Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C

Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

Emini A/S

Uafhængig revisors ISAE 3000 type 2-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling

Erklæringen omfatter perioden fra 17. februar 2020 til 31. december 2020

Indholdsfortegnelse

1. Ledelsens udtalelse

Emini behandler personoplysninger på vegne af dataansvarlige i henhold til indgåede databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt PeopleTrust-platformen, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt. Emini bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af PeopleTrust-platformen, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen for perioden 17. februar 2020 til 31. december 2020. De kriterier, der er anvendt for at give denne udtalelse, var, at den medfølgende beskrivelse:
   (i) redegør for, hvordan PeopleTrust-platformen var udformet og implementeret, herunder redegør for:
      - de typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
      - de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
      - de processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
      - de processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
      - de processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
      - de processer, der i tilfælde af brud på persondatasikkerheden, understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
      - de processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
      - kontroller, som vi med henvisning til drift og vedligeholdelse af PeopleTrust-platformens afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
      - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger
   (ii) indeholder relevante oplysninger om ændringer ved databehandlerens drift og vedligeholdelse af PeopleTrust-platformen til behandling af personoplysninger foretaget i perioden 17. februar 2020 til 31. december 2020
   (iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne drift og vedligeholdelse af PeopleTrust-platformen 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 drift og vedligeholdelse af PeopleTrust-platformen, som den enkelte dataansvarlige måtte anse for vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret i perioden 17. februar 2020 til 31. december 2020. De kriterier, der er 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
   (iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i perioden 17. februar 2020 til 31. december 2020.

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

Kongens Lyngby, den 1. marts 2021

Emini A/S

Niels Wedenborg
Adm. Direktør

2. Uafhængig revisors erklæring

Til: Emini og Eminis kunder

Omfang

Vi har fået til opgave at afgive erklæring om Eminis beskrivelse i afsnit 3 af sin Peopletrust-platform til behandling af personoplysninger på vegne af dataansvarlige omfattet af EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri 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 17. februar 2020 til 31. december 2020 (beskrivelsen) og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Emini anvender serviceunderleverandører til hosting og drift af serverne mv. Eminis systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandøren. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandøren.
Nogle af de kontrolmål, der er anført i Eminis beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Emini. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

Eminis' ansvar

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

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Deloitte er underlagt international standard om kvalitetsstyring ISQC 1 og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

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

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, *Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger*, og yderligere krav ifølge dansk revisorlovgivning med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin PeopleTrust-platform samt for kontrollernes funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. Vores handlinger har omfattet test af udformning, implementering og funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af

beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 3.

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

Begrænsninger i kontroller hos en dataansvarlig

Eminis beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og omfatter derfor ikke nødvendigvis alle de aspekter ved PeopleTrust-platformen, som hver enkelt dataansvarlig måtte anse for vigtige efter dennes særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivning 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, at:

(a) beskrivelsen af PeopleTrust-platformen, således som den var udformet og implementeret i perioden 17. februar 2020 til 31. december 2020, i alle væsentlige henseender er retvisende

(b) de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden 17. februar 2020 til 31. december 2020

(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 17. februar 2020 til 31. december 2020.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt kunder, der har anvendt Eminis platform, og som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 1. marts 2021

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

3. Systembeskrivelse af PeopleTrust

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Emini A/S' ydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af, om krav relateret til databeskyttelsesforordningen er overholdt.

3.1 Applikationsbeskrivelse

Applikationen ISAK/PeopleTrust er et system, som bruges inden for beskæftigelses-, integrations-, social-, kursus- og anden personrelateret indsats samt i vikar- og rekrutteringsbranchen. Det er et system, som håndterer personer, virksomheder, virksomhedskontaktpersoner, ordrer, fakturering, løn m.m.

Eminis kunder arbejder enten for offentlige eller private kunder. Hvis Eminis kunder arbejder for offentlige kunder, sker det oftest efter loven om beskæftigelses-, social- eller integrationsindsats. Her vil samarbejdet være reguleret af en databehandleraftale.

