NEMTILMELD.DK APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN 1. DECEMBER 2021 TIL 30. NOVEMBER 2022 OM BESKRIVELSEN AF NEMTILMELD.DK OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN 1. DECEMBER 2021 TIL 30. NOVEMBER 2022 OM BESKRIVELSEN AF NEMTILMELD.DK OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, 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) for hele perioden 1. december 2021 til 30. november 2022 udarbejdede beskrivelse i sektion 3 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 og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Databehandlerens ansvar

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

Oplysninger i sektion 5 - Supplerende informationer fra NemTilmeld.dk ApS, er ikke en del af Databehandlerens beskrivelse af Nemtilmeld.dk. Information i sektion 5 har derfor ikke været genstand for de procedurer, der udføres af BDO ved gennemgangen af beskrivelsen i sektion 3.

Revisors uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen og den operationelle effektivitet 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 og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. 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 eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

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. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

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

a. at beskrivelsen af NemTilmeld.dk og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret i hele perioden 1. december 2021 til 30. november 2022, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. december 2021 til 30. november 2022, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. december 2021 til 30. november 2022.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandleren 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 15. december 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. 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 i sektion 3 giver en retvisende beskrivelse af NemTilmeld.dk og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden 1. december 2021 til 30. november 2022. 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. Indeholder relevante oplysninger om ændringer i NemTilmeld.dk og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden 1. december 2021 til 30. november 2022

3. 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 og fungerede effektivt i hele perioden 1. december 2021 til 30. november 2022. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden 1. december 2021 til 30. november 2022.

NemTilmeld.dk ApS bekræfter, at der er implementeret og opretholdt 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 15. december 2022

NemTilmeld.dk ApS

Thomas Kjærgaard
Direktør

3. NEMTILMELD.DK APS' BESKRIVELSE AF NEMTILMELD.DK

NEMTILMELD.DK APS

NemTilmeld.dk ApS leverer et internetbaseret selvbetjeningssystem, NemTilmeld.dk, som er hostet i eget servermiljø, placeret 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. Disse tilbagemeldingsbetingelser bliver automatisk genereret ud fra hvordan brugerne har indstillet arrangementet i administrationsområdet på arrangørens konto.

ÆNDRING I PROCEDURER OG KONTROLMILJØET

I perioden 1. december 2021 til 30. november 2022 er der ikke sket væsentlige ændringer i etablerede procedurer eller i kontrolmiljøer hos NemTilmeld.dk ApS.

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 selvbetjeningssystemet 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'ere opbevares i individuelle aflåste rum i et aflåst værdiskab, når medarbejderne ikke er til stede på arbejdspladsen. Undtaget herfra er arbejds-pc'ere, der benyttes af særligt autoriserede medarbejdere

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'ere opsat automatisk skærmlås, der låser computeren efter 10 minutters inaktivitet.

Fjernarbejdspladser og fjernadgang til systemer og data

Kun NemTilmeld.dk ApS' pc'ere 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'ere 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 selvbetjeningssystemet. 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 reetablering 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'ere.

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's 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 en brugers adgang og handlinger i administrationsmodulet anonymiseres efter 3 år. Derudover slettes søge-historik i administrationsmodulet efter 6 måneder.

Logoplysningerne er beskyttede således det alene 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.

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 person.

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.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

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

BDO har udført handlinger for at opnå bevis for oplysningerne i NemTilmeld.dk APS' beskrivelse af NemTilmeld.dk samt for udformningen og den operationelle effektivitet 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 eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller 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 og har fungeret effektivt i hele perioden 1. december 2021 til 30. november 2022.

Udførte testhandlinger

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

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.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

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 og implementeret eller ikke har fungeret effektivt i perioden.

