



# revi-it

et trygt samfund med it og data

## Revisorerklæring

### Emento A/S

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder der har anvendt digital forløbsguide i perioden fra 1. april 2021 til 31. marts 2022.

Maj 2022

REVI-IT A/S | [www.revi-it.dk](http://www.revi-it.dk)  
Højbro Plads 10, 1200 København K  
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | [info@revi-it.dk](mailto:info@revi-it.dk)  
[www.dpo-danmark.dk](http://www.dpo-danmark.dk) | [www.revi-cert.dk](http://www.revi-cert.dk)

## Indholdsfortegnelse

Afsnit 1:	Emento A/S' beskrivelse af behandlingsaktivitet for leverancen af digital forløbsguide .....	1
Afsnit 2:	Emento A/S' udtalelse.....	4
Afsnit 3:	Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder der har anvendt digital forløbsguide i perioden fra 1. april 2021 til 31. marts 2022 .....	6
Afsnit 4:	Kontrolmål, udførte kontroller, test og resultater heraf .....	9

## Afsnit 1: Emento A/S' beskrivelse af behandlingsaktivitet for leverancen af digital forløbsguide

### Formålet med og baggrunden for databehandlingen

Formålet med og baggrunden for databehandlingen er, at Emento i forbindelse med levering, drift og vedligehold af Emento Forløbsguide, foretager behandling af persondata på vegne af den Dataansvarlige.

Emento Forløbsguide er en service til løbende kommunikation mellem:

- Patient/borger og/eller hospital/kommune eller
- Medarbejdere og arbejdsgiver.

Platformen består af en app, der er rettet mod borgeren/patienten/medarbejderen og en webadgang, der er rettet mod personalet. Personalet definerer et forløb som via en app løbende guider og informerer borgeren/patienten/medarbejderen.

Via appen kan borgerne/patienterne/medarbejderne sende beskeder til personalet.

### Ementos opgave

Ementos opgave er at udvikle, hoste, drifte, vedligeholde og supportere systemet.

Det er også Ementos opgave at gøre data i systemet tilgængelig for kunden på en sådan måde, at kunden kan analysere og bruge data til at bidrage til forbedring af systemet, borgernes/patienternes/medarbejderens kommunikationsforløb og arbejdsgange hos kunden.

Beskeder sendt i systemet mellem borgeren/patienten/medarbejderen og kunden, kan også blive undersøgt for at se, om der er noget information, der eventuelt kunne mangle i kommunikationsforløbet. Dertil vil personalets brug af systemet blive undersøgt for at kvalificere og tilrette arbejdsgange i systemet. Der er implementeret passende kontroller, herunder logs, der dokumenterer alle interaktioner.

### Kategorier af registrerede personer

Databehandlingen vil omfatte følgende kategorier af registrerede personer:

- Borgere/Patienter med et kommunikationsforløb hos kunden
- Nye medarbejdere med et kommunikationsforløb hos kunden
- Personale hos kunden, som anvender løsningen

## Kategorier af data der behandles

Emento behandler følgende kategorier af oplysninger:

### *Almindelige personoplysninger:*

- Identifikationsoplysninger, herunder navn, billede og e-mail
- Oplysninger om tildelte kommunikationsforløb
- Sprog og uddannelse
- Beskeder sendt mellem patient/borger og afdeling, herunder billeder sendt i beskedsystemet.
- Tekstuelle svar givet på aktiviteter
- Oplysninger om organisatorisk tilknytning samt profession og roller

### *Følsomme personoplysninger:*

- I nogle forløb kan der indgå helbredsoplysninger

### *Fortrolige personoplysninger:*

- Borger/patienters CPR.nr. anvendes til oprettelse og verificering i systemet

Fordeling af dataansvar aftales i de specifikke aftaler med kunden.

