

Revisorerklæring

Mileage Book A/S

ISAE 3000 type 2 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder der har anvendt IT-systemet Mileage Book i perioden fra 1. juli 2024 til 30. juni 2025

Marts 2026

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Indholdsfortegnelse

Sektion 1:	Mileage Book A/S' udtalelse	1
Sektion 2:	Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. juli 2024 til 30. juni 2025.....	3
Sektion 3:	Mileage Book A/S' beskrivelse af behandlingsaktivitet for leverancen af IT-systemet Mileage Book.....	5
Sektion 4:	Kontrolmål, udførte kontroller, test og resultater heraf	8

Sektion 1: Mileage Book A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Mileage Book A/S' kunder, som har indgået en databehandler-aftale med Mileage Book 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.

Mileage Book A/S anvender underdatabehandlere Microsoft, Brevo og Twilio Inc. (SendGrid). Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Mileage Book A/S' underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlers kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underdatabehandlere.

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

Mileage Book A/S bekræfter, at:

- a) Den medfølgende beskrivelse, Sektion 3, giver en retvisende beskrivelse af, hvordan Mileage Book A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 1. juli 2024 til 30. juni 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
 - (i) Redegør for, hvordan Mileage Book A/S' processer og kontroller relateret til databeskyttelse var designet 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 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 Mileage Book A/S' afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål der er anført i beskrivelsen, er identificeret i beskrivelsen
 - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

- (ii) Indeholder relevante oplysninger om ændringer ved databehandlerens IT-system Mileage Book til behandling af personoplysninger foretaget i perioden fra 1. juli 2024 til 30. juni 2025
 - (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne IT-system Mileage Book 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 IT-systemet Mileage Book 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. juli 2024 til 30. juni 2025, hvis relevante kontroller hos underdatabehandlere var operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Mileage Book A/S' kontroller i perioden fra 1. juli 2024 til 30. juni 2025.
- Kriterierne anvendt for at give denne udtalelse var, at:
- (i) de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
 - (ii) de identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og
 - (iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. juli 2024 til 30. juni 2025
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandleretik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Silkeborg, den 9. marts 2026
Mileage Book A/S

Carsten Guldhammer
Direktør

Sektion 2: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandlersaftaler med kunder i perioden fra 1. juli 2024 til 30. juni 2025

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

Omfang

Vi har fået som opgave at afgive erklæring med høj grad af sikkerhed om Mileage Book A/S' beskrivelse i Sektion 3 af IT-systemet Mileage Book i henhold til databehandlersaftaler med deres kunder i perioden fra 1. juli 2024 til 30. juni 2025 og om design og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Mileage Book A/S anvender underdatabehandlere Microsoft, Brevo og Twilio Inc. (SendGrid). Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Mileage Book A/S' underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlernes kontroller, der forudsættes i designet af Mileage Book A/S' kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos Mileage Book A/S.

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

Vores konklusion udtrykkes med høj grad af sikkerhed.

Mileage Book A/S' ansvar

Mileage Book 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 designet og implementeringen af operationelt effektive 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 on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Mileage Book 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 IT-systemet Mileage Book samt for kontrollerens 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

Mileage Book 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 IT-system Mileage Book, 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 Mileage Book A/S' IT-system Mileage Book, således som denne var designet og implementeret i perioden fra 1. juli 2024 til 30. juni 2025, i alle væsentlige henseender er tilfredsstillende præsenteret, og
- b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet og implementeret i perioden fra 1. juli 2024 til 30. juni 2025, 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. juli 2024 til 30. juni 2025.

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 Mileage Book A/S' IT-system Mileage Book 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 9. marts 2026

Grant Thornton

Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
Statsautoriseret revisor

Andreas Moos
Partner, CISA, CISM

Sektion 3: Mileage Book A/S' beskrivelse af behandlingsaktivitet for leverancen af IT-systemet Mileage Book

1. Systembeskrivelse

Formålet med databehandlerens behandling af personoplysninger er at levere IT-systemet Mileage Book og opfylde den dataansvarliges behov for registrering, håndtering og administration af nuværende samt tidligere ansattes kørselsregnskab, puljebiler, tidsregistrering, udlæg og firmakorttransaktioner samt flådestyring af den dataansvarliges køretøjer, herunder forsikringshåndtering af skader – alt sammen på en måde, der samtidig opfylder persondataforordningens krav til sikkerhed.

1.1 Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om behandling af almindelige persondata som knytter sig til Skattekravene for registrering og håndtering af kørselsregnskaber og udlæg. Desuden behandles også GPS-koordinater for brugerne af systemet.

1.2. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen omfatter nedenfor kategorier om de registrerede.