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 som dækker informationssikkerhed og databeskyttelse, baseret på risikovurdering. ▶ Informationssikkerhedspolitikken er kommunikeret til medarbejdere.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret IT-sikkerhedspolitikken for NemTilmeld. Vi har inspiceret NemTilmelds risikovurderinger og vurderet metoden passende. Vi har endvidere konstateret, at IT-sikkerhedspolitikken er af passende omfang. Vi har modtaget og inspiceret dokumentation for, at der er afholdt en awareness-workshop vedrørende IT-sikkerhed og GDPR i erklæringsperioden. Vi har endvidere observeret, at NemTilmeld løbende informerer deres ansatte om opdateringer i IT-sikkerhedspolitikken.	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 databehandlerens årshjul. Vi har konstateret, at gennemgang og revurdering er planlagt til en årlig gennemførelse. Vi har modtaget dokumentation og inspiceret, at NemTilmeld senest har gennemgået politikken juni 2022.	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 er fastlagt i politikkerne. Vi har ligeledes observeret, at informationssikkerhedspolitikken er for-	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**
	ankret i databehandlerens ledelse og at der er navngivne personer anført til de enkelte roller. Vi har desuden interviewet ledelsen og nøglemedarbejdere om ledelsesstyringen af informationssikkerhed og databeskyttelse, og fundet deres kompetencer tilstrækkelige og betryggende.	
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 IT-sikkerhedspolitikken og konstateret, at der er generelle krav for rekruttering af medarbejdere. Vi har desuden modtaget og inspiceret NemTilmelds procedure for rekruttering, herunder at kandidaten kan varetage sit hverv i NemTilmeld. Vi har endvidere observeret, at der er udarbejdet en tjekliste til rekrutteringsforløbet som skal udfyldes. NemTilmeld har informeret os om, at de ikke har ansat nye medarbejdere i 2022. En enkelt medarbejder er overgået til en ny funktion i virksomheden. Vi har modtaget og inspiceret dokumentation for en opdateret tjekliste ved ansættelse af medarbejderen som har haft funktionsskifte. NemTilmeld udfører økonomisk baggrundstjek ved ansættelse til betroede stillinger. Kontrollen har ikke været udført i 2022, hvorfor vi ikke har kunne teste den.	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	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedure og politikker for fratrædelse. Vi har observeret, at der er udformet og implementeret procedure for fratrædelse og off-boarding af medarbejdere som bl.a. indehol-	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**
underskrevne tavshedserklæring fortsat er gældende.	dende krav om orientering af tavshedspligt efter ophør af ansættelsen i kontrolskema. Vi er blevet informeret om, at én medarbejder er fratrådt i erklæringsperioden. Vi har modtaget og inspiceret dokumentation af, at kontrolskemaet for ophør af ansættelse er udfyldt rettidigt, og at den fratrådte medarbejder er informeret om sin fortsatte tavshedspligt.	
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Databehandleren afholder awareness-træning af nye medarbejdere i forhold til databeskyttelse og informationssikkerhed ved 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, som bl.a. er fastsat i rekrutteringsprocessen og tjeklisten ved ansættelse. Vi har inspiceret dokumentation for gennemført uddannelse af medarbejdere i databeskyttelse og informationssikkerhed. Medarbejder har ved funktionsskifte modtaget ny undervisning vedrørende databeskyttelse i relation til nye arbejdsopgaver. Vi har ved forespørgsler hos en relevant medarbejder, 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 gennemført awareness træning. Vi har observeret, at der er gennemført awareness træning af medarbejdere i form af spørgeskemaer, dilemmalege og	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**
	opfølgende undervisning. Vi har desuden inspiceret dokumentation af, at der er foretaget workshops vedrørende IT-sikkerhedstrusler, hvordan disse relaterer til NemTilmeld, og hvordan NemTilmeld kan håndtere disse. Vi har desuden observeret, at NemTilmeld løbende udsender relevante informationer om opdateringer af informationssikkerhedspolitikken til medarbejdere.	

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 den generelle procedure for indgåelse af databehandleraftaler. Vi har inspiceret databehandlerens skabelon for databehandleraftaler med dataansvarlige. Vi har inspiceret proces for kundeoprettelse og observeret, at den dataansvarlige, ved oprettelse af aftale, bliver bedt om at acceptere standard databehandleraftalen, forretningsbetingelser samt information om eventuel brug af underdatabehandlere. Vi har inspiceret oversigt over kunder og konstateret, at alle har underskrevet databehandleraftale. Vi har stikprøvevis påset at kunder har underskrevet databehandleraftaler i erklæringsperioden. Vi har inspiceret at databehandleraftalerne opbevares elektronisk, og er tilgængelig for begge parter.	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 inspiceret skabelon for databehandleraftaler og konstateret at denne indeholder instruks for behandling af personoplysninger i relation til NemTilmeld. Vi har inspiceret oversigt over kunder og konstateret, at alle har underskrevet/accepteret databehandleraftale.	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 de dataansvarlige og de registrerede. Vi har inspiceret årshjul for tilbagevendende kontroller. Vi har observeret, at procedurer for behandling af persondata som minimum opdateres årligt. Vi har inspiceret databehandlerens årshjul for kontroller og observeret, at revurdering af procedurer og retningslinjer for behandling af persondata er sket løbende i erklæringsperioden.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen. ▶ Databehandleren underretter uden unødigt ophold	Vi har foretaget interview med passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer samt instruktioner for	Ingen afvigelser konstateret.