Systemet leveres som software-as-a-service, og ved indgåelse af kontrakt gives kunden adgang til systemet. Emini har ansvaret for systemet og det fysiske driftsmiljø, mens kunden har ansvaret for data og brugen af systemet.

Systembeskrivelsen indeholder ydelser leveret af Emini med henblik på at få afdækket væsentlige kontrolmål ud fra virksomhedens interne kontroller, som er bygget op omkring databeskyttelsesforordningen. Beskrivelsen indeholder endvidere kritiske forretningsprocesser, som Emini har identificeret til at være væsentlige for kunder, der benytter Emini som databehandler.

Emini har implementeret interne krav og kontroller for udvikling og drift samt adgang til systemet. Virksomhedens krav er kommunikeret via politikker og retningslinjer, som både medarbejdere og underleverandører er underlagt. I forhold til medarbejdere sker det i form af en sikkerhedspolitik, sikkerhedsinstruks, ansættelseskontrakt og kontinuerlige sikkerhedsmøder. I forhold til underleverandører sker det i form af kontrakter, databehandleraftaler og kontroller.

Retningslinjer og politikker opdateres og ledelsesgodkendes kontinuerligt af Eminis direktion for at indarbejde relevante og lovmæssige krav relateret til den gældende lovgivning og god praksis på området. Der udarbejdes referater af disse møder, som underskrives af Eminis direktion og ledende medarbejdere.

3.2 Underdatabehandlere

I forhold til kunden er Emini databehandler eller underdatabehandler. Eminis adgang til og kundernes brug af systemet er reguleret af hhv. kontrakt og databehandleraftaler. Databehandleraftalen tager udgangspunkt i Datatilsynets vejledning på området. Emini arbejder alene efter instruks.

Emini anvender underleverandører i forbindelse med hosting og drift af serverne. I forhold til kundens kunde er Eminis underleverandør tredjepartsdatabehandler. Underleverandørens adgang til serverne er reguleret af hhv. kontrakt og databehandleraftaler. Eminis underleverandører arbejder alene efter instruks.

3.3 Karakteren af behandling

I systemet behandles persondata og personfølsomme data. Emini fører en generel datafortegnelse over de informationer, der kan opbevares og behandles. Det er kundernes eget ansvar at føre datafortegnelse over de specifikke informationer, som kunden arbejder med i systemet. I forhold til Eminis kunders forpligtelser som dataansvarlig eller databehandler stiller Emini og systemet følgende funktioner/services til rådighed:

- Oplysningspligt. Systemet kan på en nem og overskuelig måde dokumentere alle de oplysninger, som måtte være registreret på personobjektet

- Berigtigelse. Data, som måtte være registreret på personobjektet, og som måtte være forkerte, kan korrigeres, så de bliver retvisende
- Sletning. Data, som måtte være registreret på personobjektet, kan slettes, enten ved sletning af enkeltregistreringer eller ved sletning af personobjektet
- Portabilitet. Data, som måtte være registreret på personobjektet, kan udleveres elektronisk.

3.4 Risikovurdering

Emini gennemfører kontinuerligt en uddybende risikovurdering på relevante områder i relation til system-, udviklings- og driftsmiljøer, som vurderes ud fra tekniske, organisatoriske og operationelle aspekter. Risikovurderingsprocessen gennemføres af ledelsen i samarbejde med Eminis ledende medarbejdere i forhold til identificering og opdatering af risikolandskabet. Risikolandskabet behandler risici ved opbevaring og behandling af persondata, it-beredskab og gendannelse af systemer ved nedbrud (backup/restore) samt lignende relevante risikoområder. De trusler, som behandles, vedrører cybersikkerhed, misbrug, systemnedbrud, fysiske hændelser på lokationer, uheld, tekniske fejl og uautoriseret adgang. Endvidere er kommunikation, opbevaring af data, software, fysiske lokationer og aktiver behandlet særskilt i forlængelse af trussels- og risikolandskabet for Emini, systemet samt relevante kunder og samarbejdspartnere.

