NEMTILMELD.DK APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 20. NOVEMBER 2020 OM BESKRIVELSEN AF NEMTILMELD.DK 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

UAFHÆNGIG REVISORS ERKLÆRING 2

NEMTILMELD.DK APS' UDTALELSE 4

NEMTILMELD.DK APS' BESKRIVELSE AF NEMTILMELD.DK OG TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER 6

NemTilmeld.dk ApS 6

Behandling af personoplysninger 6

Databehandlerens garantier 7

Indgåelse af databehandleraftale 8

Instruks for behandling af personoplysninger 9

Fortrolighed og lovbestemt tavshedspligt 9

Tekniske og organisatoriske sikkerhedsforanstaltninger 9

Databeskyttelse gennem design og standardindstillinger 13

Sletning og tilbagelevering af personoplysninger 14

Bistand til den dataansvarlige 14

Fortegnelse over kategorier af behandlingsaktiviteter 14

Underretning om brud på persondatasikkerheden 14

Komplementerende kontroller hos den dataansvarlige 15

KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST 16

Artikel 28, stk. 1: Databehandlerens garantier 17

Artikel 28, stk. 3: Databehandleraftale 20

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger 21

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt 23

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger 24

Artikel 25: Databeskyttelse gennem design og standardindstillinger 38

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger 41

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige 42

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter 44

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden 45

SUPPLERENDE INFORMATION FRA NEMTILMELD.DK APS 47

UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 20. NOVEMBER 2020 OM BESKRIVELSEN AF NEMTILMELD.DK 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 NemTilmeld.dk ApS
NemTilmeld.dk ApS' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af NemTilmeld.dk ApS (databehandleren) pr. 20. november 2020 udarbejdede beskrivelse på side 6 til 15 af NemTilmeld.dk 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 på side 4 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme og implementere kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

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

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet på side 4.

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

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

Begrænsninger i kontroller hos en databehandler

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af NemTilmeld.dk, 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 på side 4. Det er vores opfattelse:

a. at beskrivelsen af NemTilmeld.dk 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. 20. november 2020, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 20. november 2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår på side 16 til 46.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens NemTilmeld.dk, 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 30. november 2020

BDO Statsautoriseret revisionsaktieselskab

Claus Bonde Hansen
Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Partner, chef for Risk Assurance

NEMTILMELD.DK APS' UDTALELSE

NemTilmeld.dk ApS varetager behandling af personoplysninger i forbindelse med NemTilmeld.dk 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 NemTilmeld.dk, 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.

NemTilmeld.dk ApS bekræfter, at den medfølgende beskrivelse på side 6 til 15 giver en retvisende beskrivelse af NemTilmeld.dk og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 20. november 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for NemTilmeld.dk, 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 kontroller, som vi med henvisning til afgrænsningen af NemTilmeld.dk har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af NemTilmeld.dk 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 NemTilmeld.dk, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

NemTilmeld.dk ApS bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 20. november 2020. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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

Nørresundby, den 26. november 2020

NemTilmeld.dk ApS

Thomas Kjærgaard
Direktør

NEMTILMELD.DK APS' BESKRIVELSE AF NEMTILMELD.DK OG TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

NEMTILMELD.DK APS

NemTilmeld.dk ApS leverer et internetbaseret selvbetjeningssystem, NemTilmeld.dk, som er hostet i eget servermiljø, placeret hos NemTilmeld.dk ApS i Danmark.

NemTilmeld.dk er et internetbaseret standardselvbetjeningssystem til administration af arrangementer. Selvbetjeningssystemet hjælper arrangører med at samle og håndtere mange af de opgaver, der har med administration af et arrangement at gøre, blandt andet håndtering af og overblik over tilmeldinger fra deltagere.

Administrationen af arrangementer i selvbetjeningssystemet sker via et administrationsområde på arrangørens konto. Arrangøren vælger, hvilke personer der skal have adgang til kontoens administrationsområde ved at give disse personer et brugernavn til kontoen.

Ved arrangørens brug af selvbetjeningssystemet behandler NemTilmeld.dk personoplysninger på vegne af arrangøren, dvs. den dataansvarlige.

Brugen af selvbetjeningssystemet NemTilmeld.dk er reguleret i forretningsbetingelserne for abonnement på NemTilmeld.dk samt en databehandleraftale, der fastsætter rettigheder og forpligtelser, når NemTilmeld.dk ApS behandler personoplysninger på vegne af den dataansvarlige.

Et sæt tilmeldingsbetingelser regulerer forholdet mellem den dataansvarlige og deltagerne til den dataansvarliges arrangementer.

BEHANDLING AF PERSONOPLYSNINGER

Karakteren af behandlingen

NemTilmeld.dk stiller det internetbaserede selvbetjeningssystem til rådighed for den dataansvarlige til administration af den dataansvarliges arrangementer. NemTilmeld.dk registrerer og opbevarer herigennem personoplysninger på vegne af den dataansvarlige.

Personoplysninger

Standardindstillingerne i selvbetjeningssystemet er sat op på en sådan måde, at der som udgangspunkt kun behandles almindelige personoplysninger, som:

- Navn
- Firma/Organisation
- Stillingsbetegnelse
- Telefonnummer
- E-mail

Hvis der skal betales for deltagelse til et arrangement igennem selvbetjeningssystemet, kræver selvbetjeningssystemet også følgende almindelige personoplysninger: adresse.

NemTilmeld.dk ApS behandler ikke yderligere almindelige personoplysninger, særlige kategorier af personoplysninger og personoplysninger om strafbare forhold, medmindre den dataansvarliges brugere instruerer NemTilmeld.dk til det gennem anvendelsen eller indstillingen af funktionerne i selvbetjeningssystemets administrationsområde.

Endvidere kan der på baggrund af sammenhængen i visse tilfælde udledes særlige kategorier af personoplysninger, f.eks. hvor deltagere er tilmeldt arrangementer hos en fagforening, interesseorganisation, politisk parti, patientforening mv.

De personer, som den dataansvarlige med et brugernavn har givet adgang til administrationsområdet på kontoen i selvbetjeningssystemet, kan ved oprettelse og redigering af et arrangement reelt indhente alle typer af personoplysninger gennem selvbetjeningssystemet. Hvordan den dataansvarliges brugere anvender og indstiller funktionerne i selvbetjeningssystemets administrationsområde, kan derfor gøre, at der behandles yderligere almindelige personoplysninger, særlige kategorier af personoplysninger og personoplysninger om strafbare forhold.

Kategorier af registrerede personer omfattet af databehandleraftalen

- Potentielle deltagere der besøger tilmeldingssiden for et arrangement
- Inviterede personer til den dataansvarliges arrangementer
- Kommende og tidligere deltagere til den dataansvarliges arrangementer
- Den dataansvarliges kontaktpersoner
- Den dataansvarliges brugere, som er de personer der via et brugernavn administrerer den dataansvarliges arrangementer i administrationsområdet, på den dataansvarliges konto i selvbetjeningssystemet.

Praktiske tiltag og kontrolforanstaltninger

NemTilmeld.dk ApS har vedtaget og indført it-sikkerhedspolitikker, -procedurer og -kontroller for virksomheden, virksomhedens medarbejdere og partnere.

NemTilmeld.dk ApS tager initiativer, der afspejler de risici, der er forbundet med den behandling, som NemTilmeld.dk ApS foretager på vegne af den dataansvarlige, således at der tages passende sikkerhedstiltag, og at risikoen for sikkerhedsbrud reduceres til et passende niveau.

NemTilmeld.dk ApS vurderer løbende det passende sikkerhedsniveau. Denne vurdering tager højde for de risici, der er forbundet med behandlingen.

Som grundlag for opdatering af tekniske eller organisatoriske tiltag gennemføres årligt en overordnet risikovurdering ud fra det generelle brug af selvbetjeningssystemet. Denne vurdering skal fremhæve sandsynlighed og konsekvenser for hændelser, der kan true beskyttelsen af de personoplysninger, NemTilmeld.dk ApS behandler på vegne af den dataansvarlige, inklusive tilfældige, forsætlige eller uforsætlige hændelser.

