www.pwc.dk

Assemble

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. maj 2023 til 30. april 2024 i henhold til databehandleraftale med dataansvarlige

Januar 2025

pwc

Indholdsfortegnelse

1. Ledelsens udtalelse

Assemble behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftale.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Assembles udviklings- og hosting-aktiviteter, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne") er overholdt.

Denne erklæring indeholder en vurdering af informationssikkerhed og foranstaltninger for alle Assembles aktiviteter i Assemble Group ApS, der dækker Assemble GmbH, Assemble World A/S, Assemble Learning A/S, Assemble Sp. z o.o. og Assemble A/S.

Assemble anvender Microsoft og T-Systems som underdatabehandlere for anvendt hosting. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Microsoft samt T-systems varetager for Assemble.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos den dataansvarlige er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Assemble bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af Assembles udviklings- og hosting-aktiviteter, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne i hele perioden fra 1. maj 2023 til 30. april 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Assembles udviklings- og hosting-aktiviteter 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 manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning af 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

- Kontroller, som vi med henvisning til Assembles udviklings- og hosting-aktiviteters afgrænsning har forudsat ville være implementeret af den dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

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

(ii) Indeholder relevante oplysninger om ændringer i databehandlerens Assembles udviklings- og hosting-aktiviteter til behandling af personoplysninger foretaget i perioden fra 1. maj 2023 til 30. april 2024

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne udviklings- og hosting-aktiviteter til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved Assembles udviklings- og hosting-aktiviteter, som den enkelte dataansvarlige måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. maj 2023 til 30. april 2024. Kriterierne anvendt for at give denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. maj 2023 til 30. april 2024.

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesreglerne.

Hellerup, den 3. januar 2025
Assemble

Morten Svendsen
Administrerende direktør

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger for perioden fra 1. maj 2023 til 30. april 2024 i henhold til databehandleraftale med dataansvarlige

Til: Assemble og den dataansvarlige

Omfang

Vi har fået som opgave at afgive erklæring om Assembles beskrivelse i afsnit 3 af deres udviklings- og hosting-aktiviteter i henhold til databehandleraftale med den dataansvarlige i hele perioden fra 1. maj 2023 til 30. april 2024 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Assemble har udformet og effektivt udført hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4.

Assemble anvender Microsoft og T-Systems som underdatabehandlere for anvendt hosting. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Microsoft samt T-systems varetager for Assemble.

Enkelte af de kontrolmål, der er anført i Assembles beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos den dataansvarlige er hensigtsmæssigt udformet og fungerer effektivt sammen med Assembles kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Assembles ansvar

Assemble er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i 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.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gæl-

dende i Danmark, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af deres udviklings- og hosting-aktiviteter samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som databehandleren har specificeret og beskrevet i ledelsens udtalelse.

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

Assembles beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Assembles udviklings- og hosting-aktiviteter, som hver enkelt dataansvarlig måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

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

a) at beskrivelsen af Assembles udviklings- og hosting-aktiviteter, således som de var udformet og implementeret i hele perioden fra 1. maj 2023 til 30. april 2024, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. maj 2023 til 30. april 2024, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. maj 2023 til 30. april 2024.

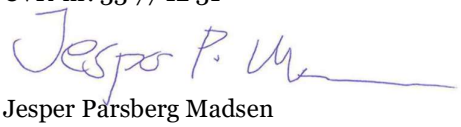
Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Assembles udviklings- og hosting-aktiviteter, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af om kravene i databeskyttelsesreglerne er overholdt.

Aarhus, den 3. januar 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31



Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

3. Beskrivelse af behandling

Introduktion

Assemble har en mission om at forbedre børns trivsel og chancer for succes i livet ved at hjælpe forældre, lærere og dagtilbud med at finde bedre måder at samarbejde med og om barnet på.

Denne beskrivelse dækker behandling af personoplysninger på vegne af kunder, der er dataansvarlige i henhold til EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "Databeskyttelsesloven") for perioden 1. maj 2023 til 30. april 2024 (beskrivelsen) samt udformning og drift af kontroller i forbindelse med de kontrolmål, der er anført i beskrivelsen.