Risikovurdering. I Eminis risikovurdering tages der bl.a. højde for den mulige indvirkning af skader, tab af omdømme, sociale konsekvenser og indflydelsen på den registreredes privatliv, som et datatab eller databrud vil medføre for den registrerede. Det vurderes også, med hvilken sandsynlighed Emini vil blive udsat for angreb med henblik på tyveri, tilintetgørelse eller forringelse af data.

- Påvirkning. Emini vurderer ud fra arten af de data, som Emini opbevarer og behandler, at et eventuelt datatab eller databrud vil medføre betydelige uhensigtsmæssigheder for de registrerede, som de dog kan overkomme uden stort besvær. På den baggrund vurderes indvirkningsgraden som middel.
- Risiko. Emini vurderer, at eftersom systemet tilgås fra og baseres på brug via internettet, er det eksponeret for en vis mængde trusler, der kan ramme infrastrukturen, navnlig i form af utilgængelighed.

3.5 Kontrolforanstaltninger

Emini har implementeret kontroller omkring behandling af personoplysninger inden for følgende områder:

- Databehandleraftaler og instruks (kontrolmål A)
- Tekniske sikringsforanstaltninger (kontrolmål B)
- Organisatoriske foranstaltninger (kontrolmål C)
- Sletning og tilbagelevering af personoplysninger (kontrolmål D)
- Opbevaring af personoplysninger (kontrolmål E)
- Anvendelse af underdatabehandlere (kontrolmål F)
- Bistand til den dataansvarlige (kontrolmål H)
- Håndtering af sikkerhedsbrud (kontrolmål I).

I afsnit 4 er de kontrolforanstaltninger, Emini anser for relevante for behandlingen af persondata, beskrevet. Nedenfor findes en uddybende beskrivelse af et udvalg af relevante kontrolforanstaltninger.

Eminis it-sikkerhedspolitik, retningslinjer og procedurer behandler og indeholder en beskrivelse af relevante systemer og ydelser relateret til systemet. Behandling og udvikling af Eminis sikkerhedsforanstaltninger foretages af ledelsen og relevante ledende medarbejdere. Vores miljø er bygget op omkring kontrollerne i denne systembeskrivelse, som benyttes til udarbejdelse af nærværende erklæring.

3.5.1 Generelle procedurer for behandling af personoplysninger (kontrolmål A)

Formål

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

Anvendte procedurer og kontroller

Eminis forretningsgange og politikker er knyttet til roller i virksomheden, hvorved efterlevelse af krav i gældende lovgivning indlemmes i arbejdsgangene for samtlige medarbejdere. Hver rolle i virksomheden har specifikke retningslinjer og procedurebeskrivelser til varetagelse af arbejdsopgaver for at sikre tilstrækkelig efterlevelse af krav. Roller gennemgås kontinuerligt af ledelsen for at sikre, at disse til stadighed overholder og efterlever de gældende krav, og at arbejdsopgaver tilknyttet rollerne er i overensstemmelse med gældende arbejdsopgaver og behandling af persondata.

Samtlige medarbejdere underskriver Eminis gældende retningslinjer, herunder forretningsgangen for IT og sikkerhed, ved ansættelse. Såfremt de gældende retningslinjer gennemgår væsentlige ændringer, attesterer medarbejdere deres samtykke på ny.

Grundlaget for den lovlige behandling er indarbejdet i hhv. kontrakt og databehandleraftaler. Lovhjemlen er kontraktuel. Emini behandler data alene efter instruks.

Retningslinjer for behandling af persondata er beskrevet i sikkerhedspolitikken. Særlige kategorier af persondata behandles og opbevares med samme høje grad af sikkerhed som almindelige persondata.

