

---

## ***Raptor Services A/S***

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger pr. 1. juni 2022 i henhold til databehandleraftale med dataansvarlige

*Juni 2022*

---

# *Indholdsfortegnelse*

1. Ledelsens udtalelse.....	3
2. Uafhængig revisors erklæring.....	5
3. Beskrivelse af behandling.....	8
4. Kontrolmål, kontrolaktivitet, test og resultat heraf.....	11

# 1. Ledelsens udtalelse

Raptor Services A/S behandler personoplysninger på vegne af dataansvarlige i henhold til databehandler-aftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt ydelser i relation til udvikling, support og drift af kundeløsninger, 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.

Raptor Services A/S anvender Microsoft som underdatabehandler for anvendt hosting. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Microsoft varetager for Raptor Services A/S.

Raptor Services A/S bekræfter, at:

- a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af ydelser i relation til udvikling, support og drift af kundeløsninger, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne pr. 1. juni 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
  - (i) Redegør for, hvordan informationssikkerhed og foranstaltninger i relation til ydelser i relation til udvikling, support og drift af kundeløsninger 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 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 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 til afgrænsning af ydelser i relation til udvikling, support og drift af kundeløsninger har forudsat ville være implementeret af den dataansvarlige, og som,

hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger
- (ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne ydelser i relation til udvikling, support og drift af kundeløsninger til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved ydelser i relation til udvikling, support og drift af kundeløsninger, som den enkelte dataansvarlige 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 pr. 1. juni 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, og
  - (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.
- c) Der er etableret 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.

Aarhus, den 17. juni 2022  
Jan Skov  
COO

## 2. Uafhængig revisors erklæring

### Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger pr. 1. juni 2022 i henhold til databehandleraftale med dataansvarlige

Til: Raptor Services A/S og dataansvarlige

#### Omfang

Vi har fået som opgave at afgive erklæring om Raptor Services A/S' beskrivelse i afsnit 3 af deres ydelser i relation til udvikling, support og drift af kundeløsninger i henhold til databehandleraftale med dataansvarlige pr. 1. juni 2022 (beskrivelsen) og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Raptor Services A/S har udformet hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4. Erklæringen omfatter ikke en vurdering af Raptor Services A/S' 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").

Raptor Services A/S anvender Microsoft som underdatabehandler for anvendt hosting. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som Microsoft varetager for Raptor Services A/S.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Vores konklusion udtrykkes med høj grad af sikkerhed.

#### Raptor Services A/S' ansvar

Raptor Services A/S 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 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 revisors 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 Raptor Services A/S' beskrivelse samt om udformningen 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 gæl-

dende 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af deres ydelser i relation til udvikling, support og drift af kundeløsninger samt for kontrollerens udformning. 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. 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.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

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**

Raptor Services A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved ydelser i relation til udvikling, support og drift af kundeløsninger, som hver enkelt dataansvarlig 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.

### **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 informationssikkerhed og foranstaltninger vedrørende ydelser i relation til udvikling, support og drift af kundeløsninger, således som det var udformet og implementeret pr. 1. juni 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 pr. 1. juni 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 dataansvarlige, der har anvendt Raptor Services A/S' ydelser i relation til udvikling, support og drift af kundeløsninger, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af om kravene i databeskyttelsesreglerne er overholdt.

Aarhus, den 17. juni 2022

**PricewaterhouseCoopers**

Statsautoriseret Revisionspartnerselskab

CVR-nr. 33 77 12 31

Jesper Parsberg Madsen

statsautoriseret revisor

mne26801

## 3. Beskrivelse af behandling

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er ydelser i relation til udvikling, support og drift af løsninger.

### Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om ydelser i relation til udvikling, support og drift af løsninger målrettet mod indsamling og behandling af personoplysninger med henblik på at målrette indhold og produkter på den dataansvarliges webtjenester, e-mail, handelsplatforme, søgemaskiner, sociale medier og andre web-relaterede tjenester samt på ikke-digitale kontaktpunkter ved brug af machine learning og algoritmer, jf. End User License Agreements.