Dette dækker områder, der også er kendt som RoPA = Verzeichnis der Verarbeitungstätigkeiten, Data Processing Agreements = Auftragsverarbeitjngsverträge og DPIA = DSFA / Datenschutzfolgenabschätzung.

Med omfattende tilpasning, kraftfulde pædagogiske funktioner samt omfattende funktioner til kapacitetsstyring, økonomistyring og personaleadministration har Assemble udviklet en state-of-the-art integreret og understøttet SaaS-løsning til dagtilbud.

Assembles løsninger er blevet implementeret i over 7.000 institutioner på 4 kontinenter og af de teknologisk førende kommuner i i Danmark, Norge, Tyskland og Schweiz.

Beskrivelse af Assembles ydelser

Assembles primære aktivitet er at udvikle og sælge det foretrukne vertikale ERP-system til dagtilbud globalt.

Assembles fokus er at give alle børn en bedre start på livet. Med platformen Nembørn sætter Assemble barnet i centrum og samler forældre, lærere og ledelse om at dele viden og arbejde sammen i et respektfuldt og engageret samarbejde omkring barnet. Resultatet er øget trivsel og bedre chance for succes i livet for det enkelte barn.

Med platformen Nemplads tilbyder Assemble næste generation software til HR-, kapacitets- og økonomistyring i dagtilbud, der letter de administrative arbejdsbyrder ved at effektivisere og digitalisere den måde dagtilbud styres på.

Denne uafhængige revisionserklæring dækker Assembles vertikale ERP-system, herunder hele Assembles produktsuite.

Assemble arbejder med et to tier setup i forhold til leverandør af hosting af applikationerne for at imødekomme kundernes krav hertil:

1. OTC T-Systems – leverandør til sikring af data kun er placeret i EU. Dette gælder også de redundante miljøer som skal sikre løsningen.

2. Microsoft Azure – leverandør hvor der er indgået aftale om at data er placeret i EU. Der er udarbejdet Transfer Impact Assessment i relation til leverandøren pga. ejerskab af selskab, som er placeret i et ikke sikkert tredjeland.

Kunder kan individuelt vælge hvilket af de to setup som ønskes anvendt. OTC T-system er bl.a. valgt da valgt da aktiviteterne er dækket af revisorerklæring 'ISAE 3000 (Revised) Report on Management's De-

scription of the Open Telekom Cloud system provided from the data centers in Germany and in the Netherlands on German Federal Office for Information Security BSI Cloud Computing Compliance Criteria Catalogue (C5)'Aktiviteterne med Microsoft Azure og OTC T-system er ikke en del af denne erklæring.

Generelt kontrolmiljø

Medarbejdere i Assembles organisation er beskæftiget primært inden for projektering, udvikling, implementering samt support.

Assembles konsulentteam har ansvaret for projekt- og implementeringsleverancen. Konsulentteamet varetager kundens interesse i driftskritiske situationer og fungerer som eskaleringsled. Assembles konsulentteam varetager endvidere supportfunktionen i forhold til slutbrugere og kunder.

Supportfunktionen sikrer forankring af processer hos slutbrugere og reagerer på opståede hændelser, som visiteres og løses eller overdrages til fejlløsning hos en specialist i udviklingsteamet. Supportfunktionen understøtter sammen med Assembles testansvarlige endvidere test og kontrol i change management-processen.

Assembles udviklingsteam er organiseret med lead developers, som har ansvar for at koordinere udviklingsopgaver inden for deres produktområde. Det er lead developers' ansvar at sikre, at funktionaliteten udvikles, vedligeholdes og testes.

For at sikre et optimalt flow har Assemble etableret centrale processer for projektering, udvikling, implementering og support. Processerne er understøttet af professionelle softwaresystemer, som understøtter incident management samt change management.

Ansvaret for sikkerhedspolitik, beredskabsplaner, driftsrutiner og beskrivelse af forretningsgang ligger hos ledelsen. Det er ledelsen, der kommunikerer eksternt med fx pressen. Ansvaret for formidling af forretningsgang og interne rutiner ligger hos ledelsen. Ved opdatering/rettelser er det ledelsens ansvar at formidle disse.

