Grant Thornton

Revisorerklæring

Garuda A/S

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder for perioden fra 1. oktober 2022 til 30. september 2023

November 2023

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Indholdsfortegnelse

Sektion 1: Garuda A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Garuda A/S' kunder, som har indgået en databehandleraftale med Garuda A/S, 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.

Garuda A/S anvender underleverandørerne og underdatabehandlerne OnlineCity ApS, SolarWinds MSP og AWS SES. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Garuda 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 Garuda A/S' beskrivelse i Sektion 3 af Garuda A/S' digitale løsninger, kan kun nås, hvis de komplementerende kontroller hos kunderne er passende designet og operationelt effektive sammen med kontrollerne hos Garuda A/S. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

Garuda A/S bekræfter, at:

a) Den medfølgende beskrivelse, Sektion 3, giver en retvisende beskrivelse af, hvordan Garuda A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 1. oktober 2022 til 30. september 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Garuda 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 Garuda A/S' digitale løsningers 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 databehandleren Garuda A/S' digitale løsninger til behandling af personoplysninger foretaget i perioden fra 1. oktober 2022 til 30. september 2023

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af Garuda A/S' beskrevne digitale løsninger 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 Garuda A/S' digitale løsninger, 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 passende designet og operationelt effektive i perioden fra 1. oktober 2022 til 30. september 2023, hvis relevante kontroller hos underleverandører var operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Garuda A/S' kontroller i perioden fra 1. oktober 2022 til 30. september 2023.

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 kompetencer og beføjelser i perioden fra 1. oktober 2022 til 30. september 2023

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.

Risskov, den 17. november 2023
Garuda A/S

Rasmus Herman Hall Mortensen
Adm. direktør

Sektion 2: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. oktober 2022 til 30. september 2023

Til Garuda A/S og Garuda A/S' kunder i rollen som dataansvarlige.

Omfang

Vi har fået som opgave at afgive erklæring med høj grad af sikkerhed om a) Garuda A/S' beskrivelse i Sektion 3 af Garuda A/S' digitale løsninger i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig i perioden fra 1. oktober 2022 til 30. september 2023 og b+c) om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Garuda A/S anvender underleverandørerne og underdatabehandlerne OnlineCity ApS, SolarWinds MSP og AWS SES. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Garuda A/S' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlernes kontroller, der forudsættes i designet af Garuda A/S´ kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos Garuda A/S.

Enkelte af de kontrolmål, der er anført i Garuda A/S' beskrivelse i Sektion 3 af Garuda A/S' digitale løsninger, kan kun nås, hvis de komplementerende kontroller hos kunderne er passende designet og operationelt effektive sammen med kontrollerne hos Garuda A/S. Erklæringen omfatter ikke hensigtsmæssigheden af designet og den operationelle effektivitet af disses komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Garuda A/S' ansvar

Garuda A/S er ansvarlig for udarbejdelsen af beskrivelsen og 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 samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Grant Thorntons 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.

Grant Thornton anvender international standard om kvalitetsstyring, ISQC 1[1] , 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.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

Grant Thorntons ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Garuda A/S' beskrivelse samt om designet og den operationelle effektivitet 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 passende designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af Garuda A/S' digitale løsninger samt for kontrollernes design og operationelle effektivitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er passende designet eller ikke er operationelt effektive. 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 "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 databehandler

Garuda 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 Garuda A/S' digitale løsninger, 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 Garuda A/S' digitale løsninger, således som denne var udformet og implementeret i perioden fra 1. oktober 2022 til 30. september 2023, 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 passende designet i perioden fra 1. oktober 2022 til 30. september 2023, 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 Garuda A/S' kontroller i perioden fra 1. oktober 2022 til 30. september 2023, 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. oktober 2022 til 30. september 2023.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Sektion 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Garuda A/S' digitale løsninger, 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 17. november 2023

Grant Thornton
Godkendt Revisionspartnerselskab

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Andreas Moos
Director, CISA, CISM

Sektion 3: Garuda A/S' beskrivelse af behandlingsaktivitet for leverancen af Garuda A/S' digitale løsninger

Formålet med denne beskrivelse er at levere oplysninger til Garuda A/S' kunder og deres interessenter (herunder revisorer) om efterlevelse af indholdet af EU' s Generelle Databeskyttelsesforordning ("GDPR").

