www.pwc.dk

Rackhosting ApS

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden fra 1. maj 2021 til 30. april 2022 i henhold til databehandleraftale med dataansvarlige

November 2022

pwc

Indholdsfortegnelse

1. Ledelsens udtalelse

Rackhosting behandler personoplysninger på vegne af Rackhostings kunder, enten som databehandler for kunder der er dataansvarlige eller som underdatabehandler hvor kunderne er databehandlere, i henhold til særskilte databehandleraftaler, knyttet til hver kundes hostingaftale.

Medfølgende beskrivelse er udarbejdet til brug for Rackhostings kunder, der har anvendt Rackhostings hostingydelser, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne") er overholdt.

Rackhosting anvender Global Connect som serviceunderleverandør til datacenter og netværk. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Global Connect varetager for Rackhosting.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunder og Global Connect er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke egnetheden af udformningen og funktionaliteten af disse komplementære kontroller.

Rackhosting bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af informationssikkerhed og foranstaltninger i relation til Rackhostings hostingydelser, der har behandlet personoplysninger for kunder omfattet af databeskyttelsesreglerne i hele perioden fra. 1. maj 2021 til 30 april 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan af informationssikkerhed og foranstaltninger i relation til Rackhostings hostingydelser 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 manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter kundens valg sker sletning eller tilbagelevering af alle personoplysninger til kunden, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at kunden kan foretage anmeldelse til tilsynsmyndigheden samt underretning af 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

- Kontroller, som vi med henvisning Rackhostings hostingydelsers afgrænsning har forudsat ville være implementeret af kunder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne hostingydelser til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og derfor ikke kan omfatte ethvert aspekt Rackhostings hostingydelser, som den enkelte kunde måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. maj 2021 til 30. april 2022. Kriterierne anvendt for at give denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

(ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. maj 2021 til 30. april 2022.

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesreglerne.

Tåstrup d. 15. november 2022

Martin Helms
Adm. Direktør – Rackhosting ApS

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000 erklæring om informationssikkerhed og foranstaltninger i relation til behandling af personoplysninger for perioden fra 1. maj 2021 til 30. april 2022 i henhold til standard databehandleraftaler med kunder.

Omfang

Vi har fået som opgave at afgive erklæring om Rackhostings beskrivelse i afsnit 3 af deres informationssikkerhed og foranstaltninger i relation til Rackhostings hostingydelser i henhold til databehandleraftale med kunder for perioden fra 1. maj 2021 til 30. april 2022 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Rackhosting har udformet og effektivt udført hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4. Erklæringen omfatter ikke en vurdering af Rackhostings generelle efterlevelse af kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne").

Rackhosting anvender Global Connect som serviceunderleverandør til datacenter og netværk. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som Global Connect varetager for Rackhosting.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunder og Global Connect er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke egnetheden af udformningen og funktionaliteten af disse komplementære kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Rackhostings ansvar

Rackhosting er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme 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.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Rackhostings beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gældende i Danmark, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af deres hostingydelser samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i ledelsens udtalelse.

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

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

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af deres informationssikkerhed og foranstaltninger i relation til Rackhostings hostingydelser, således som de var udformet og implementeret i hele perioden fra 1. maj 2021 til 30. april 2022, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet og implementeret i hele perioden fra 1. maj 2021 til 30. april 2022, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. maj 2021 til 30. april 2022.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt Rackhostings hostingydelser, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som kunder selv har udført, ved vurdering af om kravene i databeskyttelsesreglerne er overholdt.

København, den 15. november 2022
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr 33 77 12 31

Michael Clement
statsautoriseret revisor
mne23410

3. Beskrivelse af behandling

Indledning

Denne systembeskrivelse vedrører informationssikkerhed og foranstaltninger i relation til Rackhostings hostingydelser..

Rackhosting ApS anvender GlobalConnect A/S, som underleverandør af fysisk sikkerhed i datacentre, hvor Rackhosting's systemer er placeret. GlobalConnect A/S betragtes ikke som en underdatabehandler som følge af, at GlobalConnect A/S kun leverer housing services af infrastruktur.

Rackhosting ApS varetager infrastruktur, hostingplatform og monitorering i forbindelse med it-drift og hosting-aktiviteter og er i forbindelse hermed ansvarlig for at sikre implementeringen og funktionen af kontrolsystemer, for at forebygge og opdage fejl, herunder bevidste fejl, med henblik på overholdelse af kontrakter og god skik.