DATABEHANDLERENS GARANTIER

Informationssikkerhedspolitik

NemTilmeld.dk ApS har ud fra risikovurderingen udarbejdet politik for informationssikkerhed og databeskyttelse. Politikken beskriver de forholdsregler, som medarbejderne skal tage i den daglige brug af it mht. adgangskoder, placering for opbevaring af data, brug af hardware mv. Informationssikkerhedspolitikken gælder både data som er i digital form eller som er printet på papir.

Informationssikkerhedspolitikken skal være godkendt af NemTilmeld.dk ApS' ledelse. Relevante dele af informationssikkerhedspolitikken skal kommunikeres til medarbejderne.

Gennemgang af informationssikkerhedspolitik

NemTilmeld.dk ApS' ledelse har ansvaret for at informationssikkerhedspolitikken, og at reglerne er kendte og efterleves.

Informationssikkerhedspolitikken er en essentiel del af it-sikkerheden hos NemTilmeld.dk ApS og bliver vedligeholdt løbende, men som minimum taget op til intern revision 1 gang årligt samt ved væsentlige ændringer.

Organisering af informationssikkerhed

NemTilmeld.dk ApS har i informationssikkerhedspolitikken specificeret, hvorledes ansvaret for de enkelte områder er organiseret.

Informationssikkerhedspolitikken er til enhver tid tilgængelig for NemTilmeld.dk ApS' medarbejdere via et internt kommunikationsforum og gælder for NemTilmeld.dk ApS' ansatte, eksterne konsulenter, partnere, ejere og ledelse.

Rekruttering af medarbejdere

NemTilmeld.dk har en fast procedure for rekruttering af medarbejdere.

I forbindelse med baggrundstjek af en potentiel ny medarbejder er det NemTilmeld.dk ApS' ledelse, som har ansvaret for at sikre, at der tages minimum én reference samt indhentes straffeattestoplysninger på personer, der tilbydes ansættelse.

Alle medarbejdere skal som en del af ansættelseskontrakten underskrive NemTilmeld.dk ApS' tavsheds-erklæring.

Fratrædelse af medarbejdere

NemTilmeld.dk har en fast procedure for fratrædelse af medarbejdere.

I forbindelse med ansættelsesophør eller ophør af et samarbejdsforhold er det NemTilmeld.dk ApS' ansvar, at der gøres opmærksom på, at den indgåede tavshedserklæring også gælder efter et ansættelsesophør eller ophør af et samarbejdsforhold.

Samtlige aktiver, som fx computer eller telefon, der er udleveret til en medarbejder eller ekstern bruger, skal afleveres ved ansættelsesophør eller ophør af et samarbejdsforhold.

Uddannelse og instruktion af medarbejdere, der behandler personoplysninger

For at NemTilmeld.dk ApS' medarbejdere efterlever informationssikkerhedspolitikkerne og politikkerne for behandling af personoplysninger, vil der i forbindelse med ansættelsesstart og minimum én gang årligt gennemføres undervisning i sikkerhed, informationssikkerhedspolitikker og politikker for behandling af personoplysninger for alle NemTilmeld.dk ApS' medarbejdere.

Awareness og oplysningskampagner for medarbejdere

NemTilmeld.dk ApS gennemfører overfor medarbejderne løbende oplysningskampagner om informations-sikkerhed og behandling af personoplysninger fx i form af spørgeskemaundersøgelser, der benyttes som oplæg til opfølgende undervisning.

INDGÅELSE AF DATABEHANDLERAFTALE

NemTilmeld.dk ApS' standarddatabehandleraftaleskabelon godkendes skriftligt ved oprettelsen af en konto til selvbetjeningssystemet.

Databehandleraftaleskabelonen er i overensstemmelse med NemTilmeld.dk ApS' levering af selvbetje-ningssystemet til administration af arrangementer, og den godkendte aftale kan altid findes elektronisk på den dataansvarliges konto.

INSTRUKS FOR BEHANDLING AF PERSONOPLYSNINGER

Databehandleraftalen, der godkendes ved oprettelse af en konto til selvbetjeningssystemet, indeholder en instruks fra den dataansvarlige.

For at efterleve instruksen i databehandleraftalen, har NemTilmeld.dk ApS udarbejdet og implementeret skriftlige procedurer for medarbejderens behandling af personoplysninger samt kommunikation med den dataansvarlige og de registrerede.

Såfremt en medarbejder hos NemTilmeld.dk ApS er blevet opmærksom på, at den dataansvarlige har anvendt systemet uhensigtsmæssigt, er der udarbejdet procedurer for underretning af den dataansvarlige. De udarbejdede skriftlige procedurer gennemgås og opdateres løbende og minimum en gang årligt.

FORTROLIGHED OG LOVBESTEMT TAVSHEDSPLIGT

Som en del af ansættelseskontrakten, bliver alle medarbejdere hos NemTilmeld.dk gjort bekendt med og skriver under på, at de underlagt tavshedspligt.

Alle eksterne leverandører og konsulenter med adgang til personoplysninger i selvbetjeningssystemet skal være underlagt tavshedspligt ved indgåelse af kontrakt.
NemTilmeld.dk har på datoen for denne erklæring ikke nogen eksterne leverandører med adgang til personoplysninger i selvbetjeningssystemet.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

Risikovurdering

NemTilmeld.dk ApS foretager løbende, men som minimum én gang årligt, en overordnet kortlægning af risikoen for de registreredes rettigheder og frihedsrettigheder. Som en del af processen vurderes der på baggrund af de allerede implementerede risikominimerende foranstaltninger, om risikoen er minimeret tilstrækkeligt, eller om der er behov for at foretage yderligere tiltag.

Selve risikovurderingen består af flere dele:

- En kortlægning af alle de trusler og risici, behandlingen medfører, og en kategorisering (scoring, sandsynlighed og alvorlighed) heraf.
- En vurdering af, hvad der er passende tekniske og organisatoriske foranstaltninger til at sørge for, at databeskyttelsesforordningen overholdes, sammenholdt med de afledte implementeringsomkostninger.

Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse

NemTilmeld.dk ApS har udarbejdet en beredskabsplan i tilfælde af informationssikkerhedsbrud eller andre hændelser, som påvirker kritiske informationssystemer. Beredskabsplanen dækker både kommunikation med involverede parter, og detaljerede beredskabsplaner, indeholdende procedurer for fejlsøgning og procedurer for eventuel reetablering af de påvirkede informationssystemer.
Beredskabsplanen skal som minimum afprøves én gang årligt for at sikre, at beredskabsplanen er tidssvarende og effektiv. Afprøvningen af beredskabsplanen skal efterfølgende evalueres og dokumenteres.

Opbevaring af personoplysninger

For at forhindre uvedkommende i at tilgå personoplysninger, skal personoplysninger udelukkende opbevares hos NemTilmeld.dk ApS på krypterede datadiske, således at en udefrakommende ikke uden krypteringsnøgler og specialiseret viden kan tilgå personoplysninger.

NemTilmeld.dk ApS opbevarer ikke personoplysninger på vegne af den dataansvarlige i fysisk format, medmindre der foreligger en specifik instruks fra den dataansvarlige, fx i forbindelse med udskrift af navneskilte.

Fysisk adgangskontrol

NemTilmeld.dk ApS' kontor
NemTilmeld.dk ApS' kontorlokale er beskyttet mod uautoriseret adgang i form af elektronisk adgangskort, lås og indbrudsalarm, som er beskyttet med kode og koblet op til døgnbemandet vagtcentral.

Alle arbejdspc'er opbevares i individuelle aflåste rum i et aflåst værdiskab, når medarbejderne ikke er til stede på arbejdspladsen.

NemTilmeld.dk ApS' serverrum
NemTilmeld.dk ApS' serverrum er beskyttet mod uautoriseret adgang i form af elektronisk adgangskort og kode samt en indbrudsalarm, beskyttet med kode og koblet op til døgnbemandet vagtcentral. Al adgang til serverrummet logges.

NemTilmeld.dk ApS' udstyr som servere, switch, router, krydsfelt osv. i serverrum, er placeret i aflåst skab.

Udelukkende personer med arbejdsbetinget behov, har adgang til serverrummet. Gæster har kun adgang ledsaget af personer med autoriseret adgang til serverrummet.