1.2.1. Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6):

Flådestyring:

- Navn
- E-mailadresse
- Besøgte adresser
- GPS-koordinater

Puljebiler:

- Navn
- Privatadresse
- E-mailadresse
- Besøgte adresser
- GPS-koordinater

Kørselsregnskab:

- Navn
- Privatadresse
- Registreringsnummer
- E-mailadresse
- Besøgte adresser
- GPS-koordinater

Udlægshåndtering

- Navn
- E-mailadresse

Forsikringshåndtering af skader på biler:

- Skadelidte og skadevolder:
 - Navn, telefonnummer, privatadresse, medlemskab af forsikringsselskab og registreringsnummer
- Vidner
 - Navn, telefonnummer og privatadresse
- Oplysninger om hændelse, herunder
 - Beskrivelse af hændelsen
 - Tidspunkt for hændelsen
 - Adresse for hændelsen

Tidsregistrering:

- Navn
- E-mailadresse
- Arbejdstid

1.3 Behandlinger omfatter følgende kategorier af registrerede

Behandlingen omfatter nedenfor nævnte kategorier af registrerede:

- Den dataansvarliges nuværende og tidligere medarbejdere

1.4 Praktiske tiltag

Databehandlerens ansatte er orienteret i de organisatoriske sikkerhedsforanstaltninger. Herunder har de læst og underskrevet medarbejderinstruks omkring beskyttelse af persondata, personoplysninger omkring salg/marketing, virksomhedens generelle sikkerhedsrutiner, brug af hjemmearbejdsplads samt brud på datasikkerheden.

Medarbejderne er vejledt i databehandlerens overordnede krav til it-sikkerheden. Et led heri er at have gennemlæst og underskrevet informations- og it-sikkerhedspolitikken.

Databehandlerens medarbejdere, der har kundekontakt, er undervist i dataansvarliges brugeres rettigheder i forhold til databehandlerens behandling af personoplysninger efter databeskyttelsesforordningen: indsigts- og rettel-sesret, ret til sletning, ret til begrænsning af behandling af personoplysninger, ret til indsigelse, ret til dataportabilitet.

1.5 Risikovurdering

Databehandler har kortlagt virksomhedens samlede systemer i en risikorapport. Her er systemerne beskrevet og risiko- og konsekvensvurderet med en score ud fra parametrene: Fortrolighed, Tilgængelighed og Integritet.

Ingen af virksomhedens systemer og aktiver er vurderet i høj risiko. Langt størstedelen af systemerne er vurderet med risikoen Lav. Enkelte systemer har fået risikovurderingen Middel.

Organisatoriske sikkerhedsforanstaltninger angiver proceduren ved brud på datasikkerheden.

1.6 Kontrolforanstaltninger

1.6.1. Behandlinger – instrukser

Processer og procedurer er udarbejdet så de stemmer overens med databehandlertaften.

Data er identificeret og kategoriseret for hvert anvendt IT-system i en fortegnelse. Fortegnelsen danner overblik over hvert systems behandling af personoplysninger som:

- Formål og behandling (hvorfor opbevares disse data?)
- Hjemmel (med hvilken ret behandler du disse persondata?)
- Hvilke interne brugere eller brugergrupper har adgang til disse data?
- Regler for sletning af persondata

1.6.2. Kontrol og proceduregennemgang

Gennemgang af procedurer håndteres ved hjælp af faste frekvenser, hvor hver procedure har faste frekvenser for udførelse samt kontrol med procedurerne.

Frekvenserne sikrer ligeledes, at der bliver fulgt op på implementerede procedurer og standarder. Proceduregennemgang og procedurekontrol er skemalagt for perioden og supporteret af notifikationer.

1.6.3. Procedurer – Adgangsstyring

Virksomhedens adgangsstyring er beskrevet i Informationssikkerhedspolitik (Kontrol af adgang til IT) og såvel brug som administration bliver styret fra centralt hold af Mileage Books CTO.

Registrering af medarbejdernes adgangsrettigheder sker i forbindelse med nyansættelser, opsigelser, ved implementering af nye systemer og ved ændringer i arbejdsfunktioner og -opgaver.

1.6.4. Procedurer – Risikostyring

Der bliver foretaget en årlig risikovurdering med udgangspunkt i risikoen for den registrerede, for de enkelte systemer og aktiver. Systemerne vurderes i kategorierne low, medium og high.

1.6.5. Procedurer – Udvikling og anskaffelser

Udviklingsprocessen i Mileage Books udviklingsafdeling foregår med agil fremgangsmåde med udgangspunkt i principperne i SCRUM-metoden. Der bliver arbejdet i 14 dages sprint ud fra et veldefineret roadmap. Udviklingsopgaverne bliver prioriteret og styret ud fra et Kanban board.