## Praktiske tiltag

Emento har implementeret principperne fra ISO27001 og dertilhørende relevante kontroller samt en række tekniske og organisatoriske sikkerhedsforanstaltninger, der sikrer efterlevelse af den Europæiske General Data Protection Regulation og den danske Databeskyttelseslov

Tiltagene omfatter bl.a.:

- Fortegnelser over databehandlingsaktiviteter og deres juridiske hjemmel
- Slettefrister, sletteprocedurer og sletteinstrukser
- Privacy policy, Cookie policy, samtykkeerklæring og privacy notices (jvf. oplysningspligten)
- Procedurer for opfyldelse af de registreredes rettigheder (ret til indsigt, dataportabilitet, ret til sletning, ret til berigtigelse), herunder logs over henvendelser, muligheden for at få udleveret data i maskinlæsbart format og uddannelse af alle medarbejdere i GDPR
- Procedurer for tilsyn med databehandlere

## Risikovurdering

Risikovurdering og -håndtering sker som en løbende aktivitet i Emento, hvor sandsynlighed og konsekvens af potentielle hændelser vurderes i forhold til kompromittering af de registreredes rettigheder.

## Kontrolforanstaltninger

Emento har implementeret en række kontrolforanstaltninger for at tilsikre et ensartet højt niveau for informationssikkerhed. Kontrol af disse foranstaltninger, frekvens for kontrol og den ansvarlige, er beskrevet i Årshjulet.

Der gennemføres løbende awareness-aktiviteter for alle medarbejdere og tilknyttede konsulenter i Emento.

## Komplementerende kontroller hos de dataansvarlige

Eventuelle komplementerende kontroller hos de dataansvarlige fremgår af de specifikke aftaler. Den dataansvarlige er ansvarlig for:

- at kortlægge og sikre den juridiske hjemmel til behandling af personoplysninger. Emento handler på instruks fra den dataansvarlige,
- at sikre, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering,
- at sikre, at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen,
- at sikre, at den dataansvarliges brugere er ajourførte,
- at efterleve oplysningspligten til de registrerede om udøvelsen af deres rettigheder,
- at besvare anmodninger og kontrollere identiteten af de registrerede, der ønsker at udøve deres rettigheder.

## Afsnit 2: Emento A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Emento A/S' kunder, som har indgået en databehandler-aftale med Emento A/S og som har anvendt digital forløbsguide, 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.

Emento A/S anvender underleverandørerne og underdatabehandlere Team.blue Denmark A/S og GatewayAPI. I erklæringsperioden er der foretaget et skift fra anvendelse af underleverandøren og underdatabehandlere Mailchimp til GatewayAPI. Endvidere er anvendelse af underdatabehandlere Vimeo afviklet i perioden. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Emento A/S' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

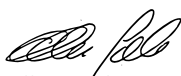
Enkelte af de kontrolmål, der er anført i Emento A/S' beskrivelse i afsnit 1 af digital forløbsguide, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Emento A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Emento A/S bekræfter, at:

- a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af, hvordan Emento A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 1. april 2021 til 31. marts 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
  - (i) Redegør for, hvordan Emento A/S' processer og kontroller relateret til databeskyttelse 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 Emento A/S' 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 digital forløbsguide til behandling af personoplysninger foretaget i hele perioden fra 1. april 2021 til 31. marts 2022.
- (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne digital forløbsguide 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 digital forløbsguide, som den enkelte dataansvarlige måtte anse vigtigt efter deres 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. april 2021 til 31. marts 2022, hvis relevante kontroller hos underleverandører var operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Emento A/S i hele perioden fra 1. april 2021 til 31. marts 2022. 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. april 2021 til 31. marts 2022
- 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.

Aarhus, den 12. maj 2022  
Emento A/S



Allan Juhl  
Adm. direktør



### Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder der har anvendt digital forløbsguide i perioden fra 1. april 2021 til 31. marts 2022

Til Emento A/S og Emento A/S' kunder i kundernes rolle som dataansvarlige.