NemTilmeld.dk ApS foretager som minimum én gang om året en gennemgang af den fysiske adgang til serverrum og øvrige faciliteter.

Fysisk sikkerhed

For NemTilmeld.dk ApS' serverrum er der etableret nødstrømforsyning, der midlertidigt vil kunne forsyne NemTilmeld.dk ApS' servere og produktionsmiljø med strøm til drift i en periode. Der er desuden etableret køleanlæg til køling af serverrummet. Kabler løber så vidt fysisk muligt i aflåste områder.

Logisk adgangskontrol

NemTilmeld.dk ApS' systemer er beskyttet af logisk adgangskontrol, som har til formål at sikre mod uautoriseret adgang, NemTilmeld.dk ApS' medarbejdere medvirker til beskyttelse af informationsaktiverne gennem korrekt brug af adgangskontrollerne.

Adgangsrettigheder
Brugernes adgange til systemer og data i systemer begrænses, så der kun gives adgang til systemer og data i det omfang brugerne har et arbejdsrelateret behov for adgangen.

NemTilmeld.dk ApS har en fast procedure for administration af brugerrettigheder, herunder i forbindelse med start, ændring og ophør af ansættelses- eller samarbejdsforhold. Proceduren foreskriver opdatering af fortegnelse for tildelte rettigheder til brugere på NemTilmeld.dk ApS' systemer. Dermed sikres, at alle brugeroprettelser og ændringer er autoriserede.
Privilegerede adgangsrettigheder tildeles kun, når der er et arbejdsrelateret behov, og tildeles kun ved forudgående godkendelse fra NemTilmeld.dk ApS' ledelse. NemTilmeld.dk ApS har udarbejdet en fast procedure for tildelingen af adgang til privilegerede adgangsrettigheder.

Minimum en gang årligt gennemgås fortegnelsen over brugerrettigheder for at sikre, at brugere og rettigheder stemmer overens med det arbejdsrelaterede behov.

Adgangskoder
NemTilmeld.dk ApS har i informationssikkerhedspolitikken fastsat regler for krav til adgangskoder, der skal følges af alle medarbejdere og eksterne konsulenter.

Alle medarbejdere hos NemTilmeld.dk ApS benytter et særligt program, som på sikker vis genererer og gemmer adgangskoder i krypteret form.

For alle brugerkonti med globale rettigheder i NemTilmeld.dk er det kun muligt at logge ind vha. to-faktor-login.

Der er på alle arbejdspc'er opsat automatisk skærmlås, der låser computeren efter 10 minutters inaktivitet.

Fjernarbejdspladser og fjernadgang til systemer og data

Kun NemTilmeld.dk ApS' pc'er må koble op på NemTilmeld.dk ApS' systemer. Kun særligt autoriserede medarbejdere har fjernadgang til NemTilmeld.dk ApS' interne netværk. Opkobling sker ved brug af VPN, og sikkerhedsmæssigt håndteres det, som hvis pc'en benyttes på kontoret. For at forbinde via VPN, skal der benyttes både certifikat og adgangskode.

Eksterne kommunikationsforbindelser

NemTilmeld.dk ApS' forbindelser til samarbejdspartnere foregår altid på sikre linjer enten som VPN-tunneler eller HTTPS-kommunikation via kendte IP-adresser. Dette for at beskytte data, som bliver transmitteret mellem NemTilmeld.dk og samarbejdspartnere.

NemTilmeld.dk ApS vedligeholder en oversigt over, hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå det interne netværk.

NemTilmeld.dk ApS har på datoen for denne erklæring ikke nogen eksterne kommunikationsforbindelser til samarbejdspartnere.

Kryptering af personoplysninger

NemTilmeld.dk ApS har udarbejdet en krypteringspolitik for kryptering af personoplysninger. Politikken definerer, hvilken protokol og den styrke der som minimum skal anvendes til kryptering.

Det er ikke tilladt at benytte bærbare medier til opbevaring af personoplysninger. Et bærbart medie er f.eks. USB-nøgle, ekstern harddisk, DVD mv.

For at forebygge brud på informationssikkerheden, anvender NemTilmeld.dk ApS altid krypterede forbindelser, når der overføres personoplysninger via internt netværk, internettet eller via e-mail.

Firewall

NemTilmeld.dk ApS benytter firewalls, som beskyttelse mod uautoriseret adgang til servere og systemer. Firewalls er konfigureret, så der kun anvendes de porte og services, der er behov for.

Konfigurationen af firewalls gennemgås løbende og det kontrolleres at opsætningen er i overensstemmelse med det tiltænkte.

Netværkssikkerhed

NemTilmeld.dk ApS' interne netværk er fysisk adskilt i forskellige sikkerhedszoner. Målsætningen er, at servere, der bruges i en zone, er svære at angribe eller tilgå fra en anden sikkerhedszone. Der bruges firewalls i op til 3 lag på netværkene for at beskytte de interne netværk.

Beskyttelse mod malware og virus

Alle arbejdspc'er hos NemTilmeld.dk ApS benytter et særligt operativsystem, der ved hjælp af domæner, rettigheder, firewall og virtuelle maskiner holder de forskellige funktioner og adgange til systemer adskilt, således at evt. trusler som virus, malware eller lign. ikke har mulighed for at forvolde skade på data, der er væsentlige for driften.

Effektiviteten af operativsystemets evne til at modstå disse trusler evalueres løbende af NemTilmeld.dk ApS med henblik på at forbedre it-sikkerheden.

Sårbarhedsscanning og penetrationstests

NemTilmeld.dk ApS får minimum én gang årligt foretaget en sårbarhedsscanning af netværket. Resultater af scanningen er dokumenteret i en rapport, som NemTilmeld.dk ApS gennemgår.

NemTilmeld.dk ApS følger løbende op på konstaterede svagheder og håndterer svaghederne ud fra en risikovurdering. Hvorledes de fundne svagheder bliver håndteret af NemTilmeld.dk ApS dokumenteres.

Sikkerhedskopiering og retablering af data

NemTilmeld.dk ApS foretager daglig backup af produktionsdata og testdata, herunder også kildekode, konfiguration m.m. Der foretages backup af alle virtuelle servere i form af snapshots. Det sikres dagligt, at backuppen er foretaget.

En kopi af backuppen opbevares på en separat lokation.

NemTilmeld.dk ApS sikrer, at produktionsdata kan reetableres baseret på foretaget backup gennem minimum 4 årlige reetableringstests.

Vedligeholdelse af systemsoftware

NemTilmeld.dk ApS' servere tjekker løbende for tilgængelige systemopdateringer med henblik på at sikre systemers tilgængelighed og sikkerhed.

NemTilmeld.dk ApS har implementeret en proces, så der regelmæssigt foretages systemopdateringer på arbejdspc'er.

Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger

NemTilmeld.dk ApS har etableret logning således, at alle succesfulde eller mislykkede adgangsforsøg til NemTilmeld.dk ApS' systemer og data logges.

NemTilmeld.dk ApS' systemer logger i applikationsloggen, når brugere foretager visning, oprettelse, ændring, eller sletning af data. Der logges, når brugere foretager ændringer via selvbetjeningssystemet NemTilmeld.dk eller direkte i databaser.

Loggede oplysninger vedrørende persondataadgang anonymiseres efter 3 år. Persondata i adgangslogning slettes efter 6 måneder.

Logoplysningerne er beskyttede. Det betyder, at det kun er brugere med systemadministratorrettigheder, som har mulighed for at foretage ændringer i logs.

Overvågning

NemTilmeld.dk ApS har med henblik på at sikre systemers tilgængelighed og sikkerhed, etableret overvågning af forskellige parametre i produktionsmiljøet, heriblandt oppetid, ydeevne og kapacitet.

Ved de på forhånd definerede grænseværdier bliver der givet alarm, således at NemTilmeld.dk ApS kan reagere på disse og foretage de nødvendige handlinger. Det dokumenteres i hændelsesloggen, såfremt der er tale om væsentlige afvigelser eller hændelser, som observeres eller indrapporteres fra f.eks. egne medarbejdere, kunder m.m.