AI kode fra Mileage Books udviklingsafdeling gennemgår både code review og test inden release af ny funktionalitet. Samtidig er appen underlagt løbende review hos Apples App Store og Google Play Store.

1.6.6. Procedurer – Håndtering af persondataanmodninger

Håndtering af persondataanmodninger følger virksomhedens Procedure for håndtering af de registreredes rettigheder. Det vil sige, at enhver henvendelse omkring persondatarettigheder skal gå gennem virksomhedens supportafdeling. Person, der søger indsigt i, ændring af eller sletning af persondata indgår i procedure tilpasset hver enkelt rettighed og modtager standardiserede besvarelser i henhold til den enkelte rettighed.

1.6.7. Procedurer – Sikkerhedshændelser

Der er udarbejdet en procedure i tilfælde af et brud på persondatasikkerheden i virksomheden. Proceduren er beskrevet i virksomhedens Procedure for sikkerhedshændelser. Sikkerhedshændelser logges og der føres samtidig fast kontrol med proceduren for sikkerhedshændelser.

1.6.8. Underleverandører

Mileage Books underdatabehandlere er listet i databehandleraftalen, samt på Mileage Books website.

Der føres tilsyn med samtlige underdatabehandlere. Mileage Books tilsyn med underdatabehandlere føres på baggrund af tilsynskoncepter efter Datatilsynets vejledning om tilsyn med databehandlere. I overensstemmelse med Datatilsynets dertilhørende vejledende pointskala, sikrer Mileage Book, at de valgte tilsynskoncepter er passende med hvor risikofyldt behandlingen hos underdatabehandlerne er.

1.6.9 Ændringer i perioden

Ingen væsentlige ændringer i perioden.

1.6.10 Komplementerende kontroller hos de dataansvarlige

De dataansvarlige har følgende forpligtelser:

- At sikre, at personoplysningerne er ajourførte
- At sikre, at den fornødne hjemmel til behandling er til stede
- At efterleve oplysningspligten til de registrerede om udøvelsen af deres rettigheder
- At sikre adgangs begrænsning, således at alene medarbejdere med et arbejdsbetinget behov herfor kan administrere brugere

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. juli 2024 til 30. juni 2025.

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Mileage Book A/S' underdatabehandlere.

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

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

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Mileage Book A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af kontrollens udførelse.
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 operationelt effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Derudover foretages der stikprøvevis test af kontrollernes operationelle effektivitet i revisionsperioden.
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 27001/2:2013. Artikler og punkter markeret med fed angiver primære områder.

Kontrol-aktivitet	GDPR-artikler	ISO 27701	ISO 27001/2:2013
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	<i>Nyt område ift. ISO 27001/2</i>
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	<i>Nyt område ift. ISO 27001/2</i>
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	<i>Nyt område ift. ISO 27001/2</i>
D.1	6, 11, 13, 14 , 32	7.4.5, 7.4.7 , 7.4.4	<i>Nyt område ift. ISO 27001/2</i>
D.2	6, 11, 13, 14, 32	7.4.5, 7.4.7 , 7.4.4	<i>Nyt område ift. ISO 27001/2</i>
D.3	13, 14	7.4.7 , 7.4.4	<i>Nyt område ift. ISO 27001/2</i>
E.1	13, 14, 28 , 30	8.4.2, 7.4.7, 7.4.8	<i>Nyt område ift. ISO 27001/2</i>
E.2	13, 14, 28 , 30	8.4.2, 7.4.7, 7.4.8	<i>Nyt område ift. ISO 27001/2</i>
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	<i>Nyt område ift. ISO 27001/2</i>
H.2	12, 13, 14 , 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>Nyt område ift. ISO 27001/2</i>
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 databehandlersaftale.

