

Maj 2021

# SystemGruppen A/S

ISAE 3000 TYPE 2 ERKLÆRING

CVR 21697974

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informations-sikkerhed og foranstaltninger i henhold til databehandleraftalen med data-ansvarlige.

**Beierholm**  
**Statsautoriseret Revisionspartnerselskab**  
Knud Højgaards Vej 9  
2860 Søborg  
CVR 32 89 54 68  
Tlf +45 39 16 76 00

[www.beierholm.dk](http://www.beierholm.dk)



# Erklæringsopbygning

## Kapitel 1:

Ledelseserklæring.

## Kapitel 2:

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftalen med SystemGruppen A/S' kunder.

## Kapitel 3:

Beskrivelse af behandling.

## Kapitel 4:


Kontrolmål, kontrolaktivitet, test og resultat heraf.

## Ledelseserklæring

SystemGruppen A/S behandler personoplysninger på vegne af sine kunder i henhold til databehandleraftalen for hostingaktiviteter.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt SystemGruppen A/S hostingaktiviteter, 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. SystemGruppen A/S bekræfter, at:

- (A) Den medfølgende beskrivelse, kapitel 3, giver en retvisende beskrivelse af SystemGruppen A/S' hostingaktiviteter, der har behandlet personoplysninger for dataansvarlige omfattet af i hele perioden fra 1. april 2020 til 31. januar 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
- (i) Redegør for, hvordan kontrollerne 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 kunden dvs. den dataansvarlige
    - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
    - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
    - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registre-rede
    - 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 systemets 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 anvendte forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger
  - (ii) Indeholder relevante oplysninger om ændringer ved SystemGruppen A/S' hostingaktiviteter i behandlingen af personoplysninger foretaget i hele perioden fra 1. april 2020 til 31. januar 2021.
  - (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov



hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontroller, som den enkelte kunde måtte anse som 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 2020 til 31. januar 2021. 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 anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer 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 2020 til 31. januar 2021.
- (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.

Aalborg, den 19. maj 2021

**Direktør, Olafur Birgisson**

SystemGruppen A/S, Gugvej 128, DK-9210 Aalborg SØ, CVR-nummer: 21697974

# Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftalen med SystemGruppen A/S' kunder

Til SystemGruppen A/S og relevante dataansvarlige

## Omfang

Vi har fået som opgave at afgive erklæring om SystemGruppen A/S' beskrivelse af hostingaktiviteterne jf. kapitel 3 i henhold til databehandleraftale med SystemGruppen A/S' kunder, i hele perioden fra 1. april 2020 til 31. januar 2021 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

## SystemGruppen A/S' ansvar

SystemGruppen A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse jf. kapitel 3, 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.

## Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisors 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.

Beierholm 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 SystemGruppen 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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sit system samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet og implementeret.

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 sit system samt for kontrollernes 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 kapitel 3.

### Begrænsninger i kontroller hos SystemGruppen A/S

SystemGruppen 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 hostingaktiviteterne, 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.

### 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 hostingaktiviteterne, således som denne var udformet og implementeret i hele perioden fra 1. april 2020 til 31. januar 2021, i alle væsentlige henseender er retvisende, og
- b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. april 2020 til 31. januar 2021
- c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. april 2020 til 31. januar 2021

### Beskrivelse af test kontroller

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

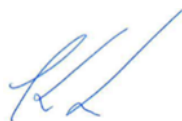
### Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 3 er udelukkende tiltænkt SystemGruppen A/S' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Søborg, den 20. maj 2021

#### Beierholm

Statsautoriseret Revisionspartnerselskab



Kim Larsen  
Statsautoriseret revisor



Allan Nielsen  
IT auditor, Konsulent

## Beskrivelse af behandling

### Indledning

Formålet med nærværende beskrivelse er at levere informationer til SystemGruppens kunder og deres revisorer vedrørende kravene i ISAE 3000, som er den internationale revisorstandard for andre erklæringsopgaver med sikkerhed herunder informationsikkerhed og foranstaltninger i henhold til databehandleraftalen med dataansvarlige.

Omfanget af denne beskrivelse er en afdækning af de kontroller som SystemGruppen har indført med henblik på efterlevelse af databehandleraftalens instrukser i forbindelse med opbevaring af data, sletning af data og anvendelse af underdatabehandlere. For afdækningen af de tekniske og organisatoriske kontroller for driften af hostingaktiviteterne samt kontrollerne for styring af informationsikkerhedsbrud henvises der til SystemGruppens ISAE 3402 type 2 erklæring.

### Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om backup af data samt oprettelse og nedlæggelse af brugere af de hostingaktiviteter som SystemGruppen leverer.