Reparation og service samt bortskaffelse af it-udstyr

NemTilmeld.dk ApS har en fast procedure for reparation af it-udstyr. Proceduren foreskriver bl.a., at såfremt udstyr indeholder personoplysninger, skal data slettes fra udstyret på sikker vis før dette sendes til reparation.

NemTilmeld.dk ApS har en fast procedure for bortskaffelse af it-udstyr. Proceduren foreskriver bl.a., at såfremt udstyr indeholder personoplysninger, skal data slettes fra udstyret på sikker vis før dette bortskaffes eller genbruges.

NemTilmeld.dk ApS fører en log over repareret og destrueret it-udstyr.

DATABESKYTTELSE GENNEM DESIGN OG STANDARDINDSTILLINGER

Udvikling og vedligeholdelse af systemer

NemTilmeld.dk ApS ønsker at tænke sikkerhed og databeskyttelse ind som en integreret del af udvikling og vedligeholdelse af selvbetjeningssystemet. NemTilmeld.dk ApS har derfor udarbejdet en procedure, der benyttes for alle udviklings- og vedligeholdelsesopgaver.

Proceduren har bl.a. til formål at sikre, at der ved væsentlige systemændringer foretages en risikovurdering. Proceduren har desuden generelt til formål at have fokus på databeskyttelse gennem Privacy by design og Privacy by default.

Et andet led i risikovurderingen indebærer, at der ved væsentlige systemændringer fastlægges krav til test og roll-back planlægning, således at der kan iværksættes foranstaltninger for at minimere problemer ved udrulning i produktionsmiljøet.

NemTilmeld.dk ApS minimerer angrebsflader ved kun at aktivere services på systemer, der er nødvendige for at selvbetjeningssystemet NemTilmeld.dk kan fungere. Som en del af kvalitetssikringen gennemfører NemTilmeld.dk unit-test på kodeniveau og automatisk test via selvbetjeningssystemet før udrulning.

NemTilmeld.dk foretager al udvikling in-house og har al ophavsret til kildekoden. Medarbejdere må derfor ikke kopiere kildekoden til eget brug. Kildekoden må kun befinde sig på udviklingsservere, produktionsservere, versionsservere og backupservere, hvor versionsserveren registrerer alle ændringer af kildekoden. Kun NemTilmeld.dk ApS' egne udviklere har adgang til kildekoden.

Adskillelse af udviklings-, test og produktionsmiljø

NemTilmeld.dk ApS har adskilt udvikling og test fra produktionsmiljøerne. Produktionsmiljøerne kører på udstyr, der kun bruges til produktion.

Udvikling og test udføres i miljøer, som er adskilte fra produktionssystemerne.

Test af ny eller ændret funktionalitet indgår som en del af proceduren for alle udviklings- eller ændringsopgaver inden udrulning til produktionsmiljøet. Ny eller ændret funktionalitet udvikles og testes i separate udviklingsmiljøer.

Selvbetjeningssystemet testes på kodeniveau med unit-test og automatisk test via selvbetjeningssystemets brugergrænseflade.

NemTilmeld.dk ApS benytter et versionsstyringssystem til at registrere alle ændringer i kildekoden.

Personoplysninger i udviklings- og testmiljø

NemTilmeld.dk anvender konstruerede testdata i udviklings- og testmiljø. I særlige tilfælde, hvor det er påkrævet til test af funktionalitet der alene kan udføres ved at anvende produktionsdata til test, skal der foretages en individuel vurdering af behovet og tidsrummet hvor data er tilgængelige for test.
Nemtilmeld.dk´s ledelse skal godkende anvendelse af produktionsdata i testmiljø. Godkendelse skal foreligge før der sker overførsel af data til testmiljø. Omfang, tidsrum og tidspunkt for sletning skal fremgå af godkendelse. Produktionsdata i testmiljøet slettes straks efter test.
I testmiljøet er personoplysninger beskyttet på samme niveau som personoplysninger i produktionsmiljø.

SLETNING OG TILBAGELEVERING AF PERSONOPLYSNINGER

Selvbetjeningssystemet NemTilmeld.dk er jfr. instruksen i databehandleraftalen sat op til at slette indsamlede personoplysninger om deltagere to år efter det pågældende arrangements afvikling. Det er endvidere muligt at opsætte særlige sletteregler for individuelle oplysninger, således at fx kosthensyn slettes dagen efter et arrangements afvikling.

Den dataansvarlige har, når som helst, mulighed for at ændre, hvor længe data opbevares, samt at gennemføre en sletning af alle personoplysninger for afviklede arrangementer. Undtaget herfra er oplysninger, der jfr. bogføringsloven kræves opbevaret af NemTilmeld.dk. Disse data slettes jfr. gældende lovgivning.

En gang om året foretager NemTilmeld.dk ApS egenkontrol af de foretagne sletninger i selvbetjeningssystemet for at sikre, at de ønskede personoplysninger er blevet slettet.

Den dataansvarlige kan til enhver tid eksportere data om deltagere til aktuelle og tidligere arrangementer på deres konto i selvbetjeningssystemet.

BISTAND TIL DEN DATAANSVARLIGE

De registreredes rettigheder

NemTilmeld.dk ApS har udarbejdet online guides, som beskriver, hvordan den dataansvarlige gennem brugen af selvbetjeningssystemet kan overholde de registreredes rettigheder. NemTilmeld.dk ApS har desuden udarbejdet procedurer for medarbejdernes håndtering af henvendelser fra en registreret.

Modtager den dataansvarlige en henvendelse om indsigt, er det i selvbetjeningssystemet muligt at give indsigt i alle de personoplysninger, der er registreret om vedkommende i selvbetjeningssystemet.

Revision og inspektion

NemTilmeld.dk ApS får en gang årligt udarbejdet en revisorerklæring af typen ISAE 3000, som vedrører de tekniske og organisatoriske sikkerhedsforanstaltninger, NemTilmeld.dk ApS har foretaget omkring behandlingen og beskyttelsen af personoplysninger.

NemTilmeld.dk ApS stiller de nødvendige ressourcer og informationer til rådighed ved fysiske tilsyn, initieret af den dataansvarlige eller Datatilsynet.

FORTEGNELSE OVER KATEGORIER AF BEHANDLINGSAKTIVITETER

NemTilmeld.dk ApS har udarbejdet en fortegnelse over kategorier af de behandlingsaktiviteter, som NemTilmeld.dk ApS udfører som databehandler. Fortegnelsen opdateres ved væsentlige ændringer og gennemgås minimum en gang om året.

Fortegnelsen opbevares elektronisk og sikkerhedskopieres en gang om måneden og kan udleveres til Datatilsynet efter anmodning.

UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

NemTilmeld.dk ApS har udarbejdet procedure for vurderingen og identifikation af brud på persondatasikkerheden for at sikre, at den dataansvarlige uden unødig forsinkelse underrettes om brud på persondatasikkerheden.

NemTilmeld.dk ApS har udarbejdet skabeloner for at sikre, at underretningen til den dataansvarlige indeholder alle nødvendige oplysninger, der er til rådighed for NemTilmeld.dk ApS.
NemTilmeld.dk ApS foretager erfaringsopsamling efter alle brud, som sammen med brud på persondatasikkerheden registreres af NemTilmeld.dk ApS i en log.

KOMPLEMENTERENDE KONTROLLER HOS DEN DATAANSVARLIGE

NemTilmeld.dk ApS har i databehandleraftalens afsnit 3 beskrevet de forpligtelser, som den dataansvarlige selv har i forbindelse med brugen af selvbetjeningssystemet.

Behandling af personoplysninger

- Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret, EU- eller EØS-medlemsstaternes nationale ret og databehandleraftalen.
- Den dataansvarlige er ansvarlig for at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
- Den dataansvarlige er ansvarlig for at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.
- Den dataansvarlige er ansvarlig for at gennemlæse og kontrollere de automatisk genererede tilmeldingsbetingelser for at sikre, at de er tilstrækkelige i forhold til reglerne i databeskyttelsesforordningen og databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, som godkendes inden tilmeldinger til et arrangement kan modtages.