den dataansvarlige i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	medarbejdere. Vi har observeret, at der er udarbejdet instrukser for underretning af dataansvarlige ved instruks der strider mod persondatalovgivningen. Vi har endvidere observeret, at der findes en tjekliste over nødvendige punkter ved indgåelse af en databehandleraftale som afviger fra NemTilmelds skabelon. Vi har inspiceret procedure for underretning af dataansvarlige i tilfælde af at Databehandleren opdager brud på lovgivning. Vi har inspiceret log over hændelser og observeret, at der føres log over hændelser, hvor brugeren har anvendt systemet uhensigtsmæssigt i forhold til instruks, samtykketekst eller lignende. Vi har observeret, at der uden unødigt ophold er taget kontakt til dataansvarlige ved identifikation af hændelser.	

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 med passende personale og inspiceret dokumentation. Vi har inspiceret dokumentation på, at nyansatte i ansættelseskontrakten skal underskrive et afsnit omkring tavshedspligt. Vi er blevet informeret om, at NemTilmeld ikke har indgået nye ansættelseskontrakter i erklæringsperioden. Vi har i stedet modtaget og inspiceret virksomhedens skabelon for ansættelseskontrakter og observeret, at medarbejdere bliver informeret om tavshedspligt i forbindelse med deres ansættelse. Vi er blevet informeret om, at NemTilmeld ikke har anvendt eksterne leverandører eller konsulenter i erklæringsperioden. Vi har desuden inspiceret proceduren for at anvendelse af eksterne konsulenter og observeret, at tavshedspligt er påkrævet ved arbejde hos NemTilmeld.	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 konsekvenser for de registrerede. Vi har inspiceret, at risikovurdering er foretaget ud fra identificerede trusler, hvorefter der foretages en vurdering af risici baseret på deres sandsynlighed og konsekvens samt implementerede risikominimerings foranstaltninger ud fra den registreredes rettigheder. Vi har inspiceret databehandlerens årshjul for kontroller og observeret, at revurdering af risikovurdering er gennemført 1 gang årligt. Vi har observeret, at risikovurderingerne er ajourført i overensstemmelse med proceduren.	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. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanen er tidssvarende og effektive i kritiske situationer.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for beredskabsplaner. Vi har inspiceret databehandlerens årshjul for kontroller og observeret, at der er planlagt årlig test af beredskabsplan.	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.*		
▶ Beredskabstest dokumenteres og evalueres.	Vi har inspiceret dokumentation for udført test af beredskabsplaner, som er gennemført i erklæringsperioden.	
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 observeret, at der er udformet politikker og instruktion i at der ikke må udskrives personoplysninger eller ske manuel behandling på vegne af dataansvarlige. Vi har på forespørgsel fået bekræftet at support og udviklere ikke udskriver personoplysninger. Vi har inspiceret procedure for brugeradministration. Vi har ligeledes inspiceret oversigt over medarbejdere og de tildelte rettigheder og observeret, at adgang til persondata er tildelt medarbejdere ud fra arbejdsbetinget behov baseret på roller. Vi har inspiceret systemkonfiguration på server hvor der opbevares personoplysninger. Vi har observeret, at harddiske på disse er krypteret. Vi har foretaget fysisk inspektion i databehandlerens lokaler. Vi har observeret, at der ikke forefindes fysiske materialer med persondata, der er opsat tyverialarm og der kræves adgangs brik for at komme ind.	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.*