Nr.	Mileage Book 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 procedurene 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 procedurene indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Vi har inspiceret, at procedurene er opdateret.	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 informeret om, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. 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.	Mileage Book 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 procedurer 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 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.	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. Vi har inspiceret, at der anvendes Microsoft Intune til at overvåge enheder (Microsoft Defender). Der er dog ikke opsat AV Policies.	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.	Mileage Book 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 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 personoplysninger, er etableret systemovervågning med alarmering. Vi har forespurgt, om der er sket opfølgning på alarmer.	Vi er blevet informeret om, at der i revisionsperioden, ikke har været alarmer der har krævet opfølgning. Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet.	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.	Mileage Book A/S' kontrolaktivitet	Grant Thorntons udførte test	Resultat af test
B.9	Der er etableret logning i systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl.	Vi har inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Vi har inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Vi har inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning. 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.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har stikprøvevis inspiceret, at personoplysninger er pseudonymiseret eller anonymiseret i udviklings- og testdatabaser. Vi har stikprøvevis inspiceret udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Vi har stikprøvevis inspiceret at ændringer til systemer, databaser og netværk er håndteret jævnfør proceduren herfor.	Vi har inspiceret, at funktionsadskillelse ikke er dokumenteret ved idriftsættelse af to (2) ud af femogtyve (25) implementerede ændringer. Ingen yderligere 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.	Mileage Book A/S' kontrolaktivitet	Grant Thorntons udførte test	Resultat af test
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.	Der foreligger ikke dokumentation for at tildeling af adgange er foretaget med relevant ledelsesgodkendelse. Ingen yderligere afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører højrisiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	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.	Mileage Book 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 informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	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.	Mileage Book A/S' kontrolaktivitet	Grant Thorntons udførte test	Resultat af test
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Vi har stikprøvevis inspiceret at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikens krav til sikringsforanstaltninger og behandlingssikkerheden.	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 stikprøvevis inspiceret, at nyansatte medarbejdere i erklæringsperioden har underskrevet en fortrolighedsaftale. Vi har stikprøvevis inspiceret at nyansatte medarbejdere i erklæringsperioden er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejders 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 stikprøvevis inspiceret, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt for fratrådte medarbejdere i erklæringsperioden.	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.	Mileage Book A/S' kontrolaktivitet	Grant Thorntons udførte test	Resultat af test
C.7	Der gennemføres løbende awarenessstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awarenessstræning.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	Vi har inspiceret dokumentation for, at databehandleren har vurderet behov for en databeskyttelsesrådgiver i perioden.	Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige. Ledelsen 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 foretages løbende – og mindst en gang årligt – vurdering af, om fortegnelsen skal opdateres.	Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	Mileage Book 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 opdateret.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Vi har stikprøvevis inspiceret, at der er aftalt opbevaringsperioder og 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 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.	Vi har ikke modtaget dokumentation der understøtter, at en skriftlig bekræftelse er tilsendt til en (1) ud af seks (6) ophørte databehandleraftaler ved sletning af data. Ingen yderligere 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.	Mileage Book 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, at procedurerne er opdateret.	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.	Vi har inspiceret at lokalitet for databehandling ikke kan specificeres for Twilio Inc. (SendGrid) Ingen yderligere 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.	Mileage Book 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 opdateret.	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 om der har været ændringer af underdatabehandlere i perioden.	Vi er blevet informeret om, at der, i erklæringsperioden, ikke har været ændringer i anvendelse af underdatabehandlere. 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.	Mileage Book 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, hvis der er noget væsentligt at rapportere.	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, tredjelandes overførselsgrundlag og lignende. Vi har forespurgt om opfølgning hos underdatabehandlere meddeles den dataansvarlige hvis der er væsentlige bemærkninger, således at denne kan tilrettelægge eventuelt tilsyn.	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.	Mileage Book A/S' kontrolaktivitet	Grant Thorntons udførte test	Resultat af test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne 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 inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.	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 inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Vi har inspiceret, at procedurerne er opdateret. Vi har inspiceret, at der er foretaget en kontrol af overførselsgrundlag.	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.	Mileage Book 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 opdateret.	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 de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer. Vi har forespurgt, om databehandleren har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder.	Vi er blevet informeret om, at databehandleren ikke har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder. Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	Mileage Book 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 procedurene 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.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awarenessstræning 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 unødigt 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 har været persondatassikkerhedsbrud i perioden.	Vi er blevet informeret om, at der ikke har været nogen persondatasikkerhedsbrud i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	Mileage Book A/S' kontrolaktivitet	Grant Thorntons udførte test	Resultat af test
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, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Vi har inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.

PENNEO

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

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

Carsten Guldhammer Skjerbæk

Underskriver 1

Serienummer: a53c0bc1-7d09-4beb-8a73-da070c93ed13

IP: 85.218.xxx.xxx

2026-03-09 14:43:49 UTC



Andreas Moos

Grant Thornton, Godkendt Revisionspartnerselskab CVR:
34209936

Underskriver 2

Serienummer: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035

IP: 87.52.xxx.xxx

2026-03-09 15:20:13 UTC



Kristian Randløv Lydolph

Underskriver 3

Serienummer: 7b9e0bc5-648f-4c07-87a8-debb5e403de6

IP: 62.243.xxx.xxx

2026-03-09 17:26:03 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskriveres digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.