Ansvaret for løbende at sikre beskyttelsen af personoplysninger i Assemble ligger hos sikkerhedsgruppen, som består af:

- Morten Svendsen, administrerende direktør
- Jesper Broe Rasmussen, Data Compliance Officer
- Elsebeth Svendsen, CFO og ansvarlig for overholdelse af lovgivningen.

Sikkerhedsgruppens arbejde planlægges i en GDPR-årsplan, der omfatter relevante aktiviteter for at sikre, at Assemble altid er i overensstemmelse med gældende lovgivning.

Både medlemmer af ledelsesorganer og øvrige ansatte følger kurser, så de er i stand til at identificere risici og styre cybersikkerhedsrisici og disses indvirken på enhedens tjenester

Risiciene for samfundsmæssig og økonomisk indvirken på modtagerne af virksomhedens ydelser identificeres via de møder der afholdes jf. GDPR-årsplanen og mitigeres gennem foranstaltninger der beskrives og implementeres gennem Assembles processer og procedurer.

Forskellige medlemmer af sikkerhedsgruppen mødes hver måned i henhold til årsplanen og gennemgår det nuværende databeskyttelsesniveau, og herunder drøftes it-sikkerhedsinitiativer til at øge it-sikkerhedsniveauet.

Perspektivet og dagsordenen varierer fra måned til måned i forhold til de forskellige aktiviteter i årsplanen, og i løbet af kalenderåret drøftes følgende områder en eller flere gange:

- It-sikkerhedspolitik (altid opdateret)
- Gennemgang af databeskyttelsespolitikken, herunder procedurer og retningslinjer

- Gennemgang af sikkerheden
- Gennemgang af eventuelle sikkerhedsbrud
- Procedurer for adgang til personoplysninger
- Procedurer for risikovurdering
- Procedurer for sikkerhed i forbindelse med støtte
- Opfølgning på uddannelse og bevidstgørelse.

For så vidt angår indgåede databehandleraftaler:

- Opfølgning på modtagelse af (nye) databehandleraftaler og godkendelse af dem

- Opfølgning på kunder med særlige krav i deres databehandleraftaler

- Opfølgning på godkendelse af potentielle underleverandører

- Opfølgning for at kontrollere, at den dataansvarlige har godkendt alle procedurer og tekniske foranstaltninger, der sikrer behandling og beskyttelse af personoplysninger

- Opfølgning for at kontrollere, at eventuelle underdatabehandlere har indført procedurer og tekniske foranstaltninger, der sikrer behandling og beskyttelse af personoplysninger

    - Herunder opfølgning på underdatabehandleres eventuelle yderligere under-underdatabehandlere til sikring af kædeansvar

- Opfølgning for at kontrollere, at forespørgsler fra den registeransvarlige med hensyn til de registreredes rettigheder (adgang, sletning, berigtigelse) er blevet behandlet på en hensigtsmæssig og rettidig måde

- Opfølgning for at kontrollere, at forespørgsler fra den registeransvarlige med hensyn til behandlingssikkerhed (artikel 32), anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (artikel 33), meddelelse om brud på persondatasikkerheden til den registrerede (artikel 34), konsekvensanalyse vedrørende databeskyttelse (artikel 35) og forudgående høring (artikel 36) er blevet behandlet på en hensigtsmæssig og rettidig måde.

Med hensyn til eventuelle hændelser:

- Opfølgning på resultatet af den dataansvarliges høring af tilsynsmyndigheden, i det omfang dette er relevant for Assembles behandling af data for denne dataansvarlige

- Opfølgning for at kontrollere, at de personer, der er bemyndiget til at behandle personoplysninger, har tavshedspligt eller er underlagt en lovbestemt tavshedspligt.

Der er etableret procedurer og kontroller, der sikrer, at ledelsen minimum en gang årligt foretager en samlet vurdering af politikker, procedurer og kontroller i relation til efterlevelse af relevant lovgivning og regulering.

Der er etableret procedurer og interne kontroller, således at der kan foretages rapportering indenfor 24 timer til relevant myndighed om hændelser, der har væsentlig indvirken i betydningen alvorlige driftsforstyrrelser eller økonomiske tab for virksomheden eller kan forårsage betydelig materiel eller immateriel skade på fysiske eller juridiske personer.