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 er elektronisk adgangskontrol for adgang til bygning og kontorlokaler. Vi har observeret, at der skal anvendes elektronisk nøglebrik ved adgang til lokaler. Vi har inspiceret serverrum. Vi har observeret, at der anvendes adgangsbrik og kode ved adgang. Derudover er der alarm på serverrum, som deaktiveres med en kode inde i rummet. Vi har observeret, at udstyr tilhørende NemTilmeld er installeret i aflåste bure. Vi har observeret at servere at monteret i aflåst rackskab inde i buret. Vi har inspiceret system for logning af adgange til serverrum. Vi har observeret, at adgang til serverummet logges. Vi har inspiceret udleveringsoversigt over nøgler til kontorlokaler. Vi har observeret, at alle nøgler er registreret med beskrivelse af medarbejder der er udleveret nøgle til. Listen over nøgler er senest gennemgået i erklæringsperioden. Vi har inspiceret selskabets årshjul for kontroller. Vi har observeret, at der er planlagt årlig gennemgang af fysisk sikkerhed, herunder foretages en gennemgang af medarbejdere med fysisk adgang til kontorlokaler og serverum. Vi har observeret, at arbejdsstationer der ikke er i brug, opbevares i aflåst værdiskab.	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.*		
	Vi har i forbindelse med vores besøg påset, at gæster ledsages ved færdsel i databehandlerens lokaler og i den øvrige bygning.	
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 krav i informationssikkerhedspolitikken. Vi har ved fysisk besøg påset at servere er beskyttet mod varme ved køleanlæg. Vi har inspiceret strømforsyning, vi har observeret, at der er redundant strømtilførsel til rackskabe og der er etableret UPS. Vi har ligeledes observeret, at der er installeret røgalarmer. Vi har ved fysisk besøg påset at der er sikring af serverrum og skabe med nøgle og elektronisk adgangssystem. og der er alarm ved indgang i serverrum. Vi har ved fysisk besøg påset netværksudstyr og kabling. Vi har observeret, at kabling og netværksudstyr i serverrum er afskærmet og beskyttet af lås.	Ingen afvigelser konstateret.
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration, der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle	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.*

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. ▶ Arbejdsstationer låser automatisk efter 10 minutter.	Vi har inspiceret politikker og procedurer for adgangsstyring, herunder at ansvar herfor er defineret i informationssikkerhedspolitikken. Vi har inspiceret dokumentation for tildeling af brugerrettigheder. Vi har observeret, at der tildeles adgang ud fra et arbejdsbetinget behov. Vi har inspiceret dokumentation for tildelte privilegerede adgange til servere og systemer. Vi har observeret, at der er foretaget gennemgang af tildelte rettigheder til alle brugere i erklæringsperioden. Vi har inspiceret system for adgangslogning. Vi har observeret, at forsøg på login registreres i adgangslog og det er på forespørgsel oplyst, at denne er tilstrækkelige til at fremfinde adgang om nødvendigt. Vi har observeret login til NemTilmeld backend system for brugere med globale roller. Vi har observeret, at der her anvendes 2-faktor autentifikation for at få adgang til systemet. Vi har inspiceret informationssikkerhedspolitik og observeret, at der er defineret krav til udformning af adgangskoder. Vi har inspiceret systemkonfiguration og observeret, at de fastsatte krav til adgangskode er efterlevet. Derudover har vi observeret, at NemTilmeld anvender passwordmanager løsning – der er krypteret - til opbevaring af adgangskoder. Vi har modtaget og inspiceret dokumentation for NemTilmelds skærmlås politik. Vi har konstateret, at skærmen låses efter 10 minutter.	