Brugere af administrationsområdet

- Den dataansvarlige er ansvarlig for at oprette og ajourføre en liste over brugerkonti, som har adgang til den dataansvarliges konto i systemet.
- Den dataansvarlige er ansvarlig for at sikre, at de oprettede brugerkonti anvender systemet i overensstemmelse med databeskyttelsesforordningen og databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og databehandleraftalen.
- Den dataansvarlige har det fulde ansvar for at vurdere og forholde sig til evt. problemstillinger, der kan opstå i forbindelse med deling af login-detaljer.
- Den dataansvarlige er ansvarlig for at informere de oprettede brugere om forpligtelserne i forhold til databehandleraftalen og forretningsbetingelserne.

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 NemTilmeld.dk ApS' beskrivelse af NemTilmeld.dk 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 NemTilmeld.dk ApS, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 20. november 2020.

Udførte testhandlinger

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

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

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, baseret på risikovurdering. ▶ Informationssikkerhedspolitikken er kommunikeret til medarbejdere.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret informationssikkerhedspolitikken. Vi har observeret, at politik for behandling af personoplysninger indgår som en del af informationssikkerhedspolitikken. Vi har inspiceret dokumentation for medarbejderinformation i relation til opdatering af informationssikkerhedspolitikken.	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret informationssikkerhedspolitik og databehandlerens årshjul for kontroller. Vi har observeret, at gennemgang og revidering af informationssikkerhedspolitikken er planlagt til gennemførelse én gang årligt i juni. Vi har observeret, at informationssikkerhedspolitikken er opdateret den 26. juni 2020.	Ingen afvigelser konstateret.
Organisering af informationssikkerhed ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed og databeskyttelse.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret informationssikkerhedspolitikken. Vi har observeret, at organisering og ansvar af informationssikkerhed er	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**
	fastlagt i politikken. Vi har ligeledes observeret, at informationssikkerhedspolitikken er forankret i databehandlerens ledelse.	
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse. ▶ Databehandleren udfører baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret informationssikkerhedspolitikken samt procedure og kontrolskema for ansættelse af medarbejdere. Vi har observeret, at der er udformet procedurer for screening og baggrundstjek af kandidater. Vi har for en udvalgt stikprøve inspiceret kontrolskema for ansættelse.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Databehandleren har udarbejdet og implementeret en procedure for off-boarding af fratrådte medarbejdere. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne tavshedserklæring fortsat er gældende.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for fratrædelse. Vi har observeret, at der er udformet og implementeret procedure for fratrædelse og off-boarding af medarbejdere. Vi har for en udvalgt stikprøve inspiceret dokumentation for fratrædelse. Vi har observeret, at medarbejderen orienteres om medarbejderens fortsatte tavshedspligt. Vi har ligeledes observeret, at den fratrædende medarbejder underskriver erklæring om fortsat tavshedspligt ved fratrædelsen.	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
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger - Databehandleren afholder awareness-træning af nye medarbejdere i forhold til databeskyttelse og informationssikkerhed ved af ansættelsen. - Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. - Databehandleren gennemfører mindst én gang årligt, uddannelse af medarbejdere i forhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for undervisning og instruktion af medarbejdere. Vi har for en udvalgt stikprøve inspiceret dokumentation for instruktion og introduktionskursus for medarbejderen. Vi har inspiceret dokumentation for uddannelse af medarbejdere i databeskyttelse og informationssikkerhed. Vi har observeret, at der er gennemført uddannelse i databeskyttelse den 27. april 2020. Vi har ved forespørgsler hos relevant personale fået bekræftet, at medarbejderen er undervist og instrueret i informationssikkerhed og behandling af personoplysninger.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere - Databehandleren udfører løbende awareness-kampagner i form af information og spørgeskemaer.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret dokumentation for awareness-træning. Vi har observeret, at der er gennemført awareness-træning af medarbejdere i form af spørgeskemaer og opfølgende undervisning den 27. april 2020.	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. - Databehandleraftaler underskrives eller godkendes i systemet ved indgåelse af kundeforholdet og opbevares elektronisk.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for indgåelse af databehandleraftaler. Vi har inspiceret databehandlerens skabelon for databehandleraftaler med dataansvarlige. Vi har observeret, at denne lever op til kravene databeskyttelsesforordningens artikel 28. Vi har inspiceret systemudtræk over dataansvarlige. Vi har for en stikprøve, inspiceret databehandleraftaler. Vi har observeret at der er indgået databehandleraftale med dataansvarlige. Vi har ligeledes observeret at databehandleraftale og fortegnelse over dataansvarlige opbevares elektronisk.	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 foretaget interview af passende personale og inspiceret dokumentation. Vi har for en stikprøve inspiceret databehandleraftaler mellem databehandler og den dataansvarlige. Vi har observeret, at databehandleraftalen indeholder instruks fra den dataansvarlige.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig. ▶ Databehandlerens procedurer gennemgås og opdateres løbende og minimum en gang årligt.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer samt instruktioner for medarbejdere. Vi har observeret, at der er udarbejdet instrukser for medarbejdernes behandling af personoplysninger og kommunikation med dataansvarlige og de registrerede. Vi har inspiceret årshjul for tilbagevendende kontroller. Vi har observeret, at procedurer for behandling af persondata opdateres mindst én gang årligt. Vi har inspiceret databehandlerens årshjul for kontroller. Vi har observeret, at revidering af procedurer og retningslinjer for behandling af personoplysninger er gennemført i september 2020.	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**
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. ▶ Databehandleren underretter uden unødigt ophold den dataansvarlige i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har foretaget interview med passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer samt instruktioner for medarbejdere. Vi har observeret, at der er udarbejdet procedure og instruks for underretning af dataansvarlige i tilfælde, hvor den dataansvarliges instruks strider mod persondatalovgivningen. Der har ikke været en hændelse til brug for test af kontrollen, hvorfor vi ikke kan udtale os herom. Vi har ved forespørgsler hos relevant personale fået bekræftet medarbejdernes forståelse for kontrollen.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt		
Kontrolmål ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Eksterne leverandører/konsulenter med adgang til personoplysninger, er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har for en udvalgt stikprøve, inspiceret ansættelseskontrakt. Vi har observeret at medarbejdere er underlagt tavshedspligt via vilkår i ansættelseskontrakten. Vi har observeret, at der ikke er eksterne leverandører med adgang til databehandlerens systemer, hvorfor der ikke er en dokumenter til brug for test af kontrollen for tavshedspligt ved kontraktindgåelse med eksterne leverandører. Vi har inspiceret politikker og procedurer. Vi har ligeledes ved forespørgsler hos relevante personale fået bekræftet medarbejdernes forståelse for kontrollen.	Ingen afvigelse 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, 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. ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedurer og dokumentation for risikovurdering. Vi har observeret, at der er gennemført risikovurdering i forhold til den registreredes rettigheder. Vi har observeret, at risikovurdering er opdateret den 13. maj 2020. Vi har observeret, at der er foretaget risikovurdering ud fra identificerede trusler. Vi har ligeledes observeret, at der er foretaget vurdering af implementerede foranstaltninger, der minimerer risiciene. Vi har inspiceret databehandlerens årshjul for kontroller. Vi har observeret, at revidering af risikovurdering er planlagt til gennemførelse en gang årligt.	Ingen afvigelse 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.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for beredskabsplaner. Vi har observeret, at der er udformet procedurer for beredskab.	Ingen afvigelse 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
▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanen er tidssvarende og effektive i kritiske situationer. ▶ Beredskabstest dokumenteres og evalueres.	Vi har inspiceret beredskabsplaner. Vi vurderer at disse er passende udformet. Vi har inspiceret databehandlerens årshjul for kontroller. Vi har observeret, at der er planlagt årlig test af beredskabsplanen. Vi har inspiceret dokumentation for test af beredskabsplanen. Vi har observeret, at der er foretaget test af beredskabsplanen den 26. juni 2020.	
Opbevaring af personoplysninger ▶ Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov. ▶ Fortrolige digitale personoplysninger opbevares i krypteret form på datadiske. ▶ Der opbevares ikke fysiske materialer, indeholdende personoplysninger der behandles på vegne af dataansvarlige.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedure for brugeradministration. Vi har ligeledes inspiceret oversigt over medarbejdere og brugerrettigheder. Vi har observeret, at adgang til personoplysninger er tildelt medarbejdere med et arbejdsbetinget behov. Vi har inspiceret systemkonfiguration for server, hvorpå der opbevares personoplysninger. Vi har observeret, at harddiske er krypterede. Vi har inspiceret politikker for opbevaring af personoplysninger. Vi har observeret, at der er udformet politik og instruktion om, at der ikke må udskrives personoplysninger, der behandles på vegne af dataansvarlige.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget fysisk inspektion i databehandlerens lokaler. Vi har observeret, at der ikke forefindes fysiske materialer med personoplysninger.	
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. - Der kræves adgangskort og kode ved adgang til datacenter. - Datacenter er monteret med alarmsystem. - Alle adgange i datacenter registreres og logges. - Servere er placeret i aflåste skabe. - Der foretages løbende, og som minimum en gang om året, gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter. - Arbejdsstationer opbevares i aflåst værdiskab, når disse ikke anvendes. - Gæster skal ledsages ved adgang i kontorområder.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret de fysiske lokaler. Vi har observeret, at der skal anvendes elektronisk nøglekort ved adgang til kontorområdet og bygningen. Vi har foretaget fysisk inspektion i serverrum. Vi har observeret, at der skal anvendes adgangskort og kode ved adgang. Vi har inspiceret system for logning af adgange til serverrum. Vi har observeret, at adgang til serverummet logges. Vi har observeret, at der er installeret aflåste bure for placering af serverskabe. Vi har observeret, at servere er monteret i aflåste bure. Vi har inspiceret udleveringsoversigt over nøgler til kontorlokaler. Vi har observeret, at alle nøgler er registreret med beskrivelse af medarbejdere, der er udleveret nøgle til. Vi har inspiceret databehandlerens årshjul for kontroller. Vi har observeret, at der er planlagt årlig gennemgang af fysisk ad-	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
	gangskontrol. Vi har inspiceret dokumentation for årlig gennemgang af medarbejdere med fysisk adgang. Vi har observeret, at der er foretaget gennemgang af liste over medarbejdere med fysisk adgang til kontorlokaler og serverum den 6. juli 2020. Vi har inspiceret værdiskab i kontorlokalet. Vi har observeret, at arbejdsstationer, der ikke er i brug opbevares i aflåst værdiskab. Vi har observeret, at gæster ledsages ved færdsel i databehandlerens lokaler.	
Fysisk sikkerhed ▶ Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. Den fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav. ▶ Databehandleren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum omfattende følgende forhold: - Klima - Strøm - Adgang - Alarmmonitorering - Brandalarm - Kabling	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret serverrum. Vi har observeret, at fysisk sikring af serverrum er i overensstemmelse med informationssikkerhedspolitikken. Vi har observeret, at servere er beskyttet mod varme ved køleanlæg. Vi har inspiceret strømforsyningen. Vi har observeret, at der er etableret redundant strømtilførsel og installeret UPS. Vi har observeret, at der er installeret røgalarm. Vi har observeret at drift af klimaanlæg og brandalarmering er en del af lejemål for kontorlokaler og serverrum.	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 netværksudstyr og kabling. Vi har observeret, at kabling og netværksudstyr i serverrum er afskærmet og beskyttet af lås.	
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration, der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriserede. ▶ 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. ▶ Der foretages logning af alle adgange til systemer og data. ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation. ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter. ▶ System for opbevaring af autentificeringsoplysninger er krypteret.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for adgangsstyring. Vi har observeret, at procedure og ansvar fremgår af informationssikkerhedspolitikken. Vi har inspiceret dokumentation for tildelte brugerrettigheder. Vi har observeret, at der tildeles adgang ud fra et arbejdsbetinget behov. Vi har inspiceret procedure og dokumentation for brugeroprettelse. Vi har observeret, at adgangsrettigheder tildeles ud fra medarbejderens arbejdsbetingede behov. Vi har inspiceret databehandlerens årshjul for kontroller. Vi har observeret, at der er planlagt årlig gennemgang af brugere og brugerrettigheder. Vi har observeret at der er foretaget gennemgang af tildelte rettigheder til servere d. 26. juni 2020.	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
▸ Arbejdsstationer låser automatisk efter 10 minutter.	Vi har inspiceret dokumentation for tildelte privilegerede adgange til servere og systemer. Vi har observeret, at der er foretaget gennemgang af tildelte rettigheder til servere den 26. juni 2020. Vi har inspiceret system for logning af adgange til systemer. Vi har observeret, at alle forsøg på login registreres i adgangslog. Vi har observeret login til backend for nemtilmeld.dk. Vi har observeret, at der skal anvendes to-faktor autentifikation ved adgang til systemet. Vi har inspiceret informationssikkerhedspolitikken. Vi har observeret, at der er udformet politikker for anvendelse af og udformning af adgangskoder. Vi har inspiceret system for opbevaring af adgangskoder. Vi har observeret at adgangskoder til fællessystemer opbevares i krypteret database. Vi har for en stikprøve inspiceret indstillinger for skærmlås for arbejdsstationer. Vi har observeret, at skærm låses automatisk efter 10 minutter.	
Fjernarbejdspladser og fjernadgang til systemer og data ▸ Der er udformet og implementeret politikker for tildeling af fjernadgang. ▸ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse.	Vi har foretaget interview af passende personale og inspiceret dokumentation.	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
▸ Fjernadgang skal foregå via certifikat og adgangskode.	Vi har inspiceret informationssikkerhedspolitikken. Vi har observeret, at der er udformet politikker for anvendelse og tildeling af fjernadgang til personoplysninger. Vi har inspiceret systemkonfiguration for VPN-forbindelse. Vi har observeret, at der anvendes certifikat og adgangskode ved oprettelse af krypteret VPN-forbindelse.	
Eksterne kommunikationsforbindelser ▸ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og SSH fra kendte IP-adresser. ▸ Udveksling af personoplysningerne via e-mail sker vha. sikkermail-løsning. ▸ Eksterne kommunikationsforbindelser er krypteret via SSH. ▸ Databehandleren har en oversigt over, hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå netværket.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret systemkonfiguration for firewall og servere. Vi har observeret, at der skal opsættes VPN -forbindelse til kontornetværket for at opnå adgang til servere. Vi har inspiceret konfiguration af firewall og netværksoversigt. Vi har observeret, at der er konfigureret filtrering af netværkstrafik til servere. Vi har inspiceret konfiguration for e-mail-server. Vi har observeret, at denne er konfigureret til at anvende kryptering ved afsendelse af e-mails. Vi har inspiceret dokumentation for egenkontrol af kryptering. Vi har observeret, at der er udført kontrol den 4. juli 2020.	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 observeret, at der ikke er eksterne kommunikationsforbindelser til interne servere.	
Kryptering af personoplysninger - Databehandleren har implementeret en krypteringspolitik for kryptering af personoplysninger. Politikken definerer styrken og protokollen for kryptering. - Der anvendes ikke bærbare medier til opbevaring eller transport af personoplysninger. - Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker for kryptering af personoplysninger. Vi har observeret, at krav til kryptering er fastlagt i politikken. Vi har observeret, at medarbejdere er informeret om, at personoplysninger ikke må opbevares på bærbare medier. Vi har inspiceret konfiguration for e-mail-server. Vi har observeret, at denne er konfigureret til at anvende kryptering ved afsendelse af e-mails.	Ingen afvigelser konstateret.
Firewall - Databehandler anvender kun services/porte, som der er behov for. - Firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret systemkonfiguration for firewall. Vi har observeret, at firewall er konfigureret med eksplicit adgang for accepterede UDP- og TCP-porte. Vi har inspiceret procedure for periodisk review af konfiguration af firewall. Vi har observeret, at der ikke er et review til brug for test af kontrollen, hvorfor vi ikke kan udtale os herom.	Ingen afvigelser konstateret.