### Personoplysninger

- Almindelige personoplysninger, herunder identifikationsoplysninger som første og tredje-parts CookieID, krypteret e-mailadresse, kundeklubs ID /medlemsnummer, købehistorik, browsing-/adfærdsmønster på den dataansvarliges hjemmeside, eventtype samt forskellige produktinformationer

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Dataansvarligs kunder

### Risikovurdering

Raptor Services A/S har formaliserede processer for risikovurdering af de ydelser, hvor der behandles persondata.

Risikovurderingen gennemgås med fastsatte intervaller, og herudover som minimum når der sker ændringer i et system, implementeres nye forretningsprocesser, tages et nyt system i brug, eller når vi som en del af vores ydelser behandler nye former for personoplysninger.

Omdrejningspunktet for risikovurderingerne er risikoen for/sandsynligheden for et brud på persondatasikkerheden, og hvad konsekvensen af et givent brud vil være for den registrerede.

Risikovurderingerne understøtter, at der til enhver tid er etableret de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, der kan beskytte data, som behandles i enten løsningerne eller i organisationen. Risikovurderingen benyttes i det videre arbejde med iværksættelse af organisatoriske og tekniske sikkerhedsmæssige tiltag til imødegåelse af de risici (risikohåndtering), der fremgår af risikovurderingen.

Risikovurderingerne foretages af ledelsen med input fra relevante medarbejdere fra organisationen. Risikovurderingerne godkendes af direktionen.

Henset til de data, vi behandler, samt de kontroller og organisatoriske og tekniske foranstaltninger, vi har implementeret for at mitigere risiko og minimere sandsynligheden for brud på persondatasikkerheden, vurderes den nuværende risikoprofil for Raptor Services A/S' ydelser som værende lav. For at sikre et konstant fokus på at minimere vores risici har vi etableret kontrolaktiviteter, som bl.a. har til formål både at forebygge og teste, at vores foranstaltninger sikrer god mitigering af disse.

### Kontrolforanstaltninger

Raptor Services A/S har formaliserede processer, der sikrer, at der tages højde for persondatasikkerheden ved onboarding af nye kunder. Dette betyder bl.a., at vi for alle nye projekter (hvor vi udfører databehandlingsaktiviteter for kunden) før idriftsættelse/opstart afstemmer roller, ansvar og forpligtelser, så vi dermed kan sikre at vores arbejdsmetoder lever op til både vores ansvar for god databehandlingsskik og instruksen fra de respektive kunder.



Raptor Services A/S har ligeledes formaliserede processer, der sikrer, at der løbende er GDPR-compliance på alle projekter. Som en del af vores kvalitetsarbejde sikrer den relevante Product Owner samt den ansvarlige leder for Professional Services, at vores fortegnelse og GDPR-compliance gennemgås kontinuerligt.

Raptor Services A/S har ligeledes formaliserede processer, der sikrer, at der løbende er GDPR-compliance på alle projekter. Som en del af vores kvalitetsarbejde sikrer den relevante Product Owner, at vores GDPR-compliance-spørgeskema gennemgås halvårligt.

Raptor Services A/S har formaliserede processer, der sikrer, at data ikke gemmes lokalt, og at data efter endt behandling slettes rettidigt i vores systemer. Derudover forpligter Raptor Services A/Ss medarbejdere sig til at overholde og sikre, at vores slettepolitik i øvrigt efterleves.

Som en del af en formaliseret proces for leverandørstyring indgås der (under)databehandleraftale med alle (under)databehandlere, hvor underdatabehandlerne pålægges mindst de samme forpligtelser, som Raptor Services A/S har overfor kunden. Ligesom det vurderes om nye (under)databehandlere lever op til kravene i Raptor Services A/S' leverandørpolitik.

Raptor Services A/S fører tilsyn med alle (under)databehandlere en gang årligt, samt hvis samarbejdets karakter ændres. Tilsynet foretages med udgangspunkt i væsentlighed og risiko. Med det menes, at der tages hensyn til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risici for fysiske personers rettigheder og frihedsrettigheder. Jo større risici, jo større er kravene til sikkerhed. Tilsynet sker ved gennemlæsning og godkendelse af certifikater, revisionserklæringer og lignende, og alt efter hvilken risiko, der er forbundet med underdatabehandlerens behandlingsaktivitet, kan der følges op ved skriftlig informationsindsamling mv.