Denne beskrivelse er afgrænset til generelle standarder for administration som beskrevet i Rackhosting ApS standardkontrakt. Specifikke forhold, der er relateret til individuelle kundekontrakter, er ikke omfattet.

Beskrivelse af ydelser, der er omfattet af erklæringen

De ydelser, som Rackhosting ApS leverer, er tilpasset flere forskellige typer af kunder. Betingelserne for de enkelte kunder er angivet i kontrakter, hvor der for hvert forretningsområde tages udgangspunkt i standardkontrakter, som kan indeholde individuelle tilretninger og optioner. Til specifikke kunder er disse betingelser angivet i driftshåndbøger, som er udleveret til kunden og fungerer som systemdokumentation.

Følgende områder dækker over de ydelser, som Rackhosting ApS tilbyder:

Hosting platform:

- VMware vCloud
- Tier 1 Storage Area Network (SAN) – primært og sekundært site
- Tier 2 Storage Area Network (SAN) – primært og sekundært site
- Tier 3 Storage Area Network (SAN) – primært og sekundært site
- Fortinet Fortigate Nextgen firewall – primært og sekundært site

Kundevendte services:

- Spamexperts e-mail Antispam & antimalware service
- DNS drift (dns1.rackhosting.com, dns2.rackhosting.com & dns3.rackhosting.com
- Veeam backup services
- Ahsay backup services
- Microsoft 365

Interne services

- Nagios overvågning
- Serviecdesk
- ControlManager
- Active directory
- Microsoft 365

Med baggrund i den ovenstående afgrænsning og nedenfor nærmere angivne systembeskrivelse vurderer Rackhosting ApS, at vi i alle væsentlige forhold har opretholdt effektive kontroller. Rackhosting ApS er opmærksom på at der kontinuerligt sker udvikling indenfor området, og Rackhosting ApS arbejder kontinuerligt på at udvikle og forbedre kontrollerne.

Arbejdet med GDPR er delt i to fokusområder – det interne, som vedrører alle interne processer hvor vi som virksomhed har med persondata at gøre (eksempelvis HR, it, marketing og økonomi) og det kundevendte, som denne erklæring omfatter, der vedrører alle de områder hvor vi interagerer med vores kunder og potentielt kunne komme i berøring med persondata.

Rackhosting ApS drifter it, som naturligvis er i overensstemmelse med gældende lovgivningsmæssige krav, herunder EU persondataforordningen, og vi har som udgangspunkt ikke berøring med kundernes persondata.

Styring af overholdelse af krav mv.

Overholdelse af kravene i relation til databeskyttelse og beskyttelse af persondata følger den organisation, som allerede er etableret i relation til håndtering af it- og informationssikkerhed.

Organisationsform og ledelse bygger på en funktionsopdelt struktur, hvor lederen for den enkelte afdeling har personaleansvar. Sikkerhedsansvaret i de enkelte processer er tildelt henholdsvis ansvarlige og udførende. Den ansvarlige har ansvar for driften og dokumentationen af de enkelte processer hos de ansatte.

Politikker og organisering

For at sikre sammenhæng mellem arbejdet med databeskyttelse / it-sikkerhed og organisationen er der oprettet et it-sikkerhedsudvalg (RH Sikkerheds Komité).

It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse, mellemledere samt driftsmedarbejdere. It-sikkerhedsudvalget refererer direkte til direktionen.

Rackhosting ApS' It-sikkerhedsudvalg består af:

- CEO, Partner & Stifter, Martin Helms
- CTO & Partner, Hans Jørgensen
- Salgschef & Partner, Philip Hegaard
- Netværkssikkerhed, Daniel Frantzen
- Dokumentation og compliance, Brian Rasmussen

Udvalget er normgivende og fastsætter på grundlag af den vedtagne it-sikkerhedspolitik, de principper og retningslinjer, der skal sikre målopfyldelsen.

Medlemmer af it-sikkerhedsrådet deltager løbende i relevant efteruddannelse inden for it-sikkerhed mv. It-sikkerheden er effektueret igennem intern strategi, politikker, standarder, procedurer og guidelines.

CTO'en er ansvarlig for den operationelle drift i henhold til de udarbejdede retningslinjer, den daglige ledelse, samt medlem af it-sikkerhedsudvalget.

Det er ligeledes CTO'en, der er ansvarlig for at kommunikere retningslinjerne, der understøtter it-sikkerhedspolitikken, ud til den enkelte ansatte.

Udvalget er normgivende og fastsætter på grundlag af den vedtagne it-sikkerhedspolitik de principper og retningslinjer, der skal sikre målopfyldelsen. Tilsvarende gælder for databeskyttelsespolitikken "GDPR retningslinjer i Rackhosting".

Udvalget behandler alle it-sikkerhedsspørgsmål og databeskyttelsesspørgsmål af principiel karakter.

Når politikker og procedurer opdateres, kommunikeres dette til medarbejdere. Politikker og procedurer er tilgængelige i ISMS værktøjet, ControlManager™, hvor medarbejderne altid kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til it-sikkerhedskoordinatoren, der sørger for relevante rettelser.

Rackhosting ApS har ikke en DPO, da den primære aktivitet for kerneforretningen ikke omfatter formidling eller berigelse af persondata, men udelukkende hosting. Rackhosting har dog en funktion (Compliance and Data protection) der varetager DPO relaterede opgaver.

CTO'en er ansvarlig for den operationelle drift i henhold til de udarbejdede retningslinjer, og er ligeledes medlem af it-sikkerhedsudvalget. Direktøren er ansvarlig for den daglige ledelse, overordnede retningslinjer samt håndteringen af hændelser. Det er medarbejdernes daglige leder, der er ansvarlig for at kommunikere retningslinjerne, der understøtter it-sikkerhedspolitikken, ud til den enkelte ansatte.

Procedurer og kontroller

Rackhosting ApS har etableret en række politikker og procedurer, som alle medarbejdere har modtaget og er trænet i at efterleve. Disse består bl.a. af:

• Informationssikkerhedspolitikken

• Persondatapolitik

• Specifikke procedurer

For hvert løsningsområde og tværgående proces jf. de forrige afsnit er der lavet en risikovurdering af setuppet og applikationen set i forhold til efterlevelse af den registreredes rettigheder, herunder vurdering af, hvorvidt der er etableret de passende tekniske og organisatoriske kontroller på områderne.

Rackhosting ApS har med afsæt i risikovurderingen etableret relevante procedurer.

Rackhosting ApS tillader ikke kunder at placere persondata på Rackhostings systemer, medmindre der er indgået en databehandleraftale med kunden (dataansvarlig eller databehandler). Når en aftale indgås, gennemgås denne efter nogle faste tjekpunkter, og alle indgåede databehandleraftaler journaliseres med beskrivelse af særlige krav fra den dataansvarlige (fx svarfrister og/eller krav til særlige kontroller). Eventuelle særlige krav kommunikeres til de relevante teams internt til efterlevelse i deres servicering af kunderne.

Tekniske og organisatoriske foranstaltninger

I relation til tekniske og organisatoriske foranstaltinger henvises til den udarbejdede ISAE 3402 erklæring.

Disse omfatter områder som:

• Medarbejdersikkerhed

• Styring af informationsrelaterede aktiver

• Adgangsstyring

• Kryptering

• Fysisk sikkerhed og miljøsikring

• Driftssikkerhed

• Kommunikationssikkerhed

• Anskaffelse, udvikling og vedligeholdelse af systemer

• Leverandørforhold

• Styring af sikkerhedshændelser

• Nød-, beredskabs- og reetableringsstyring

Henvendelser fra de dataansvarlige

Rackhosting ApS har en procedure for håndtering og dokumentation af henvendelser fra dataansvarlige i relation til bistand til håndtering af de registreredes rettigheder (indsigtsret, sletning, berigtigelse mv.).

Dokumentation af henvendelser fra dataansvarlige vedr. f.eks. indsigtsret, sletning, berigtigelse mv. håndteres i vores supportsystem.

Under hensyntagen til behandlingens karakter bistår Rackhosting så vidt muligt den dataansvarlige, ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder i henhold til Databeskyttelsesforordningen.

I det omfang Rackhosting ApS forestår behandling af persondata på vegne af og efter instruks fra den dataansvarlige, bistår Rackhosting den dataansvarlige med at sikre overholdelsen af:

- forpligtelsen til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et niveau, der er tilpasset de risici, der er forbundet med behandlingen
- forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
- forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

- forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

- forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko pga. mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen

Kontrolaktiviteter i forhold til standardskabelonen fra FSR-Danske Revisorer og Datatilsynet der ikke er inkluderet i erklæringens sektion 4

Nedenstående Kontrolaktiviteter i forhold til standardskabelonen fra FSR-Danske Revisorer og Datatilsynet der ikke er inkluderet i erklæringens sektion 4, da de ikke er relevante for Rackhostings hostingydelser:

Nr.	Databehandlerens kontrolaktivitet
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.

Komplementerende kontroller hos de dataansvarlige

Som led i levering af ydelserne er der kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i beskrivelsen. Dette omfatter bl.a.:

- Stillingtagen til konsekvenser i relation til persondatabeskyttelse når der ændres i eksisterende løsninger (privacy by design og privacy by default) og fremsættelse af ændringsanmodning hertil til Rackhosting ApS i relevant omfang.

- Stillingtagen til / test af nye versioner af løsninger ifm. implementering (change management).

- Opsætning og styring af egne brugere i løsningen i produktionsmiljøet (identity and access management).

- Opsætning og styring af Rackhosting personale, med adgang til kundens miljø (identity and access management).

- Sikring af at personfølsomme oplysninger ikke medsendes i supportsager til Rackhosting via ticketsystemet mv.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Vi har ved stikprøvetest af kundekontrakter inspiceret, at der er indgået en databehandleraftale med tilhørende instruks vedrørende behandling af personoplysninger.	Området er testet uden væsentlige bemærkninger.
A.2	Rackhosting udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	Vi har forespurgt ledelsen, om Rackhosting har implementeret procedurer til sikring af, at der bliver indgået databehandleraftale om behandlingen af personoplysninger alene foregår i henhold til instruks. Vi har ved stikprøvetest af kundekontrakter inspiceret, at der er indgået en formel og godkendt databehandleraftale med tilhørende instruks vedrørende behandling af personoplysninger.	Området er testet uden væsentlige bemærkninger.

Kontrolmål A:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
A.3	Rackhosting underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	Området er testet uden væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurerne er opdateret. Vi har ved stikprøvetest af databehandleraftaler inspiceret, at der er etableret de aftalte sikkerhedsforanstaltninger.	Området er testet uden væsentlige bemærkninger.
B.2	Rackhosting har implementeret en procedure for risikovurdering af behandling af personoplysninger på vegne af kunder. Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt risikovurderingen er opdateret og passende.	Vi har forespurgt ledelsen, om der foreligger formaliserede procedurer, der sikrer, at Rackhosting foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Vi har ved stikprøvetest af risikovurdering inspiceret, at der er udarbejdet en årlig risikovurdering, der omfatter vurdering af behandling af personoplysninger.	Området er testet uden væsentlige bemærkninger.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har forespurgt ledelsen, om der er etableret procedurer for opdatering af antivirussoftware. Vi har inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Vi har inspiceret, at antivirussoftware er opdateret.	Området er testet uden væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har forespurgt ledelsen, om der er etableret kontroller for anvendelse af firewall. Vi har inspiceret, at Rackhosting har implementeret en passende politik for netværkssikkerhed. Vi har inspiceret, at Rackhosting's firewall er konfigureret i henhold til den interne politik herfor.	Området er testet uden væsentlige bemærkninger.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har forespurgt ledelsen, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Vi har inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Området er testet uden væsentlige bemærkninger.
B.6	Adgang til personoplysninger er isoleret til brugere med et arbejdsbetinget behov herfor.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Vi har ved stikprøvetest inspiceret, at adgang til systemer og data er begrænset til brugere med et arbejdsbetinget behov.	Området er testet uden væsentlige bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har forespurgt ledelsen, om der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Vi har ved stikprøvetest inspiceret, at der er implementeret systemovervågning med alarmering ved kritiske hændelser for systemer, som behandler personoplysninger og der bliver foretaget rettidig opfølgning herpå.	Området er testet uden væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer med retningslinjer for kryptering. Vi har inspiceret, at teknologiske løsninger til kryptering er tilgængelige og aktiveret. Vi har endvidere inspiceret, at Rackhosting anvender TLS kryptering på mailserveren.	Området er testet uden væsentlige bemærkninger.
B.9	Rackhosting logger i overensstemmelse med kundens krav. Dette omfatter som minimum, at der bliver logget oplysninger om dato, brugere og oplysninger om handlinger for systemadministratorers og andre med privilegerede rettigheder. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer der sikrer tilstrækkelig logning. Vi har ved stikprøvetest inspiceret, at der er etableret systemmæssig logning på servere og databaser i henhold til kundens krav, herunder at handlinger udført af systemoperatører og brugere med særlige administrative rettigheder logges og overføres til logningsværktøj. Vi har ved stikprøvetest inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Området er testet uden væsentlige bemærkninger.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests. Vi har ved stikprøvetest inspiceret, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.	Området er testet uden væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Vi har ved udtræk af tekniske sikkerhedsparametre og -opsætninger inspiceret, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Området er testet uden væsentlige bemærkninger.
B.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, herunder om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har inspiceret, at procedurer for adgangsstyring eksisterer og er implementeret. Inspiceret ved en stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for en regelmæssig – mindst årlig – vurdering og godkendelse af tildelte brugeradgange.	Vi har noteret, at der ikke har været fratrædelser i perioden fra 1. maj 2021 til 30. april 2022, hvorfor vi ikke har kunne teste at kontrollen vedrørende fratrådte medarbejdere er implementeret. Området er testet uden væsentlige bemærkninger.

Kontrolmål B:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede, sker som minimum ved anvendelse af tofaktorautentifikation.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede. Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.	Området er testet uden væsentlige bemærkninger.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Vi har inspiceret dokumentation for, at kun autoriserede personer har fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Området er testet uden væsentlige bemærkninger.

Kontrolmål C:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
C.1	Rackhostings ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder Rackhostings medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.	Vi har forespurgt ledelsen, om der er etableret procedurer for udarbejdelse og kommunikation af informationssikkerhedspolitik. Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har endvidere inspiceret, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder Rackhostings medarbejdere. Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer minimum årlig opdatering af informationssikkerhedspolitikken. Vi har inspiceret, at der som minimum sikres årlig opdatering af informationssikkerhedspolitikken.	Området er testet uden væsentlige bemærkninger.
C.2	Rackhostings ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Vi har ved stikprøvetest af databehandleraftaler inspiceret, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.	Området er testet uden væsentlige bemærkninger.

Kontrolmål C:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
C.3	Der udføres en efterprøvning af Rackhostings medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Reference fra tidligere ansættelser • Eksamensbeviser • Straffeattest	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer, der sikrer efterprøvning af Rackhostings medarbejdere i forbindelse med ansættelse. Vi har ved stikprøvetest af databehandleraftaler inspiceret, at kravene til efterprøvning af medarbejdere i aftalen er dækket af Rackhostings procedurer for efterprøvning. Vi har ved stikprøvetest nyansatte medarbejdere inspiceret, at der er dokumentation for, at efterprøvningen har omfattet: • Reference fra tidligere ansættelser • Eksamensbeviser • Straffeattest	Området er testet uden væsentlige bemærkninger.
C.4	Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver medarbejderne introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejdernes behandling af personoplysninger.	Vi har forespurgt ledelsen, om der foreligger procedurer, der sikrer medarbejdere, underskriver en fortrolighedsaftale. Vi har ved stikprøvetest af nyansatte medarbejdere inspiceret, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Vi har ved stikprøvetest af nyansatte medarbejdere inspiceret, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information.	Området er testet uden væsentlige bemærkninger.

Kontrolmål C:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
C.5	Ved fratrædelse er der hos Rackhosting implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har forespurgt ledelsen om der er implementeret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelsen, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages.	Vi har noteret, at der ikke har været fratrædelser i perioden fra 1. maj 2021 til 30. april 2022, hvorfor vi ikke har kunne teste at kontrollen er implementeret. Området er testet uden væsentlige bemærkninger.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, som Rackhosting udfører for de dataansvarlige.	Vi har forespurgt ledelsen, om der er implementeret formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Vi har ved stikprøvetest inspiceret, at der er etableret procedurer for at sikre, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Området er testet uden væsentlige bemærkninger.
C.7	Medarbejdere gennemfører løbende awareness-træning i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har forespurgt ledelsen, om der er etableret procedurer for løbende awareness træning for medarbejdere om behandling af personoplysninger. Vi har inspiceret, at Rackhosting udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger og at denne er tilgængelig på Rackhosting's intranet.	Området er testet uden væsentlige bemærkninger.

Kontrolmål D:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Området er testet uden væsentlige bemærkninger
D.2	• Rackhosting indgår aftale med hver kunde der specificerer hvordan data opbevares og slettes.	Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til Rackhosting's opbevaringsperioder og sletterutiner. Vi har ved stikprøvetest inspiceret, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.	Området er testet uden væsentlige bemærkninger
D.3	Ved ophør af behandlingen af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har forespurgt ledelsen, om der er implementeret procedurer for behandlingen af den dataansvarliges data ved ophør af behandlingen af personoplysninger. Vi har ved stikprøvetest inspiceret, at kundens kontrakt indeholder krav om, hvordan Rackhosting skal håndtere personoplysninger ved ophør.	Vi har noteret, at der ikke har været ophør af kunder i perioden fra 1. maj 2021 til 30. april 2022, hvorfor vi ikke har kunne teste at kontrollen er implementeret. Området er testet uden væsentlige bemærkninger.

Kontrolmål E:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen, om der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at procedurerne er opdateret. Vi har ved stikprøvetest inspiceret, at kunders databehandleraftale indeholder krav om, hvordan Rackhosting skal opbevare og behandle personoplysninger.	Området er testet uden væsentlige bemærkninger.
E.2	Rackhosting har procedurer som sikrer, at Rackhostings databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har forespurgt ledelsen, om der er etableret retningslinjer for godkendelse af lokaliteter for opbevaring af personoplysninger. Vi har ved stikprøvetest inspiceret, at instruksen indeholder krav til den geografiske placering af personoplysninger.	Området er testet uden væsentlige bemærkninger.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at Rackhosting sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret. Vi har ved stikprøvetest inspiceret, at kontrakter med underdatabehandlere indeholder krav om og beskrivelse af de databeskyttelsesforpligtelser, som underdatabehandlere skal efterleve.	Vi har noteret, at der ikke anvendes underdatabehandlere, men alene Global Connect. Dette fremgår af databehandleraftaler.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har ved stikprøvetest inspiceret, at underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Vi har noteret, at der ikke anvendes underdatabehandlere, men alene Global Connect. Dette fremgår af databehandleraftaler.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelsen af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelsen af underdatabehandlere. Vi har ved stikprøvetest inspiceret, at kontrakter med underdatabehandlere indeholder krav om og beskrivelse af de databeskyttelsesforpligtelser, som underdatabehandlere skal efterleve.	Vi har noteret, at der ikke anvendes underdatabehandlere, men alene Global Connect. Dette fremgår af databehandleraftaler.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at Rackhosting sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Vi har ved stikprøvetest af underdatabehandleraftaler inspiceret, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og databehandleren.	Vi har noteret, at der ikke anvendes underdatabehandlere, men alene Global Connect. Dette fremgår af databehandleraftaler.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Vi har noteret, at der ikke anvendes underdatabehandlere, men alene Global Connect. Dette fremgår af databehandleraftaler.
F.6	På baggrund af en ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, foretager Rackhosting en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har forespurgt ledelsen, om der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Vi har noteret, at der ikke anvendes underdatabehandlere, men alene Global Connect. Dette fremgår af databehandleraftaler.

Kontrolmål H:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at Rackhosting skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen, om derer implementeret formaliserede procedurer for Rackhostings bistand til den dataansvarlige i relation til de registreredes rettigheder. Vi har ved stikprøvetest inspiceret, at der er etableret procedurer for at bistå kunder med rettidig håndtering af de registrerede anmodninger.	Området er testet uden væsentlige bemærkninger.
H.2	Rackhosting har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har forespurgt ledelsen, om der foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Området er testet uden væsentlige bemærkninger.

Kontrolmål I:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at Rackhosting skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt ledelsen, om der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har ved stikprøvetest inspiceret, at der er etableret procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden.	Området er testet uden væsentlige bemærkninger.
I.2	Rackhosting har procedurer for registrering af brud på persondatasikkerhed.	Vi har forespurgt ledelsen, om der er implementeret en procedure for håndtering af sikkerhedsbrud. Vi har ved stikprøvetest inspiceret, at Rackhosting registrerer brud på persondatasikkerheden centralt med angivelse af håndteringen af bruddet.	Vi har noteret, at der ikke har været sikkerhedsbrud i perioden 1. maj 2021 til 30. april 2022.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt, om der har været konstateret sikkerhedsbrud hos underdatabehandlerne, og inspiceret, at disse er anført i oversigten over sikkerhedshændelser.	Vi har noteret, at der ikke har været sikkerhedsbrud i perioden 1. maj 2021 til 30. april 2022.

Kontrolmål I:

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

Nr.	Rackhosting's kontrolaktivitet	PwC's udførte test	Resultat af test
I.4	Ved brud på persondatasikkerheden fremsender Rackhosting dokumentation omfattende, som minimum, de faktiske omstændigheder ved bruddet, dets virkning og omfang samt de trufne afhjælpende foranstaltninger til kunden.	Vi har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede anvisninger på: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Vi har inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Området er testet uden væsentlige bemærkninger.