3.5.2 Tekniske sikringsforanstaltninger (kontrolmål B)

Formål

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

Anvendte procedurer og kontroller

I systemet er der opsat rettighedsstyring på data, så den dataansvarlige kan opsætte begrænsning på persondata. Følgende sikkerhedsforanstaltninger benyttes:

- Personligt login. Alle brugere har et selvstændigt login bestående af et brugernavn og kodeord. For almindelige brugere skal kodeordet være minimum 8 karakterer langt og bestå af store og små bogstaver samt tal. For administratorer skal kodeordet være minimum 12 karakterer langt og bestå af store og små bogstaver samt tal
- Brugerrettighedsgrupper. Alle brugere tilhører en rettighedsgruppe, der regulerer deres adgang til de registrerede og deres funktionsrettigheder, herunder adgang til at læse, redigere og slette.
- Afdelingsbegrænsning. Alle brugere tilhører en eller flere afdelinger, hvilket dermed begrænser brugerens adgang til de registrerede, så brugeren kun kan se registrerede i den eller de afdelinger, brugeren selv tilhører
- IP-spærring. Brugeren kan begrænses IP-mæssigt, så brugeren eksempelvis kun kan tilgå systemet via særskilte netværk eller fysiske adresser.

Data beskyttes bl.a. mod tilintetgørelse, tab eller ændring gennem rettighedsstyring af, hvem der må tilgå, ændre og tilintetgøre data. Der føres en ændringslog over væsentlige ændringer, som Emini kan tilgå i tvivlstilfælde, eller backup. Teknisk sikkerhed opnås også gennem sikring af kryptering af datatrafik, servere, firewalls, backupprocedurer, sikkerhedsopdateringer og serverovervågning. Endelig opnås det gennem design, hvor rettigheder og tilsagn eksplicit slås til og ikke fra.

3.5.3 Organisatoriske foranstaltninger (kontrolmål C)

Formål

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

Anvendte procedurer og kontroller

For at imødekomme den dataansvarliges krav om passende tekniske og organisatoriske sikringsforanstaltninger til beskyttelse af personoplysninger har Emini som databehandler implementeret formelle processer, politikker og kontroller. Formelle dokumenter som it-sikkerhedspolitikken bliver hvert år revurderet og godkendt på et særskilt sikkerhedsmøde. Der tages referat af dette møde. Referatet underskrives af direktionen og virksomhedens ledende medarbejdere.

Kun autoriserede medarbejdere hos Emini har adgang til data og ret til at behandle data. Disse autorisationer kontrolleres løbende og minimum en gang om året i forbindelse med et årligt sikkerhedsmøde. Der foretages efterprøvning af Eminis medarbejdere i forbindelse med deres ansættelse. Efterprøvningen omfatter indhentning af referencer fra tidligere ansættelser samt relevante eksamensbeviser. Straffeattester indhentes ikke.

3.5.4 Sletning og tilbagelevering (kontrolmål D)

Formål

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

Anvendte procedurer og kontroller

Systemet giver mulighed for, at oplysninger, som måtte være registreret om den registrerede, kan udleveres elektronisk til den registrerede. Det kan eksempelvis være i form af en PDF- eller CSV-fil.
Det er den dataansvarlige (i dette tilfælde Eminis kunder), der er ansvarlig for, at den registreredes ret til gennemsigtig oplysning overholdes.

Systemet giver mulighed for på en nem og overskuelig måde at redegøre for, hvilke data der opbevares, og hvor i systemet data opbevares, for den enkelte registrerede.

Der er i systemet indbygget en funktionalitet, som sikrer, at den registreredes ret til sletning af egne registrerede persondata, kan understøttes.

I hhv. kontrakt og databehandleraftalen er det fastsat, at den dataansvarlige (i dette tilfælde Eminis kunder) er ansvarlig for at oprette og vedligeholde data, og at den dataansvarlige dermed også har underretningspligt ved berigtigelse eller sletning af personoplysninger.

3.5.5 Opbevaring af data (kontrolmål E)

Formål

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

Anvendte procedurer og kontroller

Eminis behandling og opbevaring af data som databehandler, er reguleret af hhv. kontrakt og databehandleraftaler. Emini behandler data alene efter instruks.

De behandlingsaktiviteter, som udføres af Emini på vegne af den dataansvarlige, fremgår af hhv. kontrakt og databehandleraftaler og er som sådan godkendt af den dataansvarlige (i dette tilfælde Eminis kunder).

3.6.6 Anvendelse af underdatabehandlere (kontrolmål F)

Formål

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

Anvendte procedurer og kontroller

Det er defineret i databehandleraftaler, at der er passende logisk og organisatorisk sikkerhed omkring PeopleTrust-platformen.