Desuden er formålet med denne beskrivelse at give oplysninger om behandlingssikkerheden, tekniske og organisatoriske foranstaltninger samt ansvar mellem dataansvarlige (vores kunder) og Garuda A/S.

Karakteren af behandlingen

Den dataansvarlige har erhvervet licens til Garuda A/S' digitale løsninger, hvor den dataansvarlige ved brug af løsningerne indtaster, uploader, importerer eller på anden vis tilføjer data, herunder personoplysninger, til løsningerne med henblik på brug, herunder til analyse og som oplæg til samtale i forbindelse med udvælgelse og udvikling af medarbejdere, samt i forbindelse med personale- og karriereplanlægning. I forbindelse med leveringen af løsningerne behandler databehandleren således personoplysninger på vegne af den dataansvarlige efter gældende regler og i overensstemmelse med indgået databehandleraftale.

Personoplysninger

Garuda A/S behandler følgende kategorier af personoplysninger. Ved brug af løsningerne er der dog mulighed for, at den dataansvarlige kan overlade behandling af alt slags data og personoplysninger til databehandleren, hvorfor databehandleren potentielt vil kunne behandle alle kategorier af personoplysninger.

Kategorier af personoplysninger:

a) Kontaktoplysninger, som personnavn, e-mailadresse, organisationstilknytning, telefonnummer

b) Brugeroplysninger, som brugernavn, nationalitet, brugerlokation og -adfærd.

c) besvarelsen af spørgeskemaet og andre sociale variabler såsom køn, alder, skoleuddannelse, praktisk uddannelse, ansvar, funktion, titel, arbejdsløshed, anciennitet.

d) evt. øvrige personoplysninger, der er nødvendige for den dataansvarliges brug af databehandlerens levering af værktøjer og services.

Garuda A/S behandler som udgangspunkt nedenstående kategorier af registrerede. Ved brug af løsningerne er der dog mulighed for, at den dataansvarlige kan overlade behandling af alt slags data og personoplysninger til databehandleren, hvorfor databehandleren potentielt vil kunne behandle personoplysninger om flere kategorier af registrerede.

Kategorier af registrerede:

e) Kandidater

f) Medarbejdere

g) Elever

h) Kursister

Instruks fra den dataansvarlige

1. Garuda A/S må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks fremgår af den indgåede databehandleraftale og er nærmere specificeret i gældende bilag A og C.
2. Garuda A/S underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.
3. Garuda A/S har sikret at 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. Garuda A/S udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.

Risikovurdering

Garuda A/S har foretaget en kortlægning over risikoen for de registreredes rettigheder, herunder en afvejning af disse risici i forhold til de forholdsregler, der er truffet for at beskytte disse rettigheder. Selve risikovurderingen består af flere dele, herunder:

- En kortlægning af alle de risici, behandlingen medfører, og en kategorisering (scoring, sandsynlighed og alvorlighed) heraf.
- En vurdering af, hvad der er passende tekniske og organisatoriske foranstaltninger til at sørge for, at forordningen overholdes, og dette kan dokumenteres.

I de risikovurderinger, som er udarbejdet Garuda A/S, er der ingen høj risiko for de registrerede på tværs af alle typer af registrerede og kategorier af personoplysninger.