Assemble har udpeget Jesper Broe Rasmussen som data compliance officer med ansvar for at sikre, at Assembles processer og ydelser overholder GDPR.

Assembles it-sikkerhedspolitik og databeskyttelsespolitik (kundevendt) gælder for alle Assembles medarbejdere og er en del af grundlaget for ansættelsesforholdet. Politikkerne danner rammen for behandling,

opbevaring, deling og sletning af data, og de indeholder procedurer for rettighedsstyring, passwordstyring, patching, logning, backup, adgangskontrol osv.

Politikkerne opdateres med bestemte intervaller og som minimum, når virksomheden indfører nye systemer, ydelser, forretningsprocesser osv. af betydning for sikkerheden eller databeskyttelsen.

Den enkelte medarbejder er ansvarlig for at overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkelte medarbejders opgaver.

Relevante partnere og leverandører er ansvarlige for at overholde Assembles informationssikkerhedspolitik og de regler, der er relevante for deres ansvarsområder – mest hensigtsmæssigt ved at deres egne sikkerhedspolitikker og regler altid afspejler Assembles krav. Partnere og leverandører er oprettet i underleverandøraftaler, databehandleraftaler og fortrolighedserklæringer og er sikret gennem erklæringer om sikkerhedsstillelse.

Alle dokumenter vedrørende databeskyttelse, herunder dokumentation, risikoanalyser, politikker, rapporter osv., opbevares i et dokumentarkiv. Adgangen til disse ressourcer er begrænset, så kun relevante medarbejdere har adgang til de forskellige oplysninger om håndtering og opfølgning på den dataansvarliges henvendelser/anmodninger om støtte, fx støtte til besvarelse af en anmodning fra en registreret (slutbrugeren) om dennes rettigheder, samt den dataansvarliges henvendelser om Assembles vurdering og høring af tilsynsmyndigheden. Ligeledes er det kun medlemmer af sikkerhedsgruppen, der har adgang til dokumentationen/analysen i tilfælde af et sikkerhedsbrud. Der opbevares ingen følsomme personoplysninger i dokumentarkivet. Følsomme personoplysninger opbevares kun i et system, hvor adgangen er sikret med tofaktorautentifikation.

De forskellige politikker og procesbeskrivelser er tilgængelige for alle medarbejdere på virksomhedens intranet.

Sikkerhedsgruppen er ansvarlig for at kontrollere, at de krævede kontroller udføres og har den tilsigtede virkning. Resultaterne drøftes i sikkerhedsgruppen, og der aftales eventuelle nødvendige foranstaltninger.

Risikovurdering

Assemble har formaliserede processer til vurdering af risikoen ved de ydelser, hvor personoplysninger behandles.

Risikovurderingen gennemgås med bestemte intervaller og desuden som minimum, når et system ændres, nye forretningsprocesser implementeres, et nyt system anvendes, eller når nye typer personoplysninger behandles som en del af Assembles ydelser.

Risikovurderingerne fokuserer på risikoen/sandsynligheden for et brud på persondatasikkerheden og konsekvenserne for den registrerede person af et sådant brud.

Risikovurderingerne er med til at sikre, at de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger altid er etableret for at beskytte de data, der behandles enten i løsningerne eller i organisationen. Risikovurderingen anvendes i det fortsatte arbejde med at etablere organisatoriske og tekniske sikkerhedsforanstaltninger for at imødegå de risici (risikostyring), der er anført i risikovurderingen.

Risikovurderinger foretages af den dataoverholdelsesansvarlige med input fra relevante medarbejdere i organisationens udviklingsafdeling. Risikovurderingerne godkendes af sikkerhedsgruppen.

Der er etableret procedurer og kontroller, der sikrer at risikovurderingen omfatter væsentlige leverandører og deres rolle, samt at der ved udvidelse med nye leverandører foretages vurdering af leverandørens sårbarheder, kvalitet af cybersikkerhedspraksis og udviklingsprocedurer.

De nuværende risikolandskaber

I betragtning af de data, som Assemble behandler, og de kontroller og organisatoriske og tekniske foranstaltninger, der er gennemført for at mindske risikoen og minimere sandsynligheden for brud på persondatasikkerheden, vurderes den nuværende risikoprofil for Assembles ydelser at være lav. For at sikre et konstant fokus på at minimere risiciene har Assemble etableret kontrolaktiviteter, der både har til formål at sikre og teste, at foranstaltningerne i tilstrækkelig grad begrænser disse risici.

Kontrolaktiviteter

Baseret på principperne i ITIL sikrer Assembles processer, at alle ændringer foretages på en planlagt og autoriseret måde i tæt samarbejde med kunden. En anmodning om ændring kan udløses af forskellige årsager, og en ikke-udtømmende liste af eksempler er vist nedenfor:

- Incident management (oftest som vedligeholdelsesforpligtigelser)
- Problem management (oftest som vedligeholdelsesforpligtigelser)
- Forslag til ny funktionalitet (initieret af kunde eller Assemble)
- Forslag til ændring af eksisterende funktionalitet (initieret af kunde eller Assemble).

Efter oprettelse af en request for change vil Assemble udføre et review, for at sikre at informationerne er tilstrækkelige. Denne proces understøttes af Service Management-systemet. Service Management-systemet anvendes til opgavestyring og prioritering af delopgaver samt arbejdsflow. Processen følger principperne i den agile udviklingsproces Kanban. Kanban-processen giver en klar prioritering af opgaverne samt et veldefineret arbejdsflow, som en opgave skal gennemgå inden frigivelse. Med Kanban-processen er der en klar prioritering af opgaver samt et veldefineret forløb, som en opgave skal gennemløbe, fra opgaven defineres, risikovurderes og til den er færdigudviklet, testet og godkendt til release og installation hos kunderne. Kanban og Service Management-systemet anvendes hos Assemble til både supportsager og nyudvikling.

Ansvaret for udvikling og implementering af opgaverne er placeret hos lead developer i udviklingsafdelingen, og ansvaret for test og godkendelse er placeret i testafdelingen. For at sikre effektive testprocesser skal der fra starten være en god dialog mellem testafdelingen og udviklingsafdelingen, og acceptkriterier for opgaven skal være præcise. Det er ikke tilladt, at samme medarbejdere kan udvikle og godkende en opgave i Service Management-systemet. Alle handlinger i Service Management-systemet logges med registrering af tidspunkt og aktør, således at der er fuld sporbarhed i forhold til opgavens gennemløb.

Når kodeændringer "pushes" til kildekoden, angives det opgavenummer, som den tilhørende opgave i Service Management-systemet var tildelt. Dermed sikres sporing af kodeændringer og sammenhængen med opgavestyringssystemet.

Versionering og releaseproces

Testorganisationen er ansvarlig for at godkende alle rettelser og nyudvikling forud for frigivelse af en ny version. Opgaver, som ikke kan godkendes, afvises og sendes tilbage til udviklingsafdelingen med forklaring på afvisningen. Opgaven indgår herefter igen i den samlede prioritering og gennemløber på ny Kanban-processen.

Efter godkendt test genereres en nyt release, som i Service Management-systemet tildeles et versionsnummer. Fra Service Management-systemet er der adgang til at gennemse samtlige de opgaver, der er løst med en given version. Samtidig med release-definitionen i Service Management-systemet generes installationsfiler, der kan installeres hos kunderne.

Supportproces

Når et incident identificeres, skal den registreres i Service Management-systemet. Alle henvendelser registreres af supportorganisationen. Henvendelser kan ske i form af telefonisk henvendelse, via e-mail eller chat, eller på Assembles eget initiativ, eksempelvis via test. Alle henvendelser registreres uanset oprindelse og kategori.

Den relevante og nødvendige dokumentation skal foreligge, for at arbejdet med identifikation og løsning kan påbegyndes. Findes den registrerede sag mangelfuld, vil henvendelse ske til kunden til sikring af, at de

manglende informationer bliver indhentet og dokumenteret på sagen, så arbejdet kan igangsættes så gnidningsfrit og hurtigt som muligt. Erfaring har vist, at langt de fleste brugerhenvendelser drejer sig om brug af systemet og dermed ikke er udtryk for problemer eller incidents. Supportorganisationen står for den umiddelbare kontakt til brugere af systemet både i forbindelse med modtagelse af henvendelser, umiddelbar hjælp og support og evt. at vende tilbage med svar eller løsninger, hvis henvendelsen ikke kunne løses i første omgang.