I forhold til kunden er Emini databehandler eller underdatabehandler. Eminis adgang til og kundernes brug af systemet er reguleret af hhv. kontrakt og databehandleraftaler. Databehandleraftalen tager udgangspunkt i Datatilsynets vejledning på området. Emini arbejder alene efter instruks.

Emini anvender underleverandører i forbindelse med hosting og drift af serverne. I forhold til kundens kunde er Eminis underleverandør tredjepartsdatabehandler. Underleverandørens adgang til serverne er reguleret af hhv. kontrakt og databehandleraftaler. Eminis underleverandører arbejder alene efter instruks.

3.6.7 Bistand til dataansvarlige (kontrolmål H)

Formål

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

Anvendte procedurer og kontroller

Systemet giver mulighed for, at oplysninger, som måtte være registreret om den registrerede, kan udleveres elektronisk til den registrerede. Det kan eksempelvis være i form af en PDF- eller CSV-fil.

Der er i systemet indbygget en funktionalitet, som sikrer, at den registreredes ret til sletning af egne registrerede persondata, kan understøttes.

3.5.8 Sikkerhedsbrud (kontrolmål I)

Formål

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

Anvendte procedurer og kontroller

For at etablere tilstrækkelig sikkerhed og forhindre, at der sker behandling i strid med gældende lovgivning eller god praksis på området, sikrer Emini et højt sikkerhedsniveau. I den forbindelse foretager Emini løbende en vurdering af risici og de mulige konsekvenser ved sikkerhedsbrud samt de foranstaltninger, Emini har implementeret.

Af Eminis sikkerhedspolitik og i de med den dataansvarlige (i dette tilfælde Eminis kunder) indgåede databehandleraftaler fremgår retningslinjer for kommunikation med relevante parter, herunder rapportering og bistand til den dataansvarlige ved sikkerhedshændelser.

Af Eminis sikkerhedspolitik og i de med den dataansvarlige (i dette tilfælde Eminis kunder) indgåede databehandleraftaler fremgår retningslinjer for kommunikation med relevante parter, herunder rapportering til den dataansvarlige ved sikkerhedshændelser. Den dataansvarlige har derefter ansvaret for at underrette de registrerede.

Komplementerende kontroller hos de dataansvarlige

- Dataansvarlig er ansvarlig for, hvilke oplysninger der registreres.
- Dataansvarlig er ansvarlig for, at oplysninger om behandlingen af personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.
- Dataansvarlig er ansvarlig for at sikre, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt oplysning om eventuel overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer.
- Dataansvarlig er ansvarlig for, at den registreredes ret til berigtigelse om behandlingen af personoplysninger overholdes.
- Dataansvarlig er ansvarlig for, at den registreredes ret til sletning af egne registrerede personoplysninger overholdes.
- Dataansvarlig er ansvarlig for, at den registreredes ret til dataportabilitet overholdes.
- Dataansvarlig er ansvarlig for at definere perioden i systemet for, hvornår data slettes.
- Dataansvarlig er ansvarlig for løbende at gennemgå login- og hændelseslog og udtage enkelthændelser til særskilt kontrol efter vurdering.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Introduktion

Denne rapport er udformet med henblik på at informere Eminis kunder om PeopleTrust-platformen og kontroller, som kan påvirke behandlingen af personoplysninger, og samtidig informere de dataansvarlige, for hvem Emini behandler personoplysninger, om funktionaliteten af de kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne hos de dataansvarlige, har til hensigt at hjælpe de dataansvarlige med at vurdere risici forbundet med den outsourcede behandling af personoplysninger, som muligvis påvirkes af kontrollerne hos Emini.

Vores test af Eminis kontroller er begrænset til de kontrolmål og relaterede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller kontroller, som forventes at være implementeret hos de dataansvarlige for at opfylde kontrolmålene.

Det er den dataansvarliges ansvar at evaluere denne information i forhold til de kontroller, som eksisterer hos den dataansvarlige. Hvis bestemte komplementerende kontroller ikke er til stede hos den dataansvarlige, kan Eminis kontroller muligvis ikke kompensere for sådanne svagheder.