Tekniske og organisatoriske kontrolforanstaltninger

Behandling af data udgør kernen af den service vi yder til vores kunder. Derfor er vores kunders tiltro og tillid til, at vi kan levere vores service på sikker og fortrolig vis også af helt afgørende betydning for vores forretningsgrundlag. Vi tager derfor databeskyttelse og GDPR meget alvorligt og har et kontinuerligt fokus på at behandle vores kunders data sikkert, herunder ved fortløbende forbedring af vores tekniske og organisatoriske sikkerhedsforanstaltninger. Følgende er en ikke udtømmende liste over vores sikkerhedsforanstaltninger, som foretages henholdsvis af Garuda A/S og/eller tilkøbt hos leverandører:

- IT-sikkerhedspolitik
- Retningslinjer for medarbejdersikkerhed
- Styring af aktiver, herunder kontrol af udlevering og returnering af aktiver ved ansættelser og fratrædelser
- Kryptografi
- Leverandørforhold og/eller tilsynsplan med underdatabehandler
- Styring af persondatassikkerhedsbrud og hændelseshåndtering
- Sikre etablering af databehandleraftaler med underdatabehandlere
- Sikre, at de krav, der pålægges i henhold til lovgivning eller af kunder via kontrakter og databehandleraftaler tilsvarende pålægges underdatabehandlere
- Kontrol og opdatering af risikovurdering, politikker og procedurer
- Løbende oplæring af medarbejderne i GDPR
- Kontrol af adgangsforhold efter arbejdsbetinger behov

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.

Når Garuda A/S gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, sikrer Garuda A/S gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår databehandleraftalen i mellem Garuda A/S og den dataansvarlige, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i databehandleraftalen og databeskyttelsesforordningen. Garuda A/S er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Garuda A/S' forpligtelser efter indgået databehandleraftalen og databeskyttelsesforordningen.

Underdatabehandleraftale(r) og eventuelle senere ændringer hertil er tilgængelig på hjemmesiderne tilhørende Garuda A/S, hvorved den dataansvarlige herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, gøres ikke tilgængeligt for den dataansvarlige.

Overførsel af personoplysninger

Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

Uden dokumenteret instruks fra den dataansvarlige kan Garuda A/S således ikke inden for rammerne af databehandleraftalen:

a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
c. behandle personoplysningerne i et tredjeland

Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, er angivet i databehandleraftalens bilag C, C.6.

De registreredes rettigheder

Garuda A/S bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at Garuda A/S så vidt muligt bistår den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

d. oplysningspligten ved indsamling af personoplysninger hos den registrerede
e. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede f. indsigtsretten
g. retten til berigtigelse
h. retten til sletning (”retten til at blive glemt”)
i. retten til begrænsning af behandling
j. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
k. retten til dataportabilitet
l. retten til indsigelse
m. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

Håndtering af persondatasikkerhedsbrud

Garuda A/S underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Underretningen til den dataansvarlige sker om muligt senest 24 timer efter, at Garuda A/S er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

I overensstemmelse indgået databehandleraftale bistår Garuda A/S den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Garuda A/S skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

I databehandleraftalens bilag C findes nærmere angivet information, som Garuda A/S tilvejebringer i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

Fortegnelse

Garuda A/S fører en fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.

Ledelsen hos Garuda A/S har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige indeholder:

- Navn og kontaktoplysninger på databehandleren, de dataansvarlige, den dataansvarliges eventuelle repræsentanter og databeskyttelsesrådgivere
- De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige
- Når det er relevant, oplysninger om overførsel til et tredjeland eller en international organisation samt dokumentation for passende garantier
- Hvis det er muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger. Der henvises i øvrigt til Sektion 4, hvor de konkrete kontrolaktiviteter er beskrevet.

Væsentlige ændringer i perioden

Der har ikke været væsentlige ændringer i perioden.