### Personoplysninger

Jf. de indgåede databehandleraftaler behandler SystemGruppen følgende typer personoplysninger:

#### Almindelige personoplysninger

- Navn
- Adresse
- E-mail
- Telefonnummer
- Betalingsoplysninger
- Kreditkortnummer
- Medarbejder ID
- Eksamensbeviser
- Kørekort
- Skatteoplysninger
- Pensionsoplysninger
- Forsikringsoplysninger
- Uddannelse
- Pas nummer
- Nummerplade

#### Følsomme personoplysninger

- Familieforhold
- Personlighedstest
- Færdighedstest
- Oplysninger om strafbare forhold
- Arbejds- og opholdstil-ladelse

#### Særligt følsomme personoplysninger

- Religiøs overbevisning
- Politiks overbevisning
- Filosofisk overbevisning
- Oplysninger om seksuel orientering
- Fagforeningsmæssigt tilhørsforhold
- Race og etnisk oprindelse
- Genetisk og biometriske forhold

Kategorier af registrerede personer omfattet af databehandleraftalen:

- ansatte
- klienter
- kunder
- samarbejdspartnere

## Risikostyring i SystemGruppen A/S

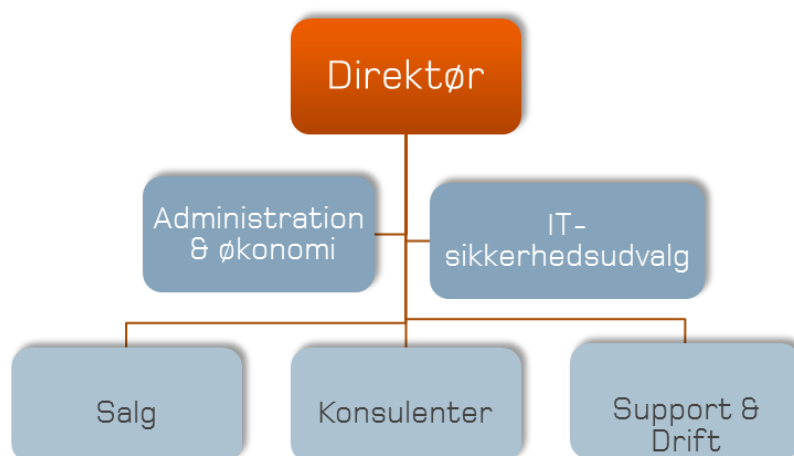
Det er SystemGruppens politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde normal drift. SystemGruppen gennemfører risikostyring og interne kontroller på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering.

SystemGruppen har indarbejdet faste procedurer for risikovurdering af forretningen. Vi sikrer dermed, at de risici, som er forbundet med de services og ydelser, som vi stiller til rådighed, er minimeret til acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vi vurderer relevante i forbindelse med at revurdere vores generelle risikovurdering.

Ansvar for risikovurderingen ligger hos direktør Olafur B. Birgisson og skal efterfølgende forankres og godkendes hos virksomhedens ledelse.

## SystemGruppen A/S' organisation og organisering af IT-sikkerheden

Ansvar og organisering i SystemGruppen A/S fremgår af nedenstående organisationsdiagram:



Direktionen i SystemGruppen, som er den øverst ansvarlige for it-sikkerheden, sørger for, at der til staidighed er etableret procedurer og systemer, der understøtter overholdelsen af den til enhver tid gældende it-sikkerhedspolitik. For at understøtte dette har SystemGruppen etableret et it-sikkerhedsudvalg, som er ansvarlig for overordnede målsætninger for implementering af it-sikkerhed på serviceydelserne.

Det er driftschefen, som er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollerbart, hvor dette overhovedet er muligt, og være udtryk for "best practice" inden for de enkelte kontrolaktiviteter på serviceområder, som tilbydes kunderne.

IT-sikkerhedsudvalget består p.t. af følgende medlemmer:

- Direktør, Olafur B. Birgisson
- Teknisk chef, Christoffer Klarskov Jacobsen

Udvalget mødes 1 gang årligt for at fastsætte og følge op på målsætninger i relationen til it-sikkerheden.



## Håndtering af IT-sikkerheden

Ledelsen hos SystemGruppen har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt. Gennem den centrale it-sikkerhedspolitik har ledelsen beskrevet SystemGruppens struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

SystemGruppens kvalitetsstyringssystem er defineret ud fra den overordnede målsætning om at levere stabil og sikker it-drift til kunderne. For at kunne gøre det er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

SystemGruppens it-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen /sikkerhedshullet omgående. Fejlen registreres i en log over sikkerhedsbrist. Når fejlen er udbedret kontrollerer SystemGruppens Tekniske Chef fejlrrettelsen og melder fejlen afhjulpet i loggen.

Alle virtuelle servere og netværksopsætninger er dokumenteret. Alle ændringer i systemerne laves på baggrund af en RFC (Request For Change). Alle RFC gemmes som dokumentation. Udførelse af ændringen dokumenteres i SystemGruppens Sagssystem. Konfigurationsfiler til netværks-enheder (firewall, routere, switche og lignende) ligger gemt som strukturerede filer et centralt sted.

Sikkerhedspolitikken sætter de grundlæggende politikker for SystemGruppens infrastruktur og omhandler ikke forhold vedrørende specifikke produkter, ydelser eller brugere.

Sikkerhedspolitikken er udarbejdet, så SystemGruppen har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Minimum én gang om året gennemgås politikker, procedurer og den operationelle drift med henblik på forbedringer.