4.2 Test af kontroller

De udførte tests i forbindelse med fastlæggelse af kontrollers funktionalitet består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos Emini
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelse af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.

4.3 Kontrolmål, kontroller og resultater af test

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

Kontrolmål A **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum en årlig vurdering af behovet for opdatering, herunder ved ændringer i den dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Ingen bemærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruksen fra den dataansvarlige.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene sker i henhold til instruks. Stikprøvevist inspiceret, at behandling af personoplysninger sker i overensstemmelse med instruks.	Ingen bemærkninger.

Kontrolmål A **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelserne 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 vurderes at være i strid med lovgivningen.	Ingen bemærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger til behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikringsforanstaltninger. Inspiceret, at procedurer er opdateret. Stikprøvevist inspiceret, at der er etableret de aftalte sikringsforanstaltninger i databehandleraftalerne.	Ingen bemærkninger.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med den dataansvarlige aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen bemærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Inspiceret, at antivirussoftware er opdateret.	Ingen bemærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem en sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewallregler er konfigureret i henhold til den interne politik herfor.	Ingen bemærkninger.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen bemærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.6	Adgang til personoplysninger er begrænset 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 brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelse af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Stikprøvevist inspiceret, at brugeres adgange til systemer og databaser er begrænset ud fra medarbejdernes arbejdsbetingede behov.	Ingen bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen bemærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og pr. 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 pr. e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, og om de dataansvarlige er behørigt orienteret herom.	Ingen bemærkninger.
B.9	Der er etableret logning i PeopleTrust-platformen.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i PeopleTrust-platformen, der anvendes til behandling og transmission af personoplysninger. Inspiceret, at logning af brugeraktiviteter i PeopleTrust-platformen, er konfigureret og aktiveret.	Ingen bemærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.10	Screensaver er påtvunget på klienter.	Inspiceret, at der er implementeret pause-skærm, herunder automatisk låsning af skærm.	Ingen bemærkninger.
B.11	Brugerne/kunderne har personlige kodeord med komplekse krav og 8 karakterer. Eminis egne medarbejdere er underlagt særskilte, komplekse krav, og sikrer selv, at kodeord er skiftet inden for de seneste 12 måneder.	Inspiceret, at der foreligger en it-sikkerheds-politik, hvori kodeordskrav er defineret. Inspiceret, at kodeordskrav er implementeret i PeopleTrust-platformen.	Vi har under vores gennemgang konstateret, at Eminis egne medarbejdere ikke påtvinges at skifte kodeord på deres lokale konto efter 12 måneder. Ingen yderligere bemærkninger.
B.12	Emini overvåger, at driftsleverandøren foretager ændringer til systemer, databaser og netværk efter fastlagte procedurer, som sikrer vedligeholdelse gennem relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for overvågning af driftsleverandørens håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.	Ingen bemærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgange revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes med et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugeradgange til systemer og databaser, som anvendes til behandling af personoplysninger. Stikprøvevist inspiceret, at medarbejderes adgange til systemer og databaser er godkendte, og tildelt ud fra et arbejdsbetinget behov. Inspiceret, at der foreligger dokumentation for regelmæssig – mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Ingen bemærkninger.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen bemærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i strid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Stikprøvevist inspiceret, at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerhed.	Ingen bemærkninger.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.3	Der udføres efterprøvning af databehandlerens medarbejdere i forbindelse med deres ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Eksamensbeviser.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med deres ansættelse. Inspiceret ved en stikprøve på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Stikprøvevist inspiceret dokumentation for, at efterprøvningen af nyansatte medarbejdere i erklæringsperioden har omfattet: • Referencer fra tidligere ansættelser • Eksamensbeviser.	Vi har konstateret, at der for en nyansat medarbejder ikke er blevet indhentet referencer fra tidligere ansættelser eller eksamensbevis. Ingen yderligere bemærkninger.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitikken og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Stikprøvevist inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale. Stikprøvevist inspiceret, at nyansatte medarbejdere i erklæringsperioden er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information.	Ingen bemærkninger.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver såsom adgangskort, pc, mobiltelefon mv. inddrages.	Ingen bemærkninger.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, og at medarbejderen er underlagt en generel tavshedspligt i relation til den behandling af personoplysninger, som databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksomme på opretholdelse af fortrolighedsaftalen og deres generelle tavshedspligt.	Ingen bemærkninger.
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 i 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 bemærkninger.