Justering af kontrolmål/kontroller jf. FSR's erklæringsskabelon

Kontrol jf. FSR's erklærings-skabelon	Justering	Begrundelse
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.	Kontrolaktivitet er taget ud af scope.	Der anvendes ikke personoplysninger i udvikling eller test miljøer, hvorfor pseudonymiseret eller anonymiseret heraf ikke er relevant.
B.11: De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Tilpasning af kontrolaktiviteten.	Der foretages løbende sårbarhedsscanninger, men ikke penetrationstests, hvorfor denne del tages ud.
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.	Kontrolaktivitet er taget ud af scope.	Der er implementeret alternative tekniske sikkerhedsforanstaltninger til to-faktor autentifikation, som vurderes tilstrækkelige, hvorfor kontrollen ikke er implementeret.
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.	Kontrolaktivitet er taget ud af scope.	Denne kontrol håndteres af vores underleverandør, som i erklæringen håndteres efter partielmetoden.

Komplementerende kontroller hos de dataansvarlige

De dataansvarlige har følgende forpligtelser:

- at sikre sig, at personoplysningerne er ajourførte
- at sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering
- at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen
- at den dataansvarliges brugere er ajourførte og således slette, opdatere eller deaktivere brugere løbende
- at sikre, at den fornødne hjemmel til behandling er til stede
- at efterleve oplysningspligten til de registrerede om udøvelsen af deres rettigheder
- at kontrollere identiteten af de registrerede, der ønsker at udøve deres rettigheder. Løsningen understøtter ligeledes den dataansvarliges ansvar ved anmodninger fra registrerede, som den dataansvarlige således selv vil kunne opfylde, dog således at Garuda A/S anerkender sin pligt til at bistå ved anmodninger herom.
- at ved valg af løsningen er den dataansvarlig bekendt med funktionen for sletning af data. Løsningen understøtter og forudsætter således, at den dataansvarlig selv skal udøve sletning eller tilbagetrækning af data, herunder tilføjet personoplysninger. Den dataansvarlige kan ved anmodning herom lade Garuda A/S forestå dette som nærmere beskrevet i indgået databehandleraftale.

Sektion 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. oktober 2022 til 30. september 2023.

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

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

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

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Garuda 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.
Genudførelse 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, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Ikke en del af ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Ikke en del af ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Ikke en del af ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Ikke en del af ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Ikke en del af ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Ikke en del af ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Ikke en del af ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Ikke en del af ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**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	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Ikke en del af ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Ikke en del af ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	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.	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. 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. 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.	Vi er blevet oplyst, at der ikke er identificeret instruks, som vurderes at være i strid med lovgivning, hvorfor vi ikke har testet kontrollens effektivitet. 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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling 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, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres. Vi har inspiceret, at procedurerne er opdaterede.	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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Vi har stikprøvevis inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Vi har stikprøvevis inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Vi har inspiceret, at antivirus software er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Vi har inspiceret, at der er opsat en firewall samt at denne er opdateret.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Vi har inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugernes adgang til personoplysninger. Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Vi har inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Vi har inspiceret, at brugernes adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Vi har stikprøvevis inspiceret, at der er sket opfølgning på alarmer, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	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. Vi har inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i erklæringsperioden. Vi har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Ingen afvigelser konstateret.

B.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold:
	
	• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
	• Sikkerhedshændelser omfattende:
	  ○ Ændringer i logopsætninger, herunder deaktivering af logning
	  ○ Ændringer i systemrettigheder til brugere
	  ○ Fejlede forsøg på log-on til systemer, databaser og netværk
	
	Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.
		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.
		
		Vi har stikprøvevis inspiceret, at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser.
		
		Vi har forespurgt til opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.
			Vi er blevet oplyst, at der ikke foretages løbende dokumenteret opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder, men at kontrollen udføres ad hoc i tilfælde af anomalier.
			
			Ingen yderligere afvigelser konstateret.