Der er i Raptor Services A/S etableret et compliance-setup bestående af kontroller, som udføres internt i organisationen efter aftalt frekvens ift. procedurens formål. Kontrollerne er systemunderstøttede, så vi sikrer, at der sker opfølgning samt eskalering ved manglende udførelse.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

### **Komplementerende kontroller hos de dataansvarlige**

Som et 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. Disse omfatter bl.a.

- Tage stilling til konsekvenser i relation til persondatabeskyttelse ved fremsættelse af ændringsønsker
- Tage stilling til/teste nye versioner af løsninger ved implementering
- Varetage opsætning og styring af egne brugere i løsningen i produktionsmiljøet
- Varetage opsætning og styring af brugere fra Raptor Services A/S, som hjælper i kundens miljø
- Sikre, at personoplysninger ikke medsendes i supportsager
- Orienter Raptor Services A/S ved ændringer i medarbejdere, som har adgang til delte sites mellem kunden og Raptor Services A/S
- Indestå for, at formålet med behandlingen af personoplysningerne er lovligt og sagligt, og at der ikke overlades Raptor Services A/S flere personoplysninger end nødvendigt til opnåelse af formålet
- Være ansvarlig for, at der på tidspunktet for personoplysningernes overdragelse til Raptor Services A/S eksisterer et gyldigt behandlingsgrundlag, herunder at et eventuelt samtykke er frivilligt, specifikt, utvetydigt og informeret samt udtrykkeligt, hvis påkrævet

- Indestå for, at de registrerede personer, som personoplysningerne vedrører, har fået tilstrækkelig information vedrørende behandlingen af personoplysningerne
- Have det primære ansvar for at afgive instruks til Raptor Services A/S om databehandlingen samt varetage forespørgsler fra de registrerede i relation til deres rettigheder.
- Indberette eventuelle brud på persondatasikkerheden til Datatilsynet

## 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.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
A.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	<p>Inspiceret, at ledelsen sikrer, at behandlingen af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret ved en stikprøve på en enkelt behandling af personoplysninger, at denne foregår i overensstemmelse med instruks.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.

### Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved en stikprøve på en enkelt databehandleraftale, at der er etableret de aftalte sikkerhedsforanstaltninger.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>
B.2	<p>Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandleren foretager en risikovurdering for at opnå en passende sikkerhed.</p> <p>Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Inspiceret, at databehandleren har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>
B.3	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.</p>	<p>Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware.</p> <p>Inspiceret, at antivirussoftware er opdateret.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>

### Kontrolmål B:

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

Nr.	Databehandlerens 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.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.  Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.  Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
B.6	Adgang til personoplysninger er isoleret til brugere med et arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger.  Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.  Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.  Inspiceret ved en stikprøve på en enkelt brugers adgang til systemer og databaser, at disse er begrænset til medarbejdernes arbejdsbetingede behov.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.

### Kontrolmål B:

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

Nr.	Databehandlerens 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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.</p> <p>Inspiceret, at teknologiske løsninger til kryptering er tilgængelige og aktiveret.</p> <p>Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
B.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> <li>• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder</li> <li>• Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> <li>○ Ændringer i logopsætninger, herunder deaktivering af logning</li> <li>○ Ændringer i systemrettigheder til brugere</li> <li>○ Fejlede forsøg på log-on til systemer, databaser og netværk</li> </ul> </li> </ul> <p>Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang af og opfølgning på logge.</p> <p>Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.</p> <p>Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og sletning.</p> <p>Inspiceret ved en stikprøve på en enkelt dags logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser.</p> <p>Inspiceret ved en stikprøve på en enkelt dags logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.

### Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
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.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved en stikprøve på en enkelt udviklings- og testdatabase, at personoplysningerne heri er pseudonymiseret eller anonymiseret. Inspiceret ved en stikprøve på en enkelt udviklings- og testdatabase, hvor personoplysningerne ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrations-tests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests. Inspiceret ved en enkelt stikprøve, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.

### Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
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.	<p>Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Inspiceret ved en stikprøve på en enkelt medarbejders adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.</p> <p>Inspiceret ved en stikprøve på en enkelt fratrådt medarbejder, at dennes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.</p> <p>Inspiceret, at der foreligger dokumentation for en regelmæssig – mindst årlig – vurdering og godkendelse af tildelte brugeradgange.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede.</p> <p>Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.</p>	Vores gennemgang har ikke givet anledning til 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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.</p> <p>Inspiceret dokumentation for, at kun autoriserede personer har fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.



**Kontrolmål C:**

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.1	<p>Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.</p>	<p>Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>
C.2	<p>Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.</p>	<p>Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.</p> <p>Inspiceret ved en stikprøve på en enkelt databehandleraftale, at kravene i aftalen er dækket af informationssikkerhedspolitikken krav til sikkerhedsforanstaltninger og behandlingssikkerheden.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>

### Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.3	<p>Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang:</p> <ul style="list-style-type: none"> <li>• Referencer fra tidligere ansættelser</li> <li>• Straffeattest</li> <li>• Eksamensbeviser</li> </ul>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.</p> <p>Inspiceret ved en stikprøve på en enkelt databehandleraftale, at kravene til efterprøvning af medarbejdere i aftalen er dækket af databehandlerens procedurer for efterprøvning.</p> <p>Inspiceret ved en stikprøve på en enkelt nyansat medarbejder, at der er dokumentation for, at efterprøvnin-gen har omfattet:</p> <ul style="list-style-type: none"> <li>• Referencer fra tidligere ansættelser</li> <li>• Straffeattest</li> <li>• Eksamensbeviser</li> </ul>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>
C.4	<p>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.</p>	<p>Inspiceret ved en stikprøve på en enkelte nyansat medarbejder, at den pågældende medarbejder har underskrevet en fortrolighedsaftale.</p> <p>Inspiceret ved en stikprøve på en enkelt nyansat medarbejder, at den pågældende medarbejder er blevet introduceret til:</p> <ul style="list-style-type: none"> <li>• Informationssikkerhedspolitikken</li> <li>• Procedurer vedrørende databehandling samt anden relevant information.</li> </ul>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>

### Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelsen, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages.  Inspiceret ved en stikprøve på en enkelt fratrådt medarbejder, at rettighederne er inaktiveret eller ophørt, samt at aktiverne er inddraget.	Vores gennemgang har ikke givet anledning til 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 databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.  Inspiceret ved en stikprøve på en enkelt fratrådt medarbejder, at der er dokumentation for opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.  Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Vores gennemgang har ikke givet anledning til 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.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
D.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
D.2	Der er i databehandleraftaler aftalt evt. specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	<p>Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.</p> <p>Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.</p> <p>Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysningerne er slettet i overensstemmelse med de aftalte sletterutiner.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
D.3	<p>Ved ophør af behandlingen af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:</p> <ul style="list-style-type: none"> <li>Tilbageleveret til den dataansvarlige og/eller</li> <li>Slettet, hvor det ikke er i modstrid med anden lovgivning.</li> </ul>	<p>Inspiceret, at der foreligger formaliserede procedurer for behandlingen af den dataansvarliges data ved ophør af behandlingen af personoplysninger.</p> <p>Inspiceret ved en stikprøve på en enkelt ophørt databehandling, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.

**Kontrolmål E:**

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
E.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>
E.2	<p>Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.</p>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.</p> <p>Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>

### Kontrolmål F:

*Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren 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.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
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. Inspiceret ved en stikprøve på en enkelt underdatabehandler fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
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.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
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. Inspiceret ved en stikprøve på en enkelt underdatabehandleraftale, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og databehandleren.	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.

### Kontrolmål F:

*Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren 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.5	<p>Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af:</p> <ul style="list-style-type: none"> <li>• Navn</li> <li>• CVR-nr.</li> <li>• Adresse</li> <li>• Beskrivelse af behandlingen.</li> </ul>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.</p> <p>Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>
F.6	<p>På baggrund af en ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, foretager databