AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF SUPPORT-DRIFTSOPGAVER AF APPLIKATIONEN RMG C3 OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

RM-Group A/S

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF SUPPORT-DRIFTSOPGAVER AF APPLIKATIONEN RMG C3 OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i RM-Group A/S
RM-Group A/S kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af RM-Group A/S (databehandleren) for hele perioden 1. januar til 31. december 2023 udarbejdede beskrivelse i sektion 3 af support-driftsopgaver af applikationen RMG C3 og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i 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.

BDO Statsautoriseret revisionsaktieselskab 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 databehandlerens beskrivelse samt om udformningen og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet 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 kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

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

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af support-driftsopgaver af applikationen RMG C3, som hver enkelt dataansvarlig måtte anse for vigtigt 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 den operationelle effektivitet af kontroller 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 databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af support-driftsopgaver af applikationen RMG C3 og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret i hele perioden 1. januar til 31. december 2023, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. januar til 31. december 2023, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. januar til 31. december 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens support-driftsopgaver af applikationen RMG C3, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 24. april 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. RM-GROUP A/S UDTALELSE

RM-Group A/S varetager behandling af personoplysninger i forbindelse med support-driftsopgaver af applikationen RMG C3 for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt support-driftsopgaver af applikationen RMG C3, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

RM-Group A/S anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

RM-Group A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af support-driftsopgaver af applikationen RMG C3 og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden 1. januar til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for support-driftsopgaver af applikationen RMG C3, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at 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 underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger 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.
    - De kontroller, som vi med henvisning til afgrænsningen af support-driftsopgaver af applikationen RMG C3 har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Indeholder relevante oplysninger om ændringer i support-driftsopgaver af applikationen RMG C3 og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden 1. januar til 31. december 2023.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af support-driftsopgaver af applikationen RMG C3 og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved support-driftsopgaver af applikationen RMG C3, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

RM-Group A/S bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. januar til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. 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.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden 1. januar til 31. december 2023.

RM-Group A/S bekræfter, at der er implementeret og opretholdt passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Allerød, den 24. April 2024

RM-Group A/S

Per Bruus
Administrerende direktør

3. RM-GROUP A/S BESKRIVELSE AF SUPPORT-DRIFTSOPGAVER AF APPLIKATIONEN RMG C3

RM-GROUP A/S

RM-Group A/S er en af de førende udbydere af operationelle Risk Managementydelser i Danmark, og de har potentiale til at udvide denne position til de nære markeder.

Selskabets aktiviteter omfatter udarbejdelse af forskellige Risk Management værktøjer til brug for implementering af operationelle Risk Management programmer. Derudover risikobegrænsende rådgivning, kurser og uddannelse.

RM-Group A/S har markedsfokus på virksomheder – offentlige som private – der har et produktions- og driftsmæssig set-up, hvor styring af risici – i bred forstand - er en af de afgørende elementer i virksomhedens samlede resultat.

RMG C3 og behandling af personoplysninger
RM-Group A/S leverer C3 som en Software-as-a-Service (SaaS) løsning i henhold til kontrakt med private virksomheder og kommuner.

C3 udvikles i Danmark på kontoret i Allerød, men løsningen afvikles dels på hosting-center i Skanderborg, dels i skyen på Google Cloud.

Der benyttes andre underdatabehandlere til afsendelse af e-mails og SMS-beskeder samt afholdelse af telekonferencer.

I forbindelse med support-driftsopgaver af applikationen RMG C3 kan visse medarbejdere i RM-Group A/S tilgå personlige oplysninger, som RM-Group A/S ' kunder lægger ind i RMG C3. Supportopgaver dækker typisk fejlretning og assistance til kunder.

STYRING AF PERSONDATASIKKERHED

RM-Group A/S har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandleren i henhold til Databeskyttelsesforordningen og Databeskyttelseslovgiven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformede i henhold til risikovurderinger, og de implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttede a it-systemer.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er strukturerede i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter:

DATABEHANDLERAFTALEN	KONTROLOMRÅDE	Artikel
Kontrolmål A: Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.	• Indgåelse af databehandleraftale med den dataansvarlige • Instruks for behandling af personoplysninger • Efterlevelse af instruks for behandling af personoplysninger	• Artikel 28, stk. 3 • Artikel 28, stk. 3, litra a • Artikel 29 • Artikel 32, stk. 4 • Artikel 28, stk. 10

DATABEHANDLERAFTALEN	KONTROLOMRÅDE	Artikel
	• Underretning af den dataansvarlige ved ulovlig instruks	• Artikel 28, stk. 3, litra h
Kontrolområde B: Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Risikovurdering • Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse • Fysisk adgangskontrol • Logisk adgangssikkerhed, herunder autorisation og adgangskontrol: • Fjernarbejdspladser og fjernadgang til systemer og data • Kryptering af personoplysninger • Firewall • Netværkssikkerhed • Antivirusprogram • Sårbarhedsscanning • Sikkerhedskopiering og retablering af data • Vedligeholdelse af systemsoftware • Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger • Overvågning • Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger • Udvikling og vedligeholdelse af systemer • Informationssikkerhed i udvikling og ændringer • Adskillelse af udviklings-, test- og produktionsmiljø • Personoplysninger i udviklings- og testmiljø • Supportopgaver	• Artikel 28, stk. 3, litra c • Artikel 25
Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.	• Informationssikkerhedspolitik • Gennemgang af informationssikkerhedspolitik • Organisering af informationssikkerhed • Rekruttering af medarbejdere • Fratrædelse af medarbejdere • Uddannelse og instruktion af medarbejdere, der behandler personoplysninger • Tavsheds- og fortrolighedsaftale meKd medarbejdere • Bistand til den dataansvarlige i forhold til behandlingssikkerhed og konsekvensanalyser • Bistand til den dataansvarlige i forhold til revision og inspektion • Fortegnelse over kategorier af behandlingsaktiviteter • Opbevaring af fortegnelsen • Datatilsynets adgang til fortegnelsen	• Artikel 28, stk. 1 • Artikel 28, stk. 3, litra b • Artikel 28, stk. 3, litra f • Artikel 28, stk. 3, litra h • Artikel 30, stk. 2, 3 og 4
Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.	• Sletning af personoplysninger • Tilbagelevering af personoplysninger	• Artikel 28, stk. 3, litra g
Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer	• Opbevaring af personoplysninger	• Artikel 28, stk. 3, litra c

DATABEHANDLERAFTALEN	KONTROLOMRÅDE	Artikel
personoplysninger i overensstemmelse med aftalen med den dataansvarlige.		
Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikker-hed.	• Underdatabehandleraftaler og instruks • Godkendelse af underdatabehandlere • Ændringer i godkendte underdatabehandlere • Oversigt over godkendte underdatabehandlere • Tilsyn med underdatabehandlere	• Artikel 28, stk. 2 og 4
Kontrolmål G Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag	• Overførsel af personoplysninger til tredjelande	• Artikel 44 - 49
Kontrolmål H Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.	• Bistand til den dataansvarlige i forhold til de registreredes rettigheder	• Artikel 28, stk. 3, litra e
Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.	• Underretning om brud på persondatasikkerheden • Identifikation og registrering af brud på persondatasikkerheden • Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden	• Artikel 33, stk. 2 • Artikel 28, stk. 3, litra f

RISIKOVURDERING

Ledelsen er ansvarlig for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som RM-Group A/S til enhver tid står over for, således at indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

Der foretages en løbende vurdering af, hvilket sikkerhedsniveau, der er passende. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitterede, opbevarede eller på anden måde behandlede.

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller udføres der en gang årligt en risikovurdering. Risikovurderingen belyser sandsynligheden for og konsekven-

serne af hændelser, der kan true persondatasikkerheden, og dermed fysiske personers rettigheder og frihedsrettigheder, herunder tilfældige, forsætlige og uforsætlige hændelser. Risikovurderingen tager hensyn til det aktuelle tekniske niveau og implementeringsomkostningerne.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller vedrører alle processer og systemer, som behandler personoplysninger på vegne af den dataansvarlige. De i kontrolskemaet anførte kontrolmål og kontrolaktiviteter er en integreret del af den efterfølgende beskrivelse.

- Der benyttes stærk kryptering af oplysninger, når de sendes over offentlige netværk.
- Der er implementeret firewalls og kontroller til sikring mod uvedkommendes adgang til systemer.
- Oplysninger krypteres i en database.
- Der tages back-up af data og systemer periodisk.
- Der er implementeret adgangskontroller, der sikrer, at kunders data er adskilt fra hinanden.
- Den enkelte brugers adgang er baseret på arbejdsbetinget behov.
- Der er logning af handlinger foretaget af brugere og privilegerede brugere.
- Det er ikke muligt for brugere at ændre i loggen.
- Personlige oplysninger som cpr-nr. anonymiseres i RMG C3. Hvis en bruger ønsker at se hele cpr. nr. bliver dette logget.
- Der indhentes ISAE 3402 erklæring fra underleverandør.
- Der er udarbejdet proces for håndtering af hændelser.
- Der er implementeret to-faktor godkendelse ved login.
- Der er kontroller, der forhindrer uautoriserede forsøg på login.
- RMG C3 understøtter 'Single Sign-on', såfremt kunden ønsker det.
- Alle systemer opdateres, jf. proces.
- Alle opdateringer til RMG C3 og underliggende systemer testes og godkendes inden idriftsættelse.
- Al systemudvikling sker i henhold til internationale standarder (OWASP)
- Der er fysisk sikring af udstyr og lokaler.

Databehandleraftale

RM-Group har indført politikker og procedurer for indgåelse af databehandlingsaftaler, der sikrer at RM-Group i tilknytning til kundekontrakten indgår en databehandleraftale.

RM-Group anvender en skabelon til databehandleraftaler i tilfælde af at kunden ikke ønsker at benytte sin egen.

Under alle omstændigheder sikres at skabelonen er i overensstemmelse med de tjenester der leveres, herunder information om brugen af underdatabehandlere. Databehandleraftalerne opbevares elektronisk.

Instruks for behandling af personoplysninger

RM-Group A/S har indført politikker og procedurer, der sikrer, at RM-Group A/S handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske, herunder hvem der hos den dataansvarlige kan give bindende instruks til RM-Group A/S. Proceduren sikrer desuden, at RM-Group A/S informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering

RM-Group A/S har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom.

Beredskabsplaner
RM-Group A/S har etableret beredskabsplaner, således at RM-Group A/S rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. RM-Group A/S har etableret et kriseberedskab, der træder i kraft i disse tilfælde. Organisering af kriseberedskabsgruppe er etableret, og der er indført retningslinjer for aktivering af kriseberedskabet.

RM-Group A/S har udformet detaljerede beredskabsplaner og planer for retablering af systemer og data, der blandt andet sikrer personuafhængighed i forbindelse med aktivering af beredskabet og retableringen. Planerne er i kopi opbevaret sikret uden for RM-Group A/S ' it-systemer. Planerne afprøves og revideres løbende i forbindelse med ændringer i systemer mv.

Fysisk adgangskontrol
RM-Group A/S har indført procedurer, der sikrer, at lokaler er beskyttede mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne. Kunder og leverandører ledsages altid.

Logisk adgangssikkerhed
RM-Group A/S har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Fjernarbejdspladser og fjernadgang til systemer og data
RM-Group A/S har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for RM group A/S' lokaler og fjernadgang til systemer og data sker via VPN-forbindelser.

Eksterne kommunikationsforbindelser
RM-Group A/S har indført procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med stærk kryptering, og at e-mails og anden kommunikation, der indeholder følsomme personoplysninger, er krypteret i forsendelsen ved anvendelse af TLS.

Kryptering af personoplysninger
RM-Group A/S har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

RM-Group A/S har indført procedurer, der sikrer, at data på personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, er krypterede ved ibrugtagning, således at adgang til data alene er muligt for autoriserede brugere. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

De algoritmer og niveauer for kryptering, der er anvendt til kryptering af enheder, servere og data, risikovurderes løbende i forhold til det aktuelle trusselsniveau.

Firewall
RM-Group A/S har indført procedurer, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Netværkssikkerhed
RM-Group A/S har indført procedurer, der sikrer, at netværk i forhold til anvendelse og sikkerhed er opdelt i et antal virtuelle netværk (VLAN), hvor trafik mellem de enkelte virtuelle netværk kontrolleres af firewall. Servere med indbygget firewall benytter denne til at sikre, at der kun gives adgang til nødvendige services.

Antivirusprogram
RM-Group A/S har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselsniveau, og der er opsat en løbende overvågning af disse systemer, herunder periodisk test for funktionalitet.

Sårbarhedsscanning og penetrationstests
RM-Group A/S har indført procedurer, der sikrer, at systemer er indført med henblik på at identificere og imødegå tekniske sårbarheder i applikationer, services og infrastruktur, således at tab af fortrolighed, integritet og tilgængelighed af systemer og data undgås.

Sikkerhedskopiering og retablering af data
RM-Group A/S har indført en procedure, der sikrer, at systemer og data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation. Sikkerhedskopier er beskyttede med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde, eller at sikkerhedskopier ødelægges ved brand, vand, hærværk eller hændelig skade.

Vedligeholdelse af systemsoftware
RM-Group A/S har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og software installeret på servere og arbejdsstationer.

Logning i systemer, databaser og netværk
RM-Group A/S har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret mod tab og sletning.

Overvågning
RM-Group A/S har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Afprøvning, vurdering og evaluering
RM-Group A/S har indført procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Databeskyttelse gennem design og standardindstillinger

RM-Group A/S har indført politikker og procedurer for udvikling og vedligeholdelse af RMG C3-platform, der sikrer en styret ændringsproces. Der anvendes et Change Management system til styring af udviklings- og ændringsopgaver, og enhver opgave følger en ensartet proces, der indledes med risikovurdering i overensstemmelse med kravene om databeskyttelse gennem design og standardindstillinger.

Udviklings-, test- og produktionsmiljø er adskilte, og der er etableret funktionsadskillelse mellem medarbejdere i udviklingsafdelingen og i drifts- og supportafdelingen. Enhver udviklings- og ændringsopgave gennemløber et testforløb, og der anvendes anonymiserede produktionsdata som testdata. Der er indført procedurer for versionskontrol, logning og sikkerhedskopiering, således at det er muligt at geninstallere tidligere versioner.

Databehandlerens garantier

RM-Group A/S har indført politikker og procedurer, der sikrer, at RM-Group A/S kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen, og at der sikres beskyttelse af den registreredes rettigheder. RM-Group A/S har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres. Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for uddannelse og instruktion af medarbejdere, der behandler personoplysninger, herunder gennemførelse af awareness og oplysningskampagner.

Fortrolighed og lovbestemt tavshedspligt

RM-Group A/S har indført politikker og procedurer, der sikrer fortrolighed ved behandlingen af personoplysninger. Alle medarbejdere i RM-Group A/S har forpligtet sig til fortrolighed ved at underskrive en ansættelseskontrakt, der indeholder vilkår om tavshed og fortrolighed.

Bistand til den dataansvarlige i forhold til behandlingssikkerhed og konsekvensanalyse

RM-Group A/S har indført politikker og procedurer, der sikrer, at RM-Group A/S kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed og artikel 36 om konsekvensanalyser.

Bistand til den dataansvarlige i forhold til revision og inspektion

RM-Group A/S indført politikker og procedurer, der sikrer, at RM-Group A/S kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til data behandlere, til rådighed for den dataansvarlige. RM-Group A/S giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndigede hertil af den dataansvarlige.

Fortegnelse over kategorier af behandlingsaktiviteter

RM-Group A/S har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt, og den kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk, og den kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

Sletning og tilbagelevering af personoplysninger

RM-Group A/S har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Opbevaring af personoplysninger

RM-Group A/S har indført procedurer, der sikrer, at opbevaring af personoplysninger alene foretages i overensstemmelse med kontrakten med den dataansvarlige og listen over lokationer i den tilhørende databehandleraftale.

Underdatabehandlere

RM-Group A/S har indført politikker og procedurer, som sikrer, at underdatabehandlere er blevet pålagt de samme databeskyttelsesforpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og RM-Group A/S, og at underdatabehandlerne kan give tilstrækkelige garantier til beskyttelse af personoplysninger. Procedurerne sikrer, at den dataansvarlige giver en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere, herunder at der sker en styring af ændringer i godkendte underdatabehandlere.

RM-Group A/S vurderer underdatabehandleren og dennes garantier, forinden der indgås aftale for at sikre, at underdatabehandleren kan overholde de forpligtelser, som er pålagt RM-Group A/S. RM-Group A/S fører et

årligt tilsyn med sine underdatabehandlere, baseret på en risikovurdering af den konkrete behandling af personoplysninger ved blandt andet at indhente revisorerklæringer af typen ISAE 3000 eller SOC 2 eller lignende dokumentation.

Overførsel af personoplysninger til tredjelande

RM-Group A/S har indført politikker og procedurer, der sikrer, at overførelsen af personoplysninger til underdatabehandlere i lande uden for EU sker i henhold til EU-US Privacy, standardkontrakt eller andet gyldigt overførselsgrundlag og ifølge instruks fra den dataansvarlige.

Bistand til den dataansvarlige i forhold til den registreredes rettigheder

RM-Group A/S har indført politikker og procedurer, der sikrer, at RM-Group A/S kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

Underretning om brud på persondatasikkerheden

RM-Group A/S har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse efter, at RM-Group A/S er blevet opmærksom på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at vurdere, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden

RM-Group A/S har indført politikker og procedurer, der sikrer, at RM-Group A/S kan bistå den dataansvarlige med artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden.

ÆNDRINGER I PERIODEN

RM-Group A/S har ikke foretaget større ændringer af support-driftsopgaver af applikationen RMG C3 og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i perioden.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Den dataansvarlige er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed opfylde Databeskyttelseslovgivningen.

- Den dataansvarlige har ansvaret for at sikre, at administratorernes brug af RMG C3 og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen.
- Den dataansvarlige styrer brugerrettighederne i RMG C3, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.
- Såfremt der indtastes særlige følsomme oplysninger i fritekstfelter, skal den dataansvarlige oplyse til RM-Group A/S, om der skal implementeres yderligere sikringsforanstaltninger.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i RM-Group A/S beskrivelse af support-driftsopgaver af applikationen RMG C3 samt for udformningen og den operationelle effektivitet af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af RM-Group A/S, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden 1. januar til 31. december 2023.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen og den operationelle effektivitet heraf er udført ved forespørgsel, inspektion, observation og genudførelse.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos RM-Group A/S passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som Wannafind leverer indenfor hosting, har vi modtaget ISAE 3402 erklæring for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. januar 2023 til 31. december 2023.

For de ydelser, som Google Commerce Limited Gordon House leverer inden for hosting, har vi modtaget ISO/IEC 27001:2013 certifikat for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller gældende til 14. maj 2024.

For de ydelser, som Sendgrid Twilio leverer indenfor e-mail afsendelse har vi modtaget SOC 2 erklæring for perioden 1. juni 2022 til 31. maj 2023 og ISO/IEC 27001:2013 certifikat gældende til den 31. oktober 2025.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i RM-Groups A/S beskrivelse af support-driftsopgaver af applikationen RMG C3 og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos RM-Group A/S, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

Resultatet af de udførte test af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet og implementeret eller ikke har fungeret effektivt i perioden.

Kontrolområde A		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Indgåelse af databehandleraftale med den dataansvarlige ▶ Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ▶ Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. ▶ Databehandleraftaler underskrives og opbevares elektronisk. ▶ Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for indgåelse af skriftlige databehandleraftaler og observeret, at der er overensstemmelse med de ydelser, som databehandleren leverer. Vi har inspiceret, at der foreligger en skabelon til brug for indgåelse af databehandleraftaler. Vi har observeret, at alle databehandleraftaler er underskrevet og opbevares elektronisk. Vi har observeret, at der i skabelon for databehandleraftalen fremgår information om brugen af underdatabehandler. Vi har stikprøvevist inspiceret indgåede databehandleraftaler og observeret, at brugen af underdatabehandlere er anført samt at dataansvarlig skal godkende eventuel ændring af underdatabehandlere.	Ingen afvigelser konstateret.
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret den seneste indgåede databehandleraftale og observeret, at databehandleraftalen indeholder en instruks. Vi har stikprøvevist inspiceret indgåede databehandleraftaler og observeret, at databehandleren kun behandler personoplysninger efter dokumenteret instruks fra den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolområde A		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig. ▶ Databehandlerens procedurer gennemgås og opdateres løbende og minimum en gang årligt. ▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevist inspiceret indgåede databehandleraftaler og observeret, at databehandleren kun behandler personoplysninger efter dokumenteret instruks fra den dataansvarlige. Vi har inspiceret procedure for behandling af personoplysninger, som seneste er opdateret april 2023. Vi har ved forespørgsel fået oplyst, at databehandler gennemgår og opdatere procedurer løbende i henhold til deres årshjul. Vi har inspiceret procedure for behandling af personoplysninger og observeret, at databehandleren efterlever den instruks fra dataansvarlig.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig, i tilfælde hvor den dataansvarliges instruks, strider mod databeskyttelseslovgivningen. ▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for underretning af dataansvarlige og observeret, at denne anfører, at i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelsesloven, skal databehandleren informere den dataansvarlige. Vi har stikprøvevist inspiceret indgåede databehandleraftaler og observeret, at databehandleren straks skal underrette den dataansvarlige i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen. Vi har ved forespørgsel fået oplyst, at der ikke er modtaget ulovlige instrukser i erklæringsperioden, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af support-driftsopgaver af applikationen RMG C3 baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret at databehandleren har en procedure for risikovurderinger og observeret, at sandsynlighed og konsekvens for at risikoen indtræffer vurderes i forhold til datas tilgængelighed, fortrolighed og integritet. Vi har endvidere inspiceret databehandlerens risikovurdering for den registrerede. Vi har observeret, at sårbarheder løbende registreres og vurderes ud fra identificerede trusler. Vi har observeret, at der i henhold til procedure for risikovurdering, er foretaget en årlig risikovurdering.	Ingen afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, beredskabsplanerne er tidssvarende og effektive i kritiske situationer. ▶ Beredskabstest dokumenteres og evalueres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens hændelsesstyringsproces som udgør beredskabsplan og observeret, at denne indeholder specifikke handlinger, hvis en hændelse gør at hele systemet kompromitteres eller hvis enkelte dataansvarlige er omfattet. Vi har observeret, at beredskabsplanen er afprøvet i erklæringsperioden. Vi har foretaget inspektion af databehandlerens test af beredskabsplan og observeret, at testen dokumenteres og evalueres.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang. ▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret at databehandleren har adgangskontrol på deres kontor. Vi kan observeret, at databehandleren dagligt kontrollerer for uautoriseret adgange og forsøg for adgang til deres kontor. Vi har ved forespørgsel fået oplyst, at databehandler løbende gennemgang, oversigt med hvem der har adgang til kontoret. Vi har inspiceret databehandleren har en checkliste for fratrådte medarbejdere og for en stikprøve observeret at den fratrådt medarbejdere har returneret nøglebrik. Vi har i forhold til serverrum inspiceret ISAE 3402 fra underdatabehandler og observeret, at der ikke er observationer i forhold til fysisk adgang og sikkerhed.	Ingen afvigelser konstateret.
Logisk adgangskontrol ▶ Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. ▶ Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. ▶ Der foretages logning af alle brugeradgange og brugeraktiviteter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at der er tre medarbejder hos databehandleren, som opretter brugere i deres systemer, herunder dataansvarliges administrative medarbejdere. Vi har ved forespørgsel fået oplyst, at databehandleren løbende evaluere brugerens arbejdsbetinget behov for rettigheder og observeret, at det senest er foretaget november 2023. Vi har observeret, at databehandler logger alle loginforsøg.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation. ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere.	Vi har for en stikprøve observeret, at brugeroprettelser følger en styret proces og kun tildeles de rettigheder, som de har et arbejdsbetinget behov for. Vi har for en stikprøve af stoppede medarbejdere i erklæringsperioden observeret, at der er foretaget blokering af adgang i systemet. Vi har ved forespørgsel fået oplyst, at der kun er to medarbejdere hos databehandleren, som kan tilgå dataansvarliges personoplysninger ud fra et arbejdsbetinget behov. Vi har stikprøvevis inspiceret brugerlister og observeret, at der ikke er andre RM-Group A/S medarbejdere end de to pågældende medarbejdere, som fremgår på listerne. Vi har observeret, at der anvendes to-faktor autentifikation, når personoplysninger hos den dataansvarlige tilgås. Vi har observeret, at databehandleren benytter Single-Sign-On. Vi har inspiceret databehandlerens regler for krav til adgangskoder og observeret, at der er sat password krav op. Vi har inspiceret adgangskodedatabase til eksterne systemer og observeret, at passwordpolitikken overholdes.	
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. ▶ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedspolitik og observeret, at den indeholder krav til brug af VPN og at arbejdsstationer skal have installeret et opdateret antivirus program.	Vi har konstateret, at databehandlerens opsætning af VPN ikke lever op til minimumskrav omkring brug af TLSv1.2. Ingen yderligere afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har for en stikprøve observeret, at antivirus program er installeret og opdateret. Vi har inspiceret konfigurationen til fjernadgang med VPN og observeret, at medarbejder med et arbejdsbetinget behov har adgang til en VPN-løsning på deres PC. Vi har inspiceret databehandlerens opsætning af VPN og observeret, at krypteringen, der benyttes, er af svag styrke. Vi har observeret, at der anvendes to-faktor autentifikation, når personoplysninger hos den dataansvarlige tilgås.	