## Databehandling af persondata

I henhold til persondataforordningen er SystemGruppen databehandler. I praksis er SystemGruppens ydelser afgrænset til opbevaring og backup af data. Således har SystemGruppen ikke direkte adgang til kunders data, herunder persondata.

I kraft af databehandlingens reelle karakter vil det ofte ikke være relevant for SystemGruppen at bistå den dataansvarlige i relation til de registreredes rettigheder. I tilfælde af at der kommer en henvendelse fra en kunde vedrørende sådanne bistand vil der være tale om en særskilt konsulentopgave hvor kriterierne, herunder kundens instruks vedr. databehandlingen, aftales på forhånd.

Jf. den indgåede databehandleraftale mellem SystemGruppen og kunderne sker der ikke en overførsel af data til tredje lande.

Ved evt. brud på persondatasikkerhed underrettes den dataansvarlige så hurtigt som muligt jf. SystemGruppens databrudsproces.

Sletning af kunders data sker ved ophør af aftalen jf. SystemGruppens datasletningsprocedure.

## Underdatabehandlere

SystemGruppen benytter kun velrenommerede, gennemprøvede kvalitetsleverandører, som er i stand til at levere den aftalte kvalitet. Alle SystemGruppens leverandører er oprettet i SystemGruppens kreditor-system.

Minimum én gang årlig gennemgås de væsentligste leverandører for deres leveringsevne, kvalitet, pris og service.



Datakapacitet fremskaffes primært hos Sentia A/S, Curanet A/S og fra Microsoft Azure.

SystemGruppens egne servere er placeret i Sentia A/S lokaler i Odense og Curanet A/S i Skanderborg. Sentia og Curanet varetager drift af serverne op til det virtuelle niveau i de respektive datacentre. Samarbejdet og ansvarsfordelingen reguleres af en formel aftale mellem parterne.

Samarbejdet og ansvarsfordelingen mellem SystemGruppen og Microsoft reguleres af Microsofts SLA for de forskellige Azure services.

SystemGruppen sikrer kvaliteten af Sentias og Curanets datacentre ved at indhente en kopi af den årlige 3402 erklæring fra disse selskaber. Tilsvarende kontrollerer SystemGruppen kvaliteten i Microsofts Cloud leverancer ved at undersøge, hvilke standarder Microsoft forpligter sig til at leve op til. Dette gøres ved regelmæssige besøg på Microsofts trustcenter hjemmeside:

<https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>

### **Kundernes ansvar (komplementerende kontroller hos kunderne)**

Ovenstående beskrivelse er baseret på ovennævnte ramme, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Ansvar for de forretningssystemer og brugersystemer, som drives via SystemGruppens hostingaktiviteter, eller kundernes egne servere som driftes af SystemGruppen, er kundernes eget ansvar. Kunderne har ansvaret for sikring af nødvendige kontroller i forbindelse med systemudvikling, anskaffelse og ændringshåndtering.

SystemGruppen er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til SystemGruppens hostingaktiviteter. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Kunderne er ansvarlige for datatransmission til SystemGruppens hostingaktiviteter, og det er kundernes ansvar at skabe den nødvendige datatransmission til SystemGruppens datacentre. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

SystemGruppens beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af SystemGruppens hostingaktiviteter. Der kan udarbejdes specifikke beredskabsplaner for den enkelte kunde efter behov i forhold til risiko ved afbrydelse i forretningsprocesser.

## KAPITEL 4:

# Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

### KONTROLMÅL A:

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

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
<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>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>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>Inspiceret, at procedurer er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.</p>	<p>Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandleren mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.</p>	<p>Vi har forespurgt databehandleren om de har modtaget instrukser fra dataansvarlige, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.</p> <p>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 ikke ved vores test konstateret væsentlige afvigelser.</p>

## KONTROLMÅL D:

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

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
<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>Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:</p> <ul style="list-style-type: none"> <li>• Tilbageleveret til den dataansvarlige og/eller</li> <li>• Slettet 30 dage efter aftalens ophør</li> </ul>	<p>Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.</p> <p>Inspiceret ved en stikprøve på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

## KONTROLMÅL F:

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.

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
<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>Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er generelt godkendt af den dataansvarlige.</p>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere samt at der foreligger underdatabehandleraftaler.</p> <p>Inspiceret, at de anvendte underdatabehandlere fremgår databehandleraftalen.</p>	<p>Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.</p>
<p>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.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.</p> <p>Vi har forespurgt databehandleren om der er sket ændringer i anvendelsen af underdatabehandlere i erklæringsperioden.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.</p>	<p>Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.</p> <p>Inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

## KONTROLMÅL F:

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.

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	<p>Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.</p> <p>Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.</p> <p>Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.</p>	Vi har ikke ved vores test konstateret væsentlige afvigelser.

## KONTROLMÅL G:

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

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har forespurgt databehandleren om den kan bekræfte, at der ikke er sket overførsel af personoplysninger til tredjelande eller internationale organisationer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

## KONTROLMÅL H:

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

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
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.	Vi har forespurgt databehandleren, om der er sket anmodning fra dataansvarlige i relation til bistand om udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede i kontrolperioden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.