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.*

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. - Fjernadgang skal foregå via certifikat og adgangskode.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret informationssikkerhedspolitikken. Vi har observeret, at der er udformet politikker for anvendelse og tildeling af fjernadgang til persondata. Vi har inspiceret systemkonfiguration på VPN opsætning til produktionsnetværket og observeret, at adgang sker ved anvendelse af gyldige certifikat og adgangskode. Vi har inspiceret, at VPN forbindelsen er krypteret.	Ingen afvigelser konstateret.
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, for at få adgang til servere, skal etableret en VPN forbindelse til kontor-netværket, hvorefter der kan etableres forbindelse til servere. Vi har inspiceret firewall konfiguration og netværks oversigt. Vi har observeret, at der er konfigureret filtrering af netværkstrafik til servere. Vi har inspiceret konfiguration for e-mail server. Vi har observeret, at der er konfigureret anvendelse af TLS-kryptering ved afsendelse af e-mail. Vi har endvidere 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.*		
	for egenkontrol af kryptering. Vi har observeret, at der er udført kontrol i erklæringsperioden. Vi har inspiceret topologitegning og via forespørgsel indhentet bekræftelse på at der ikke er etableret eksterne kommunikationsforbindelser til/fra interne servere ud over de anførte i tegningen.	
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 og 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 passende konfigureret.	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.*		
	Vi har inspiceret procedure for periodisk review af firewall konfiguration. Vi har observeret, at NemTilmeld har udført kontrol af firewall regler i erklæringsperioden.	
Netværkssikkerhed ▶ Netværkstopologien er struktureret efter best-practice principper, hvilket betyder at servere, som driver applikationer, ikke kan nås direkte fra internettet. ▶ Databehandlerens selvbetjeningssystem 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 netværks topologi. Vi har observeret, at netværket er segmenteret og 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, og 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 og observeret, at der for kritiske applikationer er konfigureret firewall der begrænser adgang til netværk og internet services. NemTilmed risikovurderer løbende på de tekniske sikringsforanstaltninger mod malware.	Ingen afvigelser konstateret.
Sårbarhedsscanning og penetrationstests ▶ Mindst en gang årligt foretages der en sårbarhedsscanning af databehandlerens selvbetjeningsløsning.	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.*		
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 inspiceret dokumentation for sårbarhedsscanning. Vi har observeret, at der foretages løbende sårbarhedsscanning, udbedring og gentest af fundne sårbarheder. Vi har påset, at der oprettes opgaver som følge af resultaterne fra sårbarhedsscanninger. Vi har inspiceret dokumentation for, at NemTilmeld har håndteret fundene sårbarheder, og dokumenteret håndteringen i virksomhedens projektstyringssystem.	
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 og observeret, at der foretages daglig sikkerhedskopiering for alle servere. Vi har inspiceret procedurer og dokumentation for systemgendannelse og observeret, at der er udformet beskrivelser til brug for reetablering. Vi har inspiceret system for overvågning og observeret, at der sendes alarm ved fejlet backup. Vi har inspiceret årshjul for kontroller og observeret, at der er planlagt test af sikkerhedskopiering 4 gange årligt. Vi har observeret, at der er fortaget genetableringstest i erklæringsperioden.	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.*		
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 informationssikkerhedspolitikken og observeret, at der er anført krav til opdatering af arbejdsstationer. Vi har inspiceret system for kontrol af opdatering for servere og observeret at servere manuelt bliver opdateret, når der er opdateringer tilgængelige. Vi har inspiceret generel vedligeholdelse plan for systemet samt den tilhørende log. Vi har desuden observeret, at NemTilmeld foretager log over månedlige opdateringer. Vi har inspiceret dokumentation for pålagte systempatch.	Ingen afvigelser konstateret
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. ▶ Logning for persondataadgang til administrationsmodulet anonymiseres efter 3 år. ▶ Personoplysninger i søge-historik slettes efter 6 måneder.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret dokumentation for opsætning af adgangslogning og observeret, at der er implementeret logning for adgangsforsøg til systemer. Vi har inspiceret applikationslog og observeret, at alle brugerhandlinger i applikationen logges 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.*		
	Vi har inspiceret database logning og observeret, at alle handlinger på database niveau logges. Vi har inspiceret sletterutiner for logningsmateriale i applikationslog for administrationsmodulet og observeret, at persondataadgange anonymiseres efter 3 år. Vi har observeret, at der foretages sletning af log for søgekriterier der er ældre end 6 måneder. Vi har ligeledes observeret, at sletning foretages dagligt.	
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 kapacitets overvågning og observeret at servere overvåges for kapacitets udnyttelse. Vi har endvidere observeret, at NemTilmeld foretager test af oppetid jævnfør virksomhedens årshjul. Vi har ligeledes inspiceret system for serviceovervågning og observeret, at der er konfigureret overvågning af kritiske services og applikationer. Vi har observeret, at der er tilknyttet alarmering til systemovervågningen. Vi har inspiceret hændelsesloggen og observeret, at væsentlige hændelser er dokumenteret i hændelseslog.	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.*		
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 og observeret, at der er udformet politikker for bortskaffelse og kassation af IT-udstyr. Vi har inspiceret procedure for reparation og destruktion af udstyr. Vi har inspiceret loggen for reparation og bortskaffelse og observeret, at der har været en reparation i erklæringsperioden. Reparationen er foregået under opsyn og hændelsen er korrekte blevet indført i log over bortskaffelse, samt at personoplysninger er korrekt slettet.	Ingen afvigelser konstateret.