Kryptering af personoplysninger ▶ Databehandleren har implementeret en krypteringspolitik for kryptering af personoplysninger. Politikken definerer styrken og protokollen for kryptering. ▶ Der benyttes stærk kryptering af oplysninger når de sendes over offentlige netværk ▶ Oplysninger krypteres i database.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren krypterer persondata i systemet. Vi har for en stikprøve observeret, at databehandlerens bærbare enheder er krypteret. Vi har observeret, at databehandleren anvender e-mail-kryptering i form af TLS ved forsendelser. Vi har observeret, at CPR-nr. er krypteret i databasen.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall til sikring mod uvedkommendes adgang til systemer. ▶ Databehandler anvender kun services/porte som de har behov for.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens firewall konfiguration, og observeret, at der anvendes et deny-by-default princip.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
▶ Firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov.	Vi har observeret, at databehandleren kun anvender porte, som der er behov for. Vi har ved forespørgsel fået oplyst, at databehandleren sørger for at porte kun er åbne, når der er behov for det samt at firewallen løbende opdateres.	
Netværkssikkerhed ▶ Netværkstopologien er struktureret efter best-practice principper, hvilket betyder at servere, som driver applikationer ikke kan nås direkte fra internettet. ▶ Databehandlerens netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet. ▶ Databehandleren anvender kendte netværksteknologier og mekanismer for at beskytte internt netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværkstypologi og observeret at netværket er segmenteret. Vi har observeret, at databehandleren anvender firewall, som beskytter deres interne netværk. Vi har observeret, at firewallen løbende opdateres. Vi har ved forespørgsel fået oplyst, at Wannafind hoster netværket. Vi har inspiceret revisorerklæring for Wannafind for perioden 1. januar til 31 december 2023 og observeret, at der ikke er nogen afvigelser om netværkssikkerhed.	Ingen afvigelser konstateret.
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer. ▶ Antivirus-software opdateres løbende og opdateret med seneste version.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens sikkerhedspolitik og observeret, at denne indeholder krav til antivirus systemer. Vi observeret, at alle arbejdsstationerne har et antivirus program installeret og at de løbende opdateres med seneste version.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har for en stikprøve observeret, at arbejdsstationer og servere har installeret og opdateret antivirus.	
Sårbarhedsscanning og penetrationstests ▶ Databehandleren gennemgår og vurderer deres underleverandør, der hoster databehandlerens netværk. ▶ Databehandleren foretager penetrationstest efter forespørgsel fra deres kunder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at Wannafind hoster netværket og at databehandleren ikke selv foretager sårbarhedsscanninger. Vi har ved forespørgsel fået oplyst, at den dataansvarlige kan bestille yderligere dokumentation for sikkerheden fx en penetrationstest. Vi har inspiceret revisorerklæring for Wannafind for perioden 1. januar til 31 december 2023 og observeret, at sårbarhedsscanning er blevet testet uden observationer.	Ingen afvigelser konstateret.
Sikkerhedskopiering og retablering af data ▶ Der foretages dagligt backup af systemer og data. ▶ Drift og opbevaring af backup er outsourcet til underleverandør. ▶ Der udføres restore-tests 4 gange årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en politik for backup. Vi har observeret, at databehandleren fortager daglige backups. Vi har inspiceret konfigurationen for backup og observeret, at denne gemmes i 14 dage. Vi har ved forespørgsel fået oplyst, at opbevaring af backup er outsourcet til Wannafind.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret revisorerklæring for Wannafind for perioden 1. januar til 31 december 2023 og observeret, at backup er blevet testet uden observationer. Vi har inspiceret, at databehandleren har opsat en kontrol for at udføre restore test hvert kvartal og har for en stikprøve observeret, at den er blevet gennemført succesfuldt.	
Vedligeholdelse af systemsoftware ▶ Databehandler fører en oversigt over systemsoftware/tredjepartsprogrammer som vedligeholdes og opdateres løbende. ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende. ▶ Databehandleren har implementeret en manuel proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret en oversigt over installeret software på arbejdsstationer og servere. Vi har inspiceret procedure for PC sikkerhed og observeret, at databehandler kontrollerer for opdateringer hver 2. uge. Vi har ved forespørgsel fået oplyst, at processen for opdatering er manuelt. Vi har for en stikprøve observeret, at arbejdsstationer og servere løbende får opdateret operativsystemer.	Ingen afvigelser konstateret.
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges. ▶ Databehandler opbevarer logs i 1000 registreringer. ▶ Databehandler monitorerer og logger netværkstrafik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren logger adgange til dataansvarliges data, herunder logins og brugerændringer i system og database. Vi har ved forespørgsel fået oplyst, at loggen for den enkelte dataansvarliges brug af systemet bliver opbevaret i 5 år.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret, at databehandler monitorerer netværkstrafikken. Vi har inspiceret log over netværkstrafik og observeret, at loggen viser de sidste 1000 registreringer.	
Overvågning ▶ Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet. ▶ Databehandleren notificeres om identificeret alarmer og følger op herpå.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren overvåger produktionsmiljø for oppe tid, ydeevne og kapacitet. Vi har inspiceret PRTG dashboard, hvoraf alarmer og uregelmæssigheder fremgår. Vi har observeret, at databehandleren reagerer og følger op på alarmer.	Ingen afvigelser konstateret.
Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger ▶ Databehandler afprøver, vurdere og evaluerer effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. De data som varetages på vegne af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens årshjul og observeret, at der er implementeret kontroller til brug for afprøvning, vurdering og evaluering af deres sikkerhedsforanstaltninger. Vi har observeret at databehandleren har foretaget evaluering for både teknisk og organisatoriske sikkerhedsforanstaltninger.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Udvikling og vedligeholdelse af systemer ▶ Databehandleren arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelses opgaver. ▶ Risikovurdering af systemændringer er udført for, at sikre databeskyttelse gennem design og standardindstillinger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi er ved forespørgsel blevet oplyst, at databehandleren arbejder med privacy-by-design som en integreret del af udvikling og vedligeholdelse. Vi har observeret, at databehandleren arbejder ud fra privacy by design i udvikling og vedligeholdelsesopgaver, herunder at der skal foretages risikovurdering af systemændringer når relevant. Vi har ved forespørgsel fået oplyst, at udvikling sker via projekter i GITlab, hvor hver delopgave er defineret samt at sikkerhedsmæssige overvejelser bliver tilføjet som kommentarer i systemet når relevant. Vi har for en stikprøve observeret, at databehandleren har foretaget risikovurdering på systemændringer.	Ingen afvigelser konstateret.
Informationssikkerhed i udvikling og ændringer ▶ Databehandler arbejder ud fra security-by-design principper i udviklings- og ændringsopgaver. ▶ Rollback-plan er implementeret i tilfælde af fejl i produktionsmiljøet. ▶ Brugeroprettelse sker som udgangspunkt med laveste brugerrettighedsniveau.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at security-by-design principper følges i udviklings- og ændringsopgaver. Vi har inspiceret, at databehandleren har en procedure for rollback igennem Gitlab. Vi har inspiceret roller og rettigheder i grupper med adgang til de to udviklingsmiljøer og observeret, at brugere er oprettet på det lavest mulige niveau i henhold til arbejdsbetinget behov.	Ingen afvigelser konstateret.

