. ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret fortegnelse over behandlingsaktiviteter i Totalløsningen og observeret, at denne opbevares elektronisk og indeholder relevante information om behandlingsaktiviteterne. Det er via forespørgsel oplyst, at databehandleren vil udlevere fortegnelsen ved anmodning fra Datatilsynet.	Ingen afvigelser konstateret

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden		
Kontrolmål ▶ *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.* ▶ *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Brud på persondatasikkerheden ▶ Databehandleren har en procedure for håndtering af brud på persondatasikkerheden. ▶ Databehandleren registrer alle databrud i relation til Totalløsningen ▶ Databehandler rapporterer brud på persondatasikkerheden til de dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer for brud på persondatasikkerheden. Vi har inspiceret log over registrerede sikkerhedsbrud hos databehandleren og observeret, at ingen af disse har berørt Totalløsningen. Det er derfor ikke mulighed at verificere, om der i givet fald sker korrekt og rettidig information til de dataansvarlige.	Ingen afvigelser konstateret

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

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."

Brian Bomholdt Nielsen
Partner
Serienummer: CVR:20222670-RID:99624274
IP: 77.243.xxx.xxx
2022-09-06 14:19:15 UTC
NEM ID

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2022-09-06 14:24:49 UTC
NEM ID

Jimmy Seneca Andersen
Udviklingschef
Serienummer: PID:9208-2002-2-563006304140
IP: 82.134.xxx.xxx
2022-09-06 14:57:24 UTC
NEM ID