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

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har ved forespørgsler hos relevant personale fået bekræftet medarbejdernes forståelse for kontrollen.	
Netværkssikkerhed ▶ Netværkstopologien er struktureret efter best-practice principper, hvilket betyder, at servere, som driver applikationer, ikke kan nås direkte fra internettet. ▶ Databehandlerens netværk er segmenteret med firewall. ▶ Databehandleren anvender firewall for at beskytte internt netværk.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret dokumentation for netværkstopologien. Vi har observeret, at netværket er segmenteret, og at servere er beskyttet af firewall.	Ingen afvigelser konstateret.
Beskyttelse mod malware og virus ▶ Der er implementeret passende tekniske foranstaltninger mod malware-risici. ▶ Der foretages løbende vurdering af de tekniske sikkerhedsforanstaltningers effektivitet.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret systemdokumentation og konfiguration for arbejdsstationer. Vi har observeret, at der anvendes en temporær isoleret virtuel maskine ved enhver opstart af applikationer. Vi har gennemgået beskyttelse af netværk ved anvendelse af kritiske applikationer. Vi har observeret, at der for kritiske applikationer er konfigureret firewall der begrænser adgang til netværk og internet services. Vi har inspiceret risikovurdering for malwarebeskyttelse.	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
Sårbarhedsscanning og penetrationstests ▶ Mindst en gang årligt foretages der en sårbarhedsscanning af databehandlerens netværk. Resultatet dokumenteres i en rapport. ▶ Databehandleren gennemgår rapporten og følger op på konstateret svagheder. ▶ Databehandleren håndterer eventuelle sårbarheder ud fra en risikovurdering. ▶ Databehandleren har dokumenteret håndteringen/mitigeringen af fundne sårbarheder.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret dokumentation for sårbarhedsscanning. Vi har observeret, at der foretages løbende sårbarhedsscanning, udbedring og gentest af identificerede sårbarheder. Vi har inspiceret system for dokumentation. Vi har observeret, at håndtering af sårbarheder dokumenteres.	Ingen afvigelser konstateret.
Sikkerhedskopiering og retablering af data ▶ Der foretages dagligt backup af systemer og data. ▶ Der foretages snapshot af alle virtuelle servere. ▶ Der er udformet procedurer for daglige kontroller af sikkerhedskopiering: ▶ Der udføres restore-tests 4 gange årligt.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret systemkonfiguration for sikkerhedskopiering. Vi har observeret, at der foretages daglig sikkerhedskopiering for alle servere. Vi har inspiceret procedurer og dokumentation for systemgendannelse. Vi har observeret, at der er udformet procedurer for systemgendannelse. Vi har ligeledes observeret, at der er udformet beskrivelser til brug for reetablering. Vi har inspiceret system for overvågning. Vi har observeret, at der sendes alarm ved fejl i sikkerhedskopieringen.	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 for kontroller og dokumentation for kontrollen for restore test. Vi har observeret, at der er planlagt test af sikkerhedskopiering 4 gange årligt. Vi har observeret, at der er foretaget test af reetablering den 24. juni 2020.	
Vedligeholdelse af systemsoftware ▶ Operativsystemsoftware på servere og arbejdsstationer opdateres løbende. ▶ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed, herunder en automatisk eller manuel overvågningsproces.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret system for kontrol af opdatering af systemsoftware på servere. Vi har observeret at der kontrolleres for opdateringer hver time. Vi har observeret at opdateringer på servere bliver installeret manuelt, når disse er tilgængelige. Vi har observeret, at der senest er foretaget opdateringer på alle servere den 18. juni 2020. Vi har inspiceret informationssikkerhedspolitikken. Vi har observeret, at der er politikker for opdatering af arbejdsstationer. Vi har for en udvalgt stikprøve inspiceret dokumentation for opdatering, og vi har observeret, at applikationer og operativsystem er opdateret.	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 ▸ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▸ Alle brugerændringer i system og databaser logges. ▸ Loggen slettes efter den fastsatte retentionsperiode. ▸ Logning for persondataadgang anonymiseres efter 3 år. ▸ Personoplysninger i adgangslogning slettes efter 6 måneder.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret dokumentation for logning. Vi har observeret, at der er implementeret logning for adgangsforsøg til systemer. Vi har inspiceret applikationslog. Vi har observeret, at alle brugerhandlinger i applikationen logges i databasen. Vi har inspiceret database-logning. Vi har observeret, at alle handlinger i database logges. Vi har inspiceret procedure og systemkonfiguration for sletning af logning. Vi har observeret, at personoplysninger i adgangslogning slettes efter 6 måneder. Der har ikke været en hændelse til brug for test af kontrollen for anonymisering af logdata efter 3 år, hvorfor vi ikke kan udtale os om dette. Vi har ved forespørgsler hos relevant personale, fået bekræftet medarbejdernes forståelse for kontrollen. Vi har ligeledes inspiceret systemkonfiguration for anonymisering af logdata efter 3 år. Vi har observeret at der foretages automatisk sletning af personhenførbare oplysninger i adgangslog, hvor registreringer der er over 3 år slettes i databasen.	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
Overvågning - Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. - Databehandleren notificeres om identificerede alarmer og følger op herpå. Væsentlige afvigelser dokumenteres i hændelseslog.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret systemkonfiguration for kapacitetsovervågning. Vi har observeret, at servere overvåges for kapacitetsudnyttelse. Vi har inspiceret system for serviceovervågning. Vi har observeret, at der er konfigureret overvågning af kritiske services og applikationer. Vi har observeret, at der er tilknyttet alarmering til overvågning. Vi har inspiceret hændelseslog. Vi har observeret, at væsentlige hændelser er dokumenteret i hændelsesloggen.	Ingen afvigelser konstateret.
Reparation og service samt bortskaffelse af it-udstyr - Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger. - Databehandleren foretager sikker sletning af data på databærende medier eller overskrivning i forbindelse med bortskaffelse og genbrug. - Databehandleren fører en oversigt af destrueret it-udstyr.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret informationssikkerhedspolitikken. Vi har observeret, at der er udformet politikker for bortskaffelse og kassation af it-udstyr.	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 procedure for reparation og destruktion af udstyr. VI har inspiceret log for reparation og bortskaffelse. Vi har observeret, at der ikke har været en hændelse til brug for test af kontrollen for reparation af it-udstyr. Vi har ved forespørgsler fået bekræftet medarbejdernes forståelse for kontrollen.	

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 backend systemer ▶ Databehandleren arbejder ud fra Privacy by design-principper i udvikling og vedligeholdelsesopgaver. ▶ Risikovurdering af systemændringer udføres for at sikre databeskyttelse gennem design og standardindstillinger.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for udvikling og vedligeholdelse. Vi har observeret at udviklere skal evaluere udviklingsopgaver i forhold til kendte svagheder. Vi har observeret, at personoplysninger skal sikres i enhver udviklingsopgave gennem Privacy by design og Privacy by default. Vi har for en udvalgt stikprøve inspiceret dokumentation for en udviklingsopgave. Vi har observeret, at der under opstart af opgaverne er foretaget risikovurdering i overensstemmelse med kravene om Privacy by design og Privacy by default. Vi har inspiceret system for oprettelse af udviklingsopgaver. Vi har observeret at risikovurdering er obligatorisk.	Ingen afvigelser konstateret.
Informationssikkerhed i udvikling og ændringer i applikationen ▶ Der foretages en individuel risikovurdering af udviklingsopgaver for fastlæggelse af krav til test og roll-back planlægning. ▶ Roll back-plan er implementeret i tilfælde af fejl i produktionsmiljøet. ▶ Databehandleren minimerer angrebsfladere ved at forholde sig til funktionaliteten og åbne services anvendelighed i udvikling- og ændringsopgaver. ▶ Kun databehandlerens udviklere har adgang til kildekode.	Vi har observeret at der er udarbejdet roll-out og roll-back plan for implementering i driftssystemer. Vi har observeret, at der i forbindelse med opstart af opgaver bliver foretaget en vurdering af risiko ved eksponering af services. Vi har inspiceret dokumentation for rettighedsstyring på kildekodeserver. Vi har observeret, at udviklingsmedarbejdere er tildelt adgang til kildekode ved hjælp af unikke certifikater.	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
Adskillelse af udviklings-, test og produktionsmiljø ▶ Der er indført funktionsadskillelse mellem udvikling og drift. ▶ Ændringer af funktionalitet testes, inden det sættes i drift. ▶ Udvikling og test udføres i udviklingsmiljø, som er adskilte fra produktionssystemer. ▶ Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedurer for udvikling og systemkonfiguration for adgang til servere. Vi har for en udvalgt stikprøve inspiceret dokumentation for test af kildekode. Vi har observeret, at der er foretaget test af kildekode før frigivelse til deployment. Vi har inspiceret system for opbevaring af kildekode. Vi har observeret, at kildekode er versioneret på udviklingsserver. Vi har inspiceret systemkonfiguration for virtualisering. Vi har observeret at servere i produktion er adskilt fra udviklingsmiljøer.	Vi har konstateret, at der ikke er implementeret funktionsadskillelse mellem produktions- og udviklingsmiljø, idet databehandlerens to medarbejdere med ansvar for udvikling har adgang til begge miljøer. Ingen yderligere afvigelser konstateret.
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes konstruerede testdata i udviklings- og testmiljø. ▶ Nemtilmeld.dk´s ledelse skal godkende anvendelse af produktionsdata i testmiljø. Godkendelse skal foreligge før der sker overførsel af data til testmiljø. Omfang, tidsrum og tidspunkt for sletning skal fremgå af godkendelse. ▶ Persondata i testmiljøer er beskyttet på samme niveau som persondata i produktionsmiljø. ▶ Persondata i testmiljøer slettes straks, når der ikke er et begrundet behov anvendelse af disse data.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret database i udviklings- og testmiljø. Vi har for en udvalgt stikprøve inspiceret data i tabellen for reservationer. Vi har observeret, at databasen indeholder konstruerede testdata. Vi har inspiceret systemkonfiguration for netværksbeskyttelse af produktionsmiljø og test- og udviklingsmiljø.	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
	Vi har inspiceret procedure og politikker for anvendelse og sletning af personoplysninger i testmiljøer. Vi har observeret, at der ikke har været en hændelse til brug for test af kontrollen anvendelse af produktionsdata i testmiljø, hvorfor vi ikke kan udtale os herom. Vi har ved forespørgsler hos relevant personale, fået bekræftet forståelse for medarbejdernes forståelse af kontrollen.	