Kontrolområde B		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Adskillelse af udviklings-, test og produktionsmiljø ▶ Der er indført funktionsadskillelse mellem udvikling og drift. ▶ Ændringer af funktionalitet testes, inden det sættes i drift. ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. ▶ Der benyttes et versionsstyringssystem som registrerer alle ændringer i kildekode. ▶ Udviklings- og testmiljøer er adskilt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret en oversigt over medarbejder, der har adgang til kildekoden. Vi har observeret, at databehandleren tester i udviklingsmiljøet før ændringer sættes i drift. Vi har observeret, at man registrerer alle ændringer i kildekoden. Vi har observeret, at der er en adskillelse mellem udviklings – og testmiljøet.	Ingen afvigelser konstateret.
Personoplysninger i udviklings- og testmiljø ▶ Der anvendes anonymiseret testdata i udviklings- og testmiljø.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at hvis der er behov for at hente persondata ned til udviklerne til brug for fejlfinding, bliver persondata anonymiseret. Vi har observeret, at data i testmiljøet er anonymiseret.	Ingen afvigelser konstateret.
Supportopgaver ▶ Supporteres adgange og håndtering af personoplysninger ved supportopgaver sker ud fra et arbejdsbetingede behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at der kun er 2 medarbejdere, som kan udføre supportopgaver efter et arbejdsbetinget behov. Vi har stikprøvevis inspiceret dokumentation for supportopgaver og observeret, at disse er udført ud fra et arbejdsbetinget behov.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Informationssikkerhedspolitik ▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Databehandleren har udarbejdet og implementeret en databeskyttelsespolitik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er implementeret en informationssikkerhedspolitik. Vi har inspiceret, at der er implementeret en databeskyttelsespolitik.	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt. ▶ Databehandlerens databeskyttelsespolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at IT-sikkerhedspolitikken er blevet opdateret årligt, senest november 2023. Vi har observeret, at databeskyttelsespolitikken er blevet opdateret i erklæringsperioden og senest april 2024.	Ingen afvigelser konstateret.
Organisering af informationssikkerhedspolitik ▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed. ▶ Databehandler har dokumenteret og etableret ledelsesstyrring af databeskyttelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed ved ledelsesgodkendelse af sikkerheds – og databeskyttelses politikken.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse. ▶ Databehandleren udfører baggrundstjek af alle jobkandidater i overensstemmelse med databehandlerens procedure og den funktion, som jobkandidaten skal besidde.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret ramme for jobsamtaler og observeret, at databehandler som en del af screeningen af potentielle medarbejdere foretager flere interviews i ansættelsesprocessen. Vi er ved forespørgsel blevet oplyst, at der indhentes straffeattest ved ansættelse af nye medarbejdere. Vi er ved forespørgsel blevet oplyst, at der er indhentet straffeattest for nye ansatte i erklæringsperioden, og vi har observeret, at det fremgår af ansættelseskontrakten, at det forudsættes, at medarbejderen til stadighed kan fremvise en ren straffeattest.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse og off-boarding af medarbejdere ved ophør af ansættelse. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedure for fratrædelse og off-boarding af medarbejdere. Vi har inspiceret, at databehandleren har en checkliste for fratrådte medarbejdere. Vi har stikprøvevis observeret, at databehandleren har fulgt deres procedure og checkliste i erklæringsperioden. Vi har inspiceret skabelon for ansættelseskontrakten og observeret at medarbejderne herigennem er forpligtet til absolut tavshed såvel under som efter ansættelsen. Vi har observeret, at den fratrådte medarbejder blev informeret om, at fortroligheden forsat er gældende efter ansættelsen.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og informationssikkerhed, i forlængelse af ansættelsen. ▶ Databehandleren foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens procedure for træning og observeret, at denne indeholder krav til træning af såvel nye som nuværende medarbejdere. Vi har observeret, at nye ansættelser i erklæringsperioden har gennemgået og forstået databehandlerens informationssikkerhedspolitik. Vi er ved forespørgsel blevet oplyst, at awareness-træning foregår løbende ved løbende information om relevante emner.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. ▶ Eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelon for ansættelseskontrakt og observeret, at medarbejderne herigennem bliver underlagt tavshedspligt. Vi har for en stikprøve observeret, at nye ansættelser i erklæringsperioden har underskrevet ansættelseskontrakt, som indeholder afsnit om tavshedspligt. Vi har ved forespørgsel fået oplyst, at processen for eksterne konsulenter er, at der bliver udarbejdet en NDA. Vi har ved forespørgsel fået oplyst, at databehandleren ikke har anvendt eksterne konsulenter i erklæringsperioden, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Bistand til den dataansvarlige i forhold til behandlingssikkerhed og konsekvensanalyser ▶ Der ydes bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har ved forespørgsel fået oplyst, at databehandleren yder bistand til den dataansvarlige i forhold til artikel 32-36, herunder at foretage konsekvensanalyse.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til revision og inspektion ▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandler bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standard skabelon for en databehandleraftale og observeret, at databehandleren heri forpligter sig til at få udarbejdet en ISAE 3000-erklæring. Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation. Vi har foretaget inspektion af databehandlerens standard skabelon for en databehandleraftale og observeret, at databehandleren heri forpligter at give dataansvarlig mulighed for fysisk tilsyn. Vi har ved forespørgsel fået oplyst, at databehandleren ikke har fået forespørgsler om fysisk tilsyn, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde C		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret at databehandleren har en fortegnelse over behandlingsaktiviteter som databehandler. Vi har ved forespørgsel fået oplyst, at fortegnelsen opdateres løbende ved væsentlige ændringer. Vi har observeret, at der er foretaget opdatering af fortegnelsen i erklæringsperioden.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens system.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at fortegnelsen opbevares elektronisk i databehandlerens system.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at fortegnelsen opbevares elektronisk i databehandlerens system og således kan udlevere fortegnelsen på anmodning fra Datatilsynet. Vi har ved forespørgsel fået oplyst, at der ikke har været anmodning fra datatilsynet herom, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde D		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelon for databehandleraftalen og observeret, at databehandleren herigennem er forpligtet til at slette alle personoplysning, der er blevet behandlet på vegne af den dataansvarlige. Vi har af liste over ophørte aftaler stikprøvevist observeret, at datebehandleren er informeret af dataansvarlige om ophør og at det er bekræftet, at systemet er lukket for den dataansvarlige efter instruks.	Ingen afvigelser konstateret.
Tilbagelevering af personoplysninger ▶ Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen. ▶ Dataansvarlig og databehandler har aftalt i hvilket format, overførelse og medie data skal tilbageleveres, når det anmodes af dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at den dataansvarlige oplyses om muligheden for at få tilbageleveret persondata efter ophørt aftale inden persondata slettes i databehandlerens system. Vi har ved forespørgsel fået oplyst, at dataansvarlig og databehandler aftaler ved ophør af aftalen, hvilket format, overførelse og medie data skal tilbageleveres via, når det anmodes af dataansvarlig. Vi har ved forespørgsel fået oplyst, at der ikke har været ophørte aftaler i erklæringsperioden, hvor der har været ønske om tilbagelevering af personoplysninger, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde E		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Opbevaring af personoplysninger ▶ Personoplysninger opbevares utilgængeligt for andre. ▶ Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper. ▶ Fortroligheden af digitale personoplysninger opbevares i krypteret form. ▶ Personoplysninger opbevares kun så længe der er hjemmel/en legitim grund.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi kan observeret, at databehandler tildeler adgang til personoplysning efter et arbejdsbetinget behov. Vi har ved forespørgsel fået oplyst, at personoplysninger bliver krypteret. Vi har ved forespørgsel fået oplyst, at kryptering sker via et SQL-script som køres automatisk. Vi har observeret, at personoplysninger opbevares i krypteret form. Vi har observeret, at databehandleren kun opbevare personoplysninger så længe, der er en aftale med den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolområde F		
Kontrolmål ▶ *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.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftaler og instruks ○ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale. ○ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ○ Databehandleraftaler med underdatabehandler underskrives og opbevares elektronisk. ○ Databehandleraftaler med underdatabehandlers indeholder informationer om brugen af underdatabehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har indgået databehandleraftaler med deres underdatabehandlere. Vi har observeret, at databehandleraftaler med underdatabehandlere er underskrevet og opbevares elektronisk. Vi har for en stikprøve inspiceret databehandleraftalen med underdatabehandleren og observeret, at underdatabehandleren kun må behandle personoplysninger efter instruks fra den dataansvarlige, herunder at databehandleraftalen indeholder informationer om at underdatabehandlere ikke må anvendes uden en skriftlig godkendelse af den dataansvarlige.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens standard skabelon for en databehandleraftale og observeret, at databehandleren heri lister anvendte underdatabehandlere. Vi har observeret, at databehandleren kun anvender godkendte underdatabehandlere.	Ingen afvigelser konstateret.