B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Vi har inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger. Vi har stikprøvevis inspiceret, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
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 til systemer, databaser og netværk er håndteret jævnfør proceduren herfor.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	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. Vi har inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons 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 informationsikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationsikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret dokumentation for ledelsens vurdering af, at informationsikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Vi har stikprøvevis inspiceret at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikkens 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 forespurgt til nyansættelser i erklæringsperioden.	Vi er blevet oplyst, at der ikke har været nyansættelser i erklæringsperioden, hvorfor vi ikke har testet kontrollens effektivitet. Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der foreligger formaliserede procedurer, som sikrer, at nyansatte medarbejdere underskriver en fortrolighedsaftale. Vi har forespurgt til nyansættelser i erklæringsperioden.	Vi er blevet oplyst, at der ikke har været nyansættelser i erklæringsperioden, hvorfor vi ikke har testet kontrollens effektivitet. 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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Vi har stikprøvevis inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget for fratrådte medarbejdere i erklæringsperioden.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der er formel procedure for fratrædelse, der sikrer, at fratrådte medarbejdere bliver orienteret omkring fortroligheden i forbindelse med fratrædelse. Vi har stikprøvevis forespurgt til, om fratrådte medarbejdere er blevet gjort opmærksom på deres fortrolighedspligt.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awareness træning af databehandlerens medarbejdere i relation til IT-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne omfattende generel IT-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at relevante medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den tilbudte awarenesstræning.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har stikprøvevis inspiceret, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Vi har stikprøvevis inspiceret, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen afvigelser konstateret.
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 det ikke er i modstrid med anden lovgivning.	Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har stikprøvevis inspiceret, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført for ophørte databehandlinger i erklæringsperioden.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons 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, om procedurerne er opdaterede.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. 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.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har stikprøvevis inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
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 inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Vi har forespurgt til ændringer af underdatabehandlere i perioden.	Vi er blevet oplyst, at der ikke har været ændringer i anvendelse af underdatabehandlere i erklæringsperioden, hvorfor vi ikke har testet kontrollens effektivitet. 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.

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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
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 inspiceret dokumentation for, at der er foretaget en 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, tredjelands 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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
G.1	Der foreligger skriftlige politikker, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om politikkerne skal opdateres.	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. Vi har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer i erklæringsperioden.	Vi er blevet informeret om, at der ikke er modtaget instruks fra dataansvarlige om overførsel af personoplysninger til tredjelande eller internationale organisationer i erklæringsperioden, hvorfor vi ikke har testet kontrollens effektivitet. 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.	Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer i erklæringsperioden.	Vi er blevet informeret om, at der ikke er modtaget instruks fra dataansvarlige om overførsel af personoplysninger til tredjelande eller internationale organisationer i erklæringsperioden, hvorfor vi ikke har testet kontrollens effektivitet. Ingen 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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har inspiceret, at der foreligger dokumentation for at anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.	Ingen afvigelser 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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	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.	*Garuda A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Vi har inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Vi har inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har forespurgt, om der er konstateret brud på persondatasikkerheden i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet kontrollens effektivitet. Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har inspiceret proceduren for sikkerhedsbrud, og påset, at den understøtter bistand til den dataansvarlige i forbindelse med brud. Vi har forespurgt, om der er konstateret brud på persondatasikkerheden i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet kontrollens effektivitet. Ingen afvigelser konstateret.

PENNEO

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

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

Rasmus Herman Hall Mortensen
Underskriver 1
Serienummer: 0e8348cc-1806-4526-a324-e7a934210f80
IP: 62.66.xxx.xxx
2023-11-17 11:14:25 UTC

Mit ID

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 147.78.xxx.xxx
2023-11-17 11:30:40 UTC

Mit ID

Jacob Helly Juell-Hansen
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serienummer: f17041a5-2020-4c05-998a-fb15e6cdd8f6
IP: 62.243.xxx.xxx
2023-11-18 16:06:11 UTC

Mit ID

Penneo dokumentnøgle: K60V4-1BTZT-HYZLO-KG43W-12TEE-G4I21