Såfremt der er tale om en henvendelse, der kræver en rettelse fra udviklingsafdelingen, er supportmedarbejderen ansvarlig for at oprette en sag i Service Management-systemet og sikre sammenkobling mellem kundehenvendelsen og Service Management-systemet. Efter løsning i udviklingsafdelingen sendes automatisk svar tilbage til supportorganisationen, der kan godkende eller afvise løsningen. Såfremt løsningen accepteres, lukkes sagen, og der gives automatisk besked til indberetteren. Den automatiske besked oplyser indberetteren om, at der er fundet en løsning på den oplevede hændelse, og opfordrer indberetteren til at rette henvendelse, såfremt indberetteren oplever, at den oplevede hændelse ikke er løst.

Der er fuld sporbarhed og historik fra slutbrugerens henvendelse over opgaveløsning til færdiggørelse og advisering af slutbrugeren.

For hændelser i forbindelse med GDPR oprettes forespørgslen i Service Management-systemet som et problem af typen "GDPR-sag" og tildeles automatisk til den dataoverholdelsesansvarlige. Spørgsmål af typen "GDPR-sag" har yderligere automatiske påmindelser tilknyttet for at sikre et rettidigt svar til forespørgeren og har også yderligere arbejdsgangstrin for at sikre underretning af tredjepart, hvis det er nødvendigt.

Alle hændelser håndteres og vurderes - herunder i forhold til konsekvenser for modtagere af virksomhedens ydelser.

Brugere og adgange

Det er udviklingsdirektøren hos Assemble, der initielt tildeler rettigheder til medarbejdere. Oprettelsen af adgangen foretages af udviklingsdirektøren selv eller på bestilling af udviklingsdirektøren. Det samme gør sig gældende for nedlæggelse af adgange – fx ifm. opsigelser. Brugere oprettes, administreres og nedlægges i henhold til den gældende sikkerhedspolitik, hvor privilegier og adgange tildeles ud fra et arbejdsrelateret behov. Medarbejdere med administratorrettigheder har mulighed for at oprette adgange til yderligere medarbejdere, og øvrige administratorer adviseres automatisk pr. e-mail når der oprettes yderligere administratoradgange.

Der findes en global oversigt omfattende alle kundeløsninger, der dokumenterer med datoangivelse, hvilke adgange der er tildelt, og der foretages periodisk gennemgang af brugere, rettigheder og adgange.

Sikker kommunikation

Assemble er en del af det etablerede tunnelkrypteringssamarbejde i Danmark. Det sker via en hostet SEPO-løsning fra IT Relation.

Integrationen sikrer, at al e-mailkommunikation mellem Assemble og de danske myndigheder og kommuner, der deltager i tunnelkrypteringssamarbejdet, automatisk krypteres – både mellem centrale postkasser og medarbejdernes egne postkasser.

Assemble har formelle processer, der sikrer, at der tages hensyn til sikkerheden af personlige data, når nye kunder kommer ind i systemet. Således kontrolleres det inden implementering/start af et nyt projekt, at kunderne er bekendt med procedurerne og arbejdsmetoderne i Assemble, og at Assemble lever op til ansvaret for god databehandlingspraksis samt til forpligtelserne som databehandler.

Assemble har formelle procedurer, der sikrer, at data ikke lagres lokalt, og at data slettes i systemerne i god tid efter behandlingen. Desuden er Assembles medarbejdere forpligtet til at overholde og sikre, at politikken for sletning af data følges.

Assemble inspicerer alle (under)forarbejdningsvirksomheder en gang om året, og hvis samarbejdets karakter ændres. Inspektionen foretages på grundlag af relevans og risiko. Det betyder, at der tages hensyn til

arten, omfanget, forholdet og formålet med den pågældende behandling samt risikoen for den enkeltes rettigheder og frihedsrettigheder. Jo større risikoen er, desto større er kravene til sikkerheden. Kontrollen foretages ved at indhente forsikringsrapporter og indsamle skriftlige oplysninger – herunder oplysninger vedrørende yderligere under-underdatabehandlere. Afhængigt af risikoen i forbindelse med underdatabehandlerens behandlingsaktiviteter kan indsamlingen af skriftlige oplysninger suppleres med fysiske besøg.