Kontrolområde F		
Kontrolmål ▶ *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.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Ændringer i godkendte underdatabehandlere ▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler. ▶ Dataansvarlig har mulighed for at gøre indsigelse vedrørende udskiftning af underdatabehandler. ▶ Ved udskiftning af underdatabehandler skal databehandleren have en ny forudgående specifik skriftlig godkendelse fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelonen for databehandleraftale og observeret, at der heri anføres, at den dataansvarlige til enhver tid skal informere, hvis der sker ændringer i relevante underdatabehandlere. Vi har stikprøvevist inspiceret indgåede databehandleraftaler og observeret at databehandleren 3 måneder før skal informere den dataansvarlige ved brug nye underdatabehandlere. Vi har ved forespørgsel fået oplyst, at der ikke er sket udskiftning af underdatabehandlere i erklæringsperioden, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet lokation for behandling samt hvilken type af behandling og kategori af personoplysninger, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en oversigt over godkendte underdatabehandlere, som indeholder information om lokation for behandling.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende. ▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren har foretaget en risikovurdering af brugen af underdatebehandlerne Amazon, Google, Vonage og Sendgrid Twilio.	Ingen afvigelser konstateret.

Kontrolområde F		
Kontrolmål ▶ *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.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året, baseret på en risikovurdering.	Vi har inspiceret, at databehandleren udfører tilsyn med deres underdatabehandlere ud fra en risikovurdering. Vi har inspiceret ISAE 3402 erklæring fra Wannafind for perioden 1. januar til 31. december 2023, Google ISO/IEC 27001:2013 certifikat gældende til 14. maj 2024, SOC 2 erklæring for Sendgrid Twilio for perioden 1. juni 2022 til 31. maj 2023 og ISO/IEC 27001:2013 certifikat gældende til den 31. oktober 2025.	

Kontrolområde G

Kontrolmål

- *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.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Overførsel af personoplysninger til tredjelande ▶ Der foreligger skriftlige procedurer for overførsel af personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. ▶ Databehandlerens procedure gennemgås og vurderes løbende, og som minimum en gang årligt, om proceduren skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelonen for databehandleraftale og observeret, at enhver overførsel af personoplysning til tredjelande eller internationale organisationer kun må foretages af datebehandleren efter instruks fra den dataansvarlige. Vi har observeret, at databehandleren anvender Google som underdatabehandler, og at data kun behandles i Frankfurt. Vi har observeret, at der ikke er indgået supportaftale med Google. Vi har observeret, at databehandleren anvender Amazon som underdatabehandler, og at data kun behandles i Luxemborg. Vi har observeret, at databehandleren anvender Vonage som underdatabehandler, og at data kun behandles i Amsterdam. Vi har observeret, at databehandleren anvender Sendgrid Twilio som underdatabehandler, og at data kun behandles i Irland. Vi har observeret, at ikke alle relevante underdatabehandlere fremgår af Data-Privacy-Framework.	Vi har konstateret, at Google, Amazon, Vonage og Sendgrid Twilio har tiltrådt det nye overførselsgrundlag EU-U.S. Data Privacy Framework, som trådte i kraft den 10. juli 2023. Databehandleren har redegjort for, at der i perioden før den 10. juli 2023, ikke skete overførsel af personoplysninger til usikre tredjelande, og at de har konfigureret samt implementeret sikringsforanstaltninger til beskyttelse af personoplysninger ved brug af Google, Amazon, Vonage og Sendgrid Twilio som underdatabehandler. Vi har konstateret, at databehandleren benytter Clickatell som underdatabehandler, uden at denne har tiltrådt det nye overførselsgrundlag EU-U.S. Data Privacy Framework. Ingen yderligere afvigelser konstateret.

Kontrolområde H

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Bistand til den dataansvarlige i forhold til de registreredes rettigheder - Databehandler har udarbejdet en procedure for bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder. - Det er muligt at give indsigt i alle oplysninger, der er registreret i support-driftsopgaver af applikationen RMG C3.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelonen for databehandleraftale og observeret, at databehandleren herigennem forpligter sig i at yde bistand til den dataansvarlige. Vi har ved forespørgsel fået oplyst, at der ikke har været forespørgsel fra den dataansvarlige i forhold til bistand i erklæringsperioden, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.

Kontrolområde I		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelonen for databehandleraftale og observeret, at databehandleren herigennem forpligter sig at sikre underretning til den dataansvarlige ved brud på persondatasikkerheden. Vi har ved forespørgsel fået oplyst, at der ikke er sket brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har opsat overvågning af supportdriftsopgaver af applikationen RMG C3 til detektion af brud på persondatasikkerhed. ▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har observeret, at databehandleren registeret potentielle databrud i deres interne registreringssystem, til brug for løbende vurdering af databrud. Vi har ved forespørgsel fået oplyst, at der ikke er sket brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunne efterprøve kontrollen.	Ingen afvigelser konstateret.
Bistand til den dataansvarlige i forhold til brud på persondatasikkerheden ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret skabelonen for databehandleraftale og observeret, at databehandleren herigennem forpligter sig at bistå den dataansvarlige i forhold til brud på persondatasikkerheden.	Ingen afvigelser konstateret.

Kontrolområde I		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har ved forespørgsel fået oplyst, at der ikke har været forespørgsel om bistand, hvorfor vi ikke har kunne efterprøve kontrollen.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

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."

Nicolai Tobias Visti Pedersen
Partner, Statsautoriseret revisor
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 185.81.xxx.xxx
2024-04-25 12:47:18 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner, chef for Risk Assurance, CISA, CRISC
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2024-04-25 12:47:34 UTC

Per Bruus
Administrerende direktør
På vegne af: RM-Group
Serienummer: d2b43f24-1d73-4523-9fde-2850f15cedad
IP: 87.61.xxx.xxx
2024-04-25 12:48:09 UTC