Artikel 25: Databeskyttelse gennem design og standardindstillinger

Kontrolmål

- *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Udvikling og vedligeholdelse af back-end 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 i processen skal evaluere udviklingsopgaver og sikre persondata gennem udnyttelse af privacy by design og privacy by default. Vi har stikprøvevis inspiceret dokumentation for udviklingsopgaver og observeret, at der under opstart af opgaverne er foretaget risikovurdering af privacy by design og privacy by default. Vi har inspiceret system for håndtering af udviklingsopgaver og observeret, at risikovurdering ikke kan fravælges (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 foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedurer og politikker for udvikling og vedligeholdelse og observeret, at der er udarbejdet roll-out og roll-back plan for implementering i driftssystemer. Vi har observeret, at der er udformet procedurer for informationssikkerhed i udviklingen. Vi er blevet informeret om, at der i erklæringsperioden ikke har været aktuelle roll-out eller roll-back planer. Vi er blevet informeret om, at der i erklæringsperioden ikke har været opgaver som har krævet roll-back planer. Vi har derfor ikke kunne teste kontrollen. Vi har i stedet konstateret, at NemTilmeld i forgangne erklæringsperiode har udarbejdet roll-back-planer.	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 observeret, at der i forbindelse med opstart af opgaver, bliver foretaget en vurdering af risiko ved eksponering af services. Vi har inspiceret dokumentation af NemTilmelds gennemgang af komponenter, for at reducere angrebsfalder, dertil hvordan komponenterne skal håndteres. Vi har inspiceret dokumentation for rettighedsstyring på kildekodeserver og observeret, at udviklingsmedarbejdere som de eneste er tildelt adgang til kildekode vha. unikke certifikater.	
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 stikprøvevis for udvalgte udviklingsopgaver i erklæringsperioden inspiceret dokumentation for gennemført test af kildekode og observeret, at der er foretaget test af kildekode før frigivelse til deployment. Vi har inspiceret systemkonfiguration for virtualisering og observeret, at servere i produktion er segmenteret fra udviklingsmiljøer. Vi har inspiceret tildelte rettigheder i udviklings- og produktionsmiljøet og observeret, at udviklere har adgang til begge miljøer. Vi har inspiceret system for opbevaring af kildekode, og observeret, at kildekode er versioneret på udviklingsserver.	Vi konstaterer, at der ikke er implementeret fuld funktionsadskillelse mellem produktions- og udviklingsmiljø, idet databehandlerens medarbejdere med ansvar for udvikling også har adgang til produktionsmiljøet. Ingen yderligere 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
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes konstruerede testdata i udviklings- og testmiljø. ▶ Ledelse hos databehandler 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 og stikprøvevis observeret, at databasen indeholder konstruerede testdata. Vi har inspiceret systemkonfiguration for netværksbeskyttelse af produktionsmiljø og test- og udviklingsmiljø. Vi har inspiceret procedure og politikker for anvendelse og sletning af personoplysninger i testmiljøer. Vi har via forespørgsel fået oplyst, at der ikke i erklæringsperioden har været overført persondata til udvikling- og/eller testmiljøer. Vi har ved forespørgsler hos relevant personale, fået bekræftet forståelse for medarbejdernes forståelse af kontrollen.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren kan slette og tilbagelevere personoplysninger, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks 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 og observeret, at den dataansvarlige i selvbetjeningssystemet har adgang til at fastsætte kriterier (politik) for sletning af den dataansvarliges registrerede personoplysninger. Vi har stikprøvevis inspiceret databehandleraftale og forretningsbetingelser og observeret, at der foreligger instruks fra de dataansvarlige om opbevaringer af persondata indtil den, af den dataansvarlige konfigurerede slettepolitik, er gennemført. Vi har inspiceret funktionalitet i NemTilmeld.dk omkring den dataansvarliges muligheder for valg af datasletning. Vi har inspiceret, at databehandler har opsat automatisk sletning af personoplysninger baseret på de individuelle dataansvarliges konfiguration af slettepolitik. Vi har inspiceret procedure for egenkontrol af sletning, og observeret, at der er gennemført egenkontrol i erklæringsperioden.	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 og observeret, at der er udformet guides til dataansvarlige for eksport af data for tidligere arrangementer i et 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 guide til kunderne i, hvordan de 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. Vi har inspiceret system for udlæsning af registrerede persondata og 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 32-36.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret procedurer for bistand til dataansvarlige til overholdelse af artikel 32-36 og observeret, at der er udformet passende retningslinjer for at bistå den dataansvarlige med at overholde sine forpligtigelser i forbindelse med brud på persondatasikkerheden.	Ingen afvigelser konstateret
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.	Vi har foretaget interview af passende personale og inspiceret dokumentation.	Ingen afvigelser konstateret