#### Omfang

Vi har fået til opgave at afgive erklæring med høj grad af sikkerhed om Emento A/S' beskrivelse i "Afsnit 1" af digital forløbsguide i henhold til databehandleraftaler med deres kunder, i kundernes rolle som dataansvarlige i hele perioden fra 1. april 2021 til 31. marts 2022 og b+c) om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Emento A/S anvender underleverandørerne og underdatabehandlerne Team.blue Denmark A/S og GatewayAPI. I erklæringsperioden er der foretaget et skift fra anvendelse af underleverandøren og underdatabehandleren Mailchimp til GatewayAPI. Endvidere er anvendelse af underdatabehandleren Vimeo afviklet i perioden. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Emento A/S' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlerens kontroller, der forudsættes i designet af Emento A/S' kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos Emento A/S.

Enkelte af de kontrolmål, der er anført i Emento A/S' beskrivelse i afsnit 1 af digital forløbsguide, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Emento A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

#### Emento A/S' ansvar

Emento A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i "Afsnit 2", 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, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

#### Vores 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.



REVI-IT A/S anvender international standard om kvalitetsstyring, ISQC 1<sup>1</sup>, og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

## Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Emento A/S' beskrivelse samt om udformningen og funktionen 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 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 digital forløbsguide samt for kontrollerens udformning og 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 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, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "Afsnit 1".

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

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

---

<sup>1</sup> ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

## 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 digital forløbsguide, således som denne var udformet og implementeret i perioden fra 1. april 2021 til 31. marts 2022, i alle væsentlige henseender er retvisende, og
- (b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra 1. april 2021 til 31. marts 2022, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører var operationelt effektive, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Emento A/S' kontroller i perioden fra 1. april 2021 til 31. marts 2022, 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 perioden fra 1. april 2021 til 31. marts 2022.

## Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i afsnit 4.

## Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Emento A/S' digital forløbsguide, 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 databeskyttelsesforordningen er overholdt.

København, den 12. maj 2022

### REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Christian H. Riis  
Partner, CISA



Michael Marseen  
Statsautoriseret revisor

## Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

Vores arbejde er udført i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-I nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden fra 1. april 2021 til 31. marts 2022.

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Emento A/S' underleverandører og underdatabehandlere.

Kontroller udført hos de dataansvarlige er ikke omfattet af vores erklæring.

Vi har udført vores tests af kontroller hos Emento A/S via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Emento A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres.
Genduførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

## Kortlægning af kontrolområder op mod GDPR-artikler, ISO 27701 og ISO 27001/2

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2.

Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
A.1	5, 26, <b>28</b> , 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, <b>8.2.2</b>	Nyt område ift. ISO 27001/2
A.2	<b>28</b> , 29, 48	8.5.5, 6.15.2.2, <b>6.15.2.2</b>	18.2.2
A.3	<b>28</b>	<b>8.2.4, 6.15.2.2</b>	18.2.2
B.1	31, <b>32</b> , 35, 36	<b>5.2.2</b>	4.2
B.2	<b>32</b> , 35, 36	<b>7.2.5, 5.4.1.2, 5.6.2</b>	6.1.2, 5.1, 8.2
B.3	<b>32</b>	<b>6.9.2.1</b>	<b>12.2.1</b>
B.4	28 stk. 3; litra e, <b>32</b> ; <b>stk. 1</b>	<b>6.10.1.1, 6.10.1.2, 6.10.1.3, 6.11.1.3</b>	<b>13.1.2, 13.1.3, 14.1.3, 14.2.1</b>
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	<b>32</b>	<b>6.6</b>	9.1.1, 9.2.5
B.7	<b>32</b>	<b>6.9.4</b>	12.4
B.8	<b>32</b>	<b>6.15.1.5</b>	18.1.5
B.9	<b>32</b>	<b>6.9.4</b>	12.4
B.10	<b>32</b>	<b>6.11.3</b>	14.3.1
B.11	<b>32</b>	<b>6.9.6.1</b>	12.6.1
B.12	28, <b>32</b>	<b>6.9.1.2, 8.4</b>	12.1.2
B.13	<b>32</b>	<b>6.6</b>	9.1.1
B.14	<b>32</b>	<b>7.4.9</b>	Nyt område ift. ISO 27001/2
B.15	<b>32</b>	<b>6.8</b>	11.1.1-6
C.1	<b>24</b>	<b>6.2</b>	5.1.1, 5.1.2
C.2	<b>32, 39</b>	<b>6.4.2.2, 6.15.2.1, 6.15.2.2</b>	7.2.2, 18.2.1, 18.2.2
C.3	<b>39</b>	<b>6.4.1.1-2</b>	7.1.1-2
C.4	28, 30, <b>32, 39</b>	<b>6.10.2.3, 6.15.1.1, 6.4.1.2</b>	7.1.2, 13.2.3
C.5	<b>32</b>	<b>6.4.3.1, 6.8.2.5, 6.6.2.1</b>	7.3.1, 11.2.5, 8.3.1
C.6	<b>28, 38</b>	<b>6.4.3.1, 6.10.2.4</b>	7.3.1, 13.2.4
C.7	<b>32</b>	<b>5.5.3, 6.4.2.2</b>	7.2.2, 7.3
C.8	<b>38</b>	<b>6.3.1.1, 7.3.2</b>	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, <b>30, 32</b> , 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, <b>7.2.8</b> , 7.5.1, 7.5.2, 7.5.3, 7.5.4, <b>8.2.6</b> , 8.4.2, 8.5.2, 8.5.6	Nyt område ift. ISO 27001/2
D.1	6, 11, <b>13, 14, 32</b>	<b>7.4.5, 7.4.7, 7.4.4</b>	Nyt område ift. ISO 27001/2
D.2	6, 11, 13, 14, <b>32</b>	<b>7.4.5, 7.4.7, 7.4.4</b>	Nyt område ift. ISO 27001/2
D.3	13, <b>14</b>	<b>7.4.7, 7.4.4</b>	Nyt område ift. ISO 27001/2
E.1	13, 14, <b>28, 30</b>	<b>8.4.2, 7.4.7, 7.4.8</b>	Nyt område ift. ISO 27001/2
E.2	13, 14, <b>28, 30</b>	<b>8.4.2, 7.4.7, 7.4.8</b>	Nyt område ift. ISO 27001/2
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, <b>32</b> , 35, 40, 41, 42	5.2.1, <b>7.2.2, 7.2.6</b> , 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	<b>28</b>	<b>8.5.7</b>	15
F.3	<b>28</b>	<b>8.5.8, 8.5.7</b>	15
F.4	<b>33, 34</b>	<b>6.12.1.2</b>	15
F.5	<b>28</b>	<b>8.5.7</b>	15
F.6	<b>33, 34</b>	<b>6.12.2</b>	15.2.1-2
G.1	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1, 7.5.2, 7.5.3, 7.5.4, 8.5.1, 8.5.2, 8.5.3</b>	13.2.1, 13.2.2

<b>G.2</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, <b>8.4.2</b> , 8.5.2, 8.5.3	13.2.1
<b>G.3</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
<b>H.1</b>	12, <b>13, 14</b> , 15, 20, 21	<b>7.3.5, 7.3.8, 7.3.9</b>	<i>Nyt område ift. ISO 27001/2</i>
<b>H.2</b>	12, <b>13, 14</b> , 15, 20, 21	<b>7.3.5, 7.3.8, 7.3.9</b>	<i>Nyt område ift. ISO 27001/2</i>
<b>I.1</b>	<b>33, 34</b>	<b>6.13.1.1</b>	16.1.1-5
<b>I.2</b>	<b>33, 34</b> , 39	6.4.2.2, <b>6.13.1.5, 6.13.1.6</b>	16.1.5-6
<b>I.3</b>	<b>33, 34</b>	<b>6.13.1.4</b>	16.1.5
<b>I.4</b>	<b>33, 34</b>	<b>6.13.1.4</b> , 6.13.1.6	16.1.7

## Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
A.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Vi har inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	<p>Vi har inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.</p>	Ingen afvigelser konstateret.
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.	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Vi har inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.</p> <p>Vi har forespurgt, om databehandleren har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.</p>	<p>Vi er blevet informeret om, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, hvorfor vi ikke har kunnet testet effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>

## Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p> <p>Vi har stikprøvevis inspiceret, at der er etableret de sikringsforanstaltninger, der er aftalt i databehandleraftaler.</p>	Ingen afvigelser konstateret.
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 dataansvarlige aftalte sikringsforanstaltninger.	<p>Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Vi har inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Vi har stikprøvevis inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.</p>	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	<p>Vi har inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software.</p> <p>Vi har inspiceret, at antivirus software er opdateret.</p>	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	<p>Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.</p> <p>Vi har inspiceret, at firewall er konfigureret i henhold til intern politik herfor.</p>	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	<p>Vi har forespurgt, hvorvidt interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.</p> <p>Vi har inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.</p>	Ingen afvigelser konstateret.



## Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugernes adgang til personoplysninger.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.</p> <p>Vi har inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.</p> <p>Vi har stikprøvevis inspiceret, at brugernes adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.</p>	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	<p>Vi har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret systemovervågning med alarmering.</p> <p>Vi har stikprøvevis inspiceret, at der er sket opfølgning på alarmer.</p>	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	<p>Vi har 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.</p> <p>Vi har inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden.</p> <p>Vi har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.</p> <p>Vi har forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.</p>	Ingen afvigelser konstateret.

## Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.9	Der er etableret logning i systemer, databaser og netværk.  Logoplysninger er beskyttet mod manipulation og tekniske fejl.	Vi har 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 og opfølgning på logs.  Vi har inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.  Vi har inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen afvigelser konstateret.
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.	Vi har 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.  Vi har stikprøvevis inspiceret, at personoplysninger er pseudonymiseret eller anonymiseret i udviklings- og testdatabaser.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har stikprøvevis inspiceret, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.  Vi har inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.  Vi har stikprøvevis inspiceret, at ændringer håndteres jf. proceduren.	Ingen afvigelser konstateret.

## Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Vi har stikprøvevis inspiceret, at medarbejdernes adgange til systemer og databaser er godkendt, og at der er et arbejdsbetinget behov.</p> <p>Vi har inspiceret, at der foreligger dokumentation for regelmæssig – og mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.</p>	Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede.</p> <p>Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.</p>	Ingen afvigelser konstateret.
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.	<p>Vi har 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.</p> <p>Vi har inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.</p>	Ingen afvigelser konstateret.

## Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/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. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering.  Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.  Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.  Vi har stikprøvevis inspiceret, at kravene til efterprøvning af medarbejdere i databehandleraftalerne er dækket af databehandlerens procedurer for efterprøvning.  Vi har stikprøvevis inspiceret, at der er dokumentation for, at efterprøvningen af nyansatte medarbejdere i erklæringsperioden har omfattet: <ul style="list-style-type: none"> <li>• Ansøgerens CV</li> <li>• Uddannelse og professionelle kvalifikationer</li> <li>• Verificering af straffeattest</li> </ul>	Ingen afvigelser konstateret.

## Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	<p>Vi har stikprøvevis inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale.</p> <p>Vi har stikprøvevis inspicere, at nyansatte medarbejdere i erklæringsperioden er blevet introduceret til:</p> <ul style="list-style-type: none"> <li>Informationssikkerhedspolitikken</li> <li>Procedurer vedrørende databehandling, samt anden relevant information</li> </ul>	Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	<p>Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages</p> <p>Vi har forespurgt om der har været fratrådte medarbejdere i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været nogle fratrådte medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>
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, databehandleren udfører for de dataansvarlige.	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.</p> <p>Vi har forespurgt om der har været fratrådte medarbejdere i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været nogle fratrådte medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	<p>Vi har inspiceret, at databehandleren udbyder awarenessstræning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.</p> <p>Vi har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awarenessstræning.</p>	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	<p>Vi har inspiceret dokumentation for, at databehandleren har vurderet behov for en databeskyttelsesrådgiver i perioden.</p> <p>Vi har inspiceret dokumentation for, at DPO'en er blevet inddraget i relevante opgaver i erklæringsperioden.</p>	Ingen afvigelser konstateret.

## Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
C.9	<p>Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.</p> <p>Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige indeholder:</p> <ul style="list-style-type: none"> <li>• Navn og kontaktoplysninger på databehandleren, de dataansvarlige, den dataansvarliges eventuelle repræsentanter og databeskyttelsesrådgivere</li> <li>• De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige</li> <li>• Når det er relevant, oplysninger om overførsel til et tredjeland eller en international organisation samt dokumentation for passende garantier</li> <li>• Hvis det er muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger.</li> </ul> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om fortegnelsen skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Vi har inspiceret, at fortegnelser indeholder:</p> <ul style="list-style-type: none"> <li>• Navn og kontaktoplysninger på databehandleren, de dataansvarlige, den dataansvarliges eventuelle repræsentanter og databeskyttelsesrådgivere</li> <li>• De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige</li> <li>• Når det er relevant, oplysninger om overførsel til et tredjeland eller en international organisation samt dokumentation for passende garantier</li> <li>• Hvis det er muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger.</li> </ul>	Ingen afvigelser konstateret.

## Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
D.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	Ingen afvigelser konstateret.

## Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.  Vi har inspiceret, at procedurerne er opdaterede.  Vi har stikprøvevis inspiceret, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: <ul style="list-style-type: none"> <li>Tilbageleveret til den dataansvarlige og/eller</li> <li>Slettet, hvor det ikke er i modstrid med anden lovgivning.</li> </ul>	Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.  Vi har forespurgt til ophørte databehandlinger i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været ophørte databehandlinger i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.  Ingen afvigelser konstateret.

## Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.  Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.



## Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	<p>Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.</p> <p>Vi har stikprøvevis 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.</p>	Ingen afvigelser konstateret.

## Kontrolmål F – Anvendelse af underdatabehandlere

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt 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.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
F.1	<p>Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	<p>Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere.</p> <p>Vi har stikprøvevis inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.</p>	Ingen afvigelser konstateret.

## Kontrolmål F – Anvendelse af underdatabehandlere

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt 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.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har forespurgt til procedurer for underretning af de dataansvarlige ved ændringer i anvendelse af generelt godkendte underdatabehandlere.  Vi har inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.  Vi har stikprøvevis inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.  Vi har inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.  Vi har forespurgt vedrørende risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.  Vi har inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelandes overførselsgrundlag og lignende.	Ingen afvigelser konstateret.

## Kontrolmål G – Overførsel af personoplysninger til tredjelande

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.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
G.1	<p>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.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har 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.</p> <p>Vi har inspiceret, at procedurerne er opdateret.</p>	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	<p>Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over underdatabehandlere hvor der er risiko for overførsler af personoplysninger til tredjelande eller internationale organisationer.</p> <p>Vi har stikprøvevist inspiceret, at der i databehandleraftalerne, er specificeret procedure for overførsel af personoplysninger til tredjelande.</p>	Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag.</p> <p>Vi har inspiceret, at procedurerne er opdateret.</p> <p>Vi har stikprøvevist inspiceret, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige.</p>	Ingen andre afvigelser konstateret.

## Kontrolmål H – De registreredes rettigheder

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.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
H.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Vi har inspiceret, at procedurerne er opdaterede.</p>	Ingen afvigelser konstateret.
H.2	<p>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.</p>	<p>Vi har inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> <li>• Udlevering af oplysninger</li> <li>• Rettelse af oplysninger</li> <li>• Sletning af oplysninger</li> <li>• Begrænsning af behandling af personoplysninger</li> <li>• Oplysning om behandling af personoplysninger til den registrerede.</li> </ul> <p>Vi har inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.</p>	Ingen afvigelser konstateret.

## Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	Emento A/S' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Vi har inspiceret, at proceduren er opdateret.</p>	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	<p>Vi har inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p> <p>Vi har inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.</p>	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	<p>Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p> <p>Vi har forespurgt, om der har været persondatasikkerhedsbrud i erklæringsperioden.</p>	<p>Vi er blevet informeret om, at der ikke har været nogen persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret.</p>
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Data-tilsynet.	<p>Vi har inspiceret, at der foreligger procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Vi har inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p>	Ingen afvigelser konstateret.