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 i databehandleraftalen. ▶ Der gennemføres mindst én gang årligt egenkontrol af sletning.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret databehandleraftale og procedurer for sletning. Vi har inspiceret selvbetjeningssystem. Vi har observeret, at den dataansvarlige i selvbetjeningssystemet har adgang til at slette registrerede personoplysninger. Vi har inspiceret databehandleraftale og forretningsbetingelser. Vi har observeret at der foreligger instruks fra dataansvarlige til fortsat opbevaring af persondata indtil den, af dataansvarlige konfigurerede sletning, er udført. Vi har for en udvalgt stikprøve inspiceret standardindstillinger for sletning af personoplysninger. Vi har inspiceret procedure for egenkontrol af sletning. Vi har observeret, at der er gennemført egenkontrol af sletning den 27. maj 2020.	Ingen afvigelser konstateret.
Tilbagelevering af personoplysninger ▶ Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks ved ophør af hovedaftalen.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedurer for tilbagelevering af personoplysninger. Vi har observeret, at der er udformet vejledninger til dataansvarlige for eksport af data for tidligere arrangementer. Vi har observeret, at registrerede personoplysninger kan eksporteres i struktureret dataformat.	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 ▶ Databehandleren 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 NemTilmeld.dk.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedurer for bistand til dataansvarlige. Vi har observeret, at der er udformet vejledning til den dataansvarlige om, hvordan de kan anvende systemet til at opfylde kravene om registreredes rettigheder. Vi har observeret, at der er udformet retningslinjer for medarbejderes modtagelse af henvendelse fra den registrerede. Vi har inspiceret system for udlæsning af registrerede personoplysninger. Vi har observeret, at alle registrerede oplysninger er tilgængelige.	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.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedurer for bistand til dataansvarlige. Vi har observeret at der er udformet guide til den dataansvarlige i hvordan denne kan anvende systemet til at overholde de registreredes rettigheder. Vi har observeret at der er udformet retningslinjer for medarbejderes modtagelse af henvendelse fra den registrerede.	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
Revision og inspektion ▶ Databehandleren er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandleren bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret databehandleraftaler. Vi har observeret, at databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger Vi har inspicereret procedurer for revision og tilsyn. Vi har observeret, at der er udarbejdet procedure for imødekommelse af dataansvarliges og tilsynsmyndigheders forespørgsler i forbindelse med revision og inspektion. Vi har inspiceret databehandleraftalen. Vi har observeret, at der i databehandleraftalen er aftalt adgang til revision og inspektion.	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 kategorier af behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret databehandlerens fortegnelse over kategorier af databehandlingsaktiviteter. Vi har observeret at dette er en generel fortegnelse for systemet NemTilmeld.dk. Vi har inspiceret fortegnelse over dataansvarlige. Vi har observeret, at fortegnelse opbevares i administrationssystemet og kan udtrækkes og eksporteres ved behov.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev. ▶ En gang månedligt sikkerhedskopieres fortegnelsen og placeres i et sikret arkiv.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret system for opbevaring af dokumentation. Vi har observeret, at fortegnelser opbevares elektronisk. Vi har inspiceret arkiv for sikkerhedskopi af fortegnelse.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har foretaget interview af passende personale. Vi har fået oplyst, at databehandleren på forespørgsel udleverer fortegnelse til tilsynsmyndighederne.	Ingen afvigelser konstateret.

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

Kontrolmål

- *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.*
- *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for håndtering af brud på informationssikkerheden, herunder brud på persondatasikkerheden. Vi har observeret, at der er udformet procedurer for underretning af den dataansvarlige ved identificerede brud på persondatasikkerheden. Vi har observeret, at der er udformet standardskabeloner til brug for underretning af den dataansvarlige. Vi har inspiceret log for registrering af brud på persondatasikkerhed. Vi har observeret, at der er foretaget registrering af konstaterede brud på persondatasikkerheden. Vi har observeret, at relevante oplysninger er videregivet til den dataansvarlige uden unødig forsinkelse. Vi har observeret, at kommunikation med dataansvarlige arkiveres.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for håndtering af brud på informationssikkerheden. Vi har observeret at der er udformet procedurer for identifikation af brud på persondatasikkerheden. Vi har ligeledes observeret, at der er udarbejdet retningslinjer og træning af medarbejdere i identifikation af personoplysninger og brud på persondatasikkerheden.	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
Registrering af brud på persondatasikkerheden ▶ Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen. ▶ Databehandleren har udarbejdet og implementeret en procedure for erfaringsopsamling ved brud på persondatasikkerheden.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret log for registrering af brud på persondatasikkerhed. Vi har observeret, at der er foretaget registrering af konstaterede brud på persondatasikkerhed. Vi har inspiceret dokumentation for registrerede brud på persondatasikkerheden. Vi har observeret, at der er foretaget erfaringsopsamling og opfølgende uddannelse af medarbejdere.	Ingen afvigelser konstateret.

SUPPLERENDE INFORMATION FRA NEMTILMELD.DK APS

På baggrund af BDO's konstaterede afvigelser i ISAE 3000-erklæringen har NemTilmeld.dk ApS følgende supplerende information:

Adskillelse af udviklings-, test og produktionsmiljø

Hos NemTilmeld.dk ApS er der ikke implementeret funktionsadskillelse mellem produktion og udvikling. Det er en ledelsesbeslutning, baseret på en vurdering af fordele og ulemper ved at funktionsadskille produktion og udvikling i en lille virksomhed med to medarbejdere i udviklingsteamet.

Funktionsadskillelsen ville medføre, at udrulning af ændringer i selvbetjeningssystemet ikke vil kunne foretages, hvis en medarbejder i udviklingsteamet er fraværende.

NemTilmeld.dk ApS ønsker at prioritere muligheden for hurtige og fleksible ændringer i selvbetjeningssystemet, så fx udrulning af mindre rettelser eller nye vigtige tiltag ikke er afhængig af sygdom, koordinering af ferie mv.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 80

BDO Statsautoriseret revisionsaktieselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO netværk bestående af uafhængige medlemsfirmaer. BDO er varemærke for både BDO netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.300 medarbejdere, mens det verdensomspændende BDO netværk har ca. 90.000 medarbejdere i mere end 165 lande.

Copyright - BDO Statsautoriseret revisionsaktieselskab, cvr.nr. 20 22 26 70.