▶ 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 inspiceret en databehandleraftale og observeret, at databehandler er forpligtet til at udarbejde ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger Vi har inspiceret procedurer for revision og tilsyn og observeret, at der er udarbejdet procedure for imødekommelse af dataansvarliges og tilsynsmyndigheders forespørgsler i forbindelse med revision og inspektion. Vi har observeret, at der i en databehandleraftale er aftalt adgang til revision og inspektion.	

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 databehandlingsaktiviteter og observeret, at der er udarbejdet en fortegnelse over kategorier af behandlingsaktiviteter. Vi har observeret, at dette er en generel fortegnelse over behandlingsaktiviteter for systemet NemTilmeld. Vi har inspiceret fortegnelse over dataansvarlige og observeret, at fortegnelsen opbevares i et administrationssystem, der kan udtrækkes og eksporteres ved behov. Det er via forespørgsel oplyst, at fortegnelsen ajourføres i tilfælde af ændringer i behandlingsaktiviteterne.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens system. ▶ En gang månedligt sikkerhedskopieres fortegnelsen og placeres i et sikret arkiv.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har observeret, at fortegnelse opbevares elektronisk i administrationssystemet og kan udtrækkes og eksporteres efter behov. Vi har påset, at NemTilmeld har en backup af deres dokumentsystem hvori er en kopi af fortegnelsen er sikkerhedskopieret.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har foretaget interview af passende personale.	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**
	Vi har fået oplyst at databehandleren på forespørgsel, udleverer fortegnelse til kontrolmyndigheder.	

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 elektronisk.	Vi har foretaget interview af passende personale og inspiceret dokumentation. Vi har inspiceret politikker og procedurer for håndtering af brud på informationssikkerhed og observeret, at der er udformet procedurer for underretning af den dataansvarlige ved identificerede brud på persondatasikkerhed. Vi har observeret, at der er udformet standard skabeloner til brug for underretning af dataansvarlige. Vi har inspiceret log for registrering af brud på persondatasikkerhed og observeret, at der er foretaget registrering af konstaterede brud på persondatasikkerhed. Vi har stikprøvevis udvalgt brud på persondatasikkerheden og observeret, at relevante oplysninger er videregivet til den dataansvarlige uden unødig forsinkelse.	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 informationssikkerhed og observeret, at der er udformet procedurer for identifikation af brud på persondatasikkerhed. Vi har ligeledes observeret, at der er udarbejdet retningslinjer og træning af medarbejdere i identifikation af persondata og brud på persondatasikkerhed.	Ingen afvigelser konstateret.

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 og observeret, at der er foretaget registrering af konstaterede brud på persondatasikkerhed. Vi har observeret, at relevante oplysninger er videregivet til den dataansvarlige. Vi har observeret, at der er foretaget erfaringsopsamling og opfølgende uddannelse af medarbejdere. Vi har observeret, at NemTilmeld halvårligt gennemgår hændelsesloggen for databrud og vurderer tendenser.	Ingen afvigelser konstateret.

5. 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 kun to medarbejdere i udviklingsteamet.

Funktionsadskillelsen ville medføre, at udrulning af ændringer i selvbetjeningssystemet vil besværliggøres væsentligt, hvis der er fravær i udviklingsteamet.

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 og ferie mv.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

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 167 lande.

PENNEO

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

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

Thomas Kjærgaard
Direktør
Serienummer: a40ba70f-918c-4314-a195-486014535627
IP: 77.68.xxx.xxx
2022-12-15 13:14:34 UTC
MitID

Mikkel Jon Larssen
Partner
Serienummer: CVR:20222670-RID:52744874
IP: 77.243.xxx.xxx
2022-12-15 13:30:51 UTC
NEM ID

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2022-12-15 13:43:02 UTC
NEM ID

Penneo dokumentnøgle: T4WZE-KNQCZ-S1GB1-0CYFC-EK1IG-T1N51