Kontrolmål D **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Personoplysninger opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret. Det er således den dataansvarliges eget ansvar at slette eventuelle persondata i henhold til gældende lovgivning, kutyme og andre retningslinjer.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Stikprøvevist inspiceret på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger kan slettes i overensstemmelse med de aftalte sletterutiner.	Ingen bemærkninger.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor dette ikke er i strid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Stikprøvevist inspiceret dokumentation for, at Emini har foretaget tilbagelevering/sletning af data i henhold til proceduren ved ophør af behandling af personoplysninger for den dataansvarlige.	Ingen bemærkninger.

Kontrolmål E **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Stikprøvevist inspiceret, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen bemærkninger.
E.2	Databehandlerens databehandling, herunder 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. Stikprøvevist inspiceret, 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 bemærkninger.

Kontrolmål F **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der specifikt eller generelt er godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Stikprøvevist inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen bemærkninger.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere 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 anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Vi har fået oplyst, at der ikke har været ændring i anvendelsen af underdatabehandlerne i erklæringsperioden. Ingen bemærkninger.

Kontrolmål F **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen eller lignende med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Stikprøvevist inspiceret, at underdatabehandleraftalerne indeholder de samme krav og forpligtelser, som er anført i databehandleraftalerne mellem Emini og de dataansvarlige.	Ingen bemærkninger.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de påkrævede oplysninger om de enkelte underdatabehandlere.	Ingen bemærkninger.

Kontrolmål F **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.6	Databehandleren foretager på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren, såfremt opfølgningen giver anledning til forhold, som måtte vedrøre dataansvarlige og Eminis behandling af personoplysninger på vegne af dataansvarlige.	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 den senest indhentede ISAE 3402 erklæring og ISAE 3000 erklæring, dækkende 2019, fra Sentia og konstateret, at der er foretaget opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerhed, tredjelandsoverførsel og lignende. Inspiceret den senest indhentede SOC2 erklæring, dækkende 2019, fra Interxion og konstateret, at der er foretaget opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerhed, tredjelandsoverførsel og lignende. Forespurgt, om der er foretaget orientering til dataansvarlige i forbindelse med opfølgning hos underdatabehandlere.	Ingen bemærkninger.

Kontrolmål H **Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med rettelse og sletning af oplysninger om behandling af personoplysninger, udlevering af sådanne oplysninger til den registrerede eller begrænsning af behandling af personoplysninger.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
H.2	Databehandleren har etableret procedurer, som, i det omfang dette er aftalt, muliggør rettidig bistand til den dataansvarlige i relation til rettelse og sletning af oplysninger om behandling af personoplysninger, udlevering af sådanne oplysninger til den registrerede eller begrænsning af behandling af personoplysninger.	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 dokumentation for, at de anvendte systemer og databaser understøtter gennemførelse af de nævnte detaljerede procedurer. Stikprøvevist inspiceret, at udlevering, rettelse eller sletning af oplysninger om behandling af personoplysninger, begrænsning af sådan behandling eller oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.	Ingen bemærkninger.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen bemærkninger.
I.2	Databehandleren har etableret følgende kontroller for identificering af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik.	Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i identificering af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges, og at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv.	Ingen bemærkninger.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet gjort 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 gjort opmærksom på bruddet på persondatasikkerheden.	Vi har fået oplyst, at der ikke har været nogen brud på persondatasikkerheden inden for de seneste 12 måneder. Ingen yderligere bemærkninger.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Anmeldelsen skal indeholde en beskrivelse 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 procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser ved 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 til håndtering af bruddet på persondatasikkerheden.	Vi har fået oplyst, at der ikke har været nogen brud på persondatasikkerheden inden for de seneste 12 måneder. Ingen yderligere bemærkninger.