Der indgås (under)behandlingsaftaler med alle (under)behandlere, hvori underbehandlerne har mindst de samme forpligtelser som Assemble har over for kunden.

Der foretages kontrol for at verificere, at den indgåede (under)behandlingsaftale overholdes, herunder at (under)behandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Ledelsen har foretaget vurdering af leverandører som led i etablering af politikker og kontroller set ud fra virksomhedens ydelsers samlede effekt på samfundet.

Assemble har etableret et compliance-setup bestående af kontroller, der udføres internt i organisationen med den aftalte hyppighed i overensstemmelse med procedurens formål. Disse kontroller er blevet etableret for at sikre overholdelse af ovenstående initiativer og procedurer samt andre GDPR-spørgsmål. Kontrollerne er systemstyret for at give Assemble mulighed for at sikre opfølgning og eskalering i tilfælde af manglende gennemførelse. Sikkerhedsgruppen i Assemble har det primære ansvar for drift og forvaltning af denne kontrolopsætning, selv om udførelsen af kontrollerne kan uddelegeres til de relevante personer inden for et bestemt ansvarsområde.

Information og kommunikation

Når nye medarbejdere bliver ansat hos Assemble, får de relevante oplysninger om og bliver gjort opmærksomme på håndteringen af personoplysninger og Assembles processer til beskyttelse af personoplysninger.

Assemble håndterer al kommunikation med registrerede personer gennem formelle processer, der understøttes af hotline- og opgaveforvaltningssystemer, som anvendes i Assemble.

Det er den enkelte teamleder, der har ansvaret for at kommunikere internt i Assemble. Det er ledelsen, der er ansvarlig for at kommunikere til kunder og pressen.

Rapporteringen udarbejdes af de enkelte afdelinger og godkendes af ledelsen, inden den sendes til kunden.

Der er etableret procedurer og kontroller til sikring af brug af MFA m.v., beskyttelse af kommunikation og etablering af nødkommunikation, hvor det er relevant.

Overvågning

Ledelsen er ansvarlig for at overvåge sikkerhedsbrud og den opfølgning, der foretages på dem. Det er også ledelsen, der tager initiativ til at udbedre eventuelle sikkerhedsbrud. Det er medarbejderens ansvar at indberette sikkerhedsbrud eller mistanke herom til ledelsen med det samme.

Der er etableret procedurer og kontroller, der sikrer, at beredskabsplanen og test heraf omfatter væsentlige leverandører og deres rolle.

Ledelsen foretager i øvrigt løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet. F.eks. efter et brud på persondatasikkerheden, gennem et tæt og løbende samarbejde med it-revision og i forbindelse med revisionserklæringers udvisende.

Ledelsen udbedrer uden ugrundet ophold udeståender, konstateret i forbindelse med udfærdigelse af revisionserklæringer.

Overvågningen sker i overensstemmelse med de gældende sikkerhedspolitikker samt definerede operationelle processer såsom support og ændringsstyring.

Efter en formel procedure følger sikkerhedsgruppen hvert kvartal op på status for GDPR-arbejdet, modtagelsen og godkendelsen af (nye) databehandleraftaler og følger op for at kontrollere, at forespørgsler fra den dataansvarlige med hensyn til registreredes rettigheder (adgang, sletning, berigtigelse) er blevet behandlet på en passende og rettidig måde.

Komplementære kontroller hos de dataansvarlige

Forudsætninger vedrørende kundernes ansvar er beskrevet i individuelle kontrakter. Kunden er ansvarlig for egne data. Det betyder, at kunden er ansvarlig for de ændringer, der måtte foretages i data, når der er logget på systemet med individuelle brugernavne og adgangskoder. Ved tredjepartsadgang bestilt af kunden er det kunden, som har ansvaret for opfølgning på kontrollen.

Detaljerne fremgår af kontrolmål og kontrolaktiviteter ifølge skema med oplistning og test heraf.

Som en del af leveringen af ydelser skal den dataansvarlige gennemføre visse kontroller, der er vigtige for at nå de kontrolmål, der er specificeret i beskrivelsen. Dette omfatter:

- at overveje konsekvenserne i forbindelse med beskyttelsen af personoplysninger, når der fremsættes anmodninger om ændringer
- at være ansvarlig for at sikre, at der findes et retsgrundlag for behandlingen på tidspunktet for overførslen af personoplysningerne til Assemble – herunder at ethvert samtykke er frit givet, specifikt, informeret, utvetydigt og udtrykkeligt, hvis det er påkrævet
- at garantere, at de personer, som personoplysningerne vedrører (de registrerede), er blevet tilstrækkeligt informerede om behandlingen af deres personoplysninger
- at have det primære ansvar for at give Assemble instruktioner om databehandling og håndtere anmodninger fra registrerede personer om deres rettigheder
- at rapportere eventuelle brud på persondatasikkerheden til det nationale databeskyttelsesagentur.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	Inspiceret, at ledelsen sikrer, at behandlingen af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen afvigelser noteret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet, i tilfælde hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Ingen afvigelser noteret.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på databehandleraftaler, at der er etableret de aftalte sikkerhedsforanstaltninger.	Ingen afvigelser noteret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandleren foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandleren har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Ingen afvigelser noteret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Inspiceret, at antivirussoftware er opdateret.	Ingen afvigelser noteret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor.	Ingen afvigelser noteret.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser noteret.
B.6	Adgang til personoplysninger er isoleret til brugere med et arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret ved en stikprøve på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser noteret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at der ved en stikprøve på alarmer er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Ingen afvigelser noteret.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Ingen afvigelser noteret.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: ○ Ændringer i logopsætninger, herunder deaktivering af logning ○ Ændringer i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang af og opfølgning på logge. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og sletning. Inspiceret ved en stikprøve på logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser. Inspiceret ved en stikprøve på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.	Ingen afvigelser noteret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved en stikprøve på udviklings- og testdatabaser, at personoplysningerne heri er pseudonymiseret eller anonymiseret. Inspiceret ved en stikprøve på udviklings- og testdatabaser, hvor personoplysningerne ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Ingen afvigelser noteret.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt til de dataansvarlige i behørigt omfang.	Ingen afvigelser noteret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen afvigelser noteret.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, herunder om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved en stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for en regelmæssig – mindst årlig – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser noteret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede, sker som minimum ved anvendelse af tofaktorautentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.	Ingen afvigelser noteret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Ingen afvigelser noteret.

Kontrolmål C:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser noteret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser noteret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser.	Ingen afvigelser noteret.

Kontrolmål C:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.4	Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver medarbejderne introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejdernes behandling af personoplysninger.	Inspiceret ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved to stikprøver på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information.	Ingen afvigelser noteret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelsen, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at rettighederne er inaktiveret eller ophørt, samt at aktiverne er inddraget.	Ingen afvigelser noteret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, som databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen afvigelser noteret.

Kontrolmål C:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

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

Kontrolmål D:

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
D.2	Der er aftalt krav til databehandlerens opbevaringsperioder og sletterutiner i databehandleraftaler.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysningerne er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen afvigelser noteret.
D.3	Ved ophør af behandlingen af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandlingen af den dataansvarliges data ved ophør af behandlingen af personoplysninger. Inspiceret ved en stikprøve på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen afvigelser noteret.

Kontrolmål E:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen afvigelser noteret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser noteret.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser noteret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelsen af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelsen af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændringer i anvendelsen af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser noteret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser noteret.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser noteret.
F.6	På baggrund af en ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, foretager databehandleren en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen afvigelser noteret.

Kontrolmål G:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved en stikprøve på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Ingen afvigelser noteret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Ingen afvigelser noteret.

Kontrolmål H:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.	Ingen afvigelser noteret.

Kontrolmål I:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af adgang til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafikken overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen afvigelser noteret.

Kontrolmål I:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden. Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 72 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen afvigelser noteret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Disse procedurer skal indeholde anvisninger på beskrivelser af: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede anvisninger på: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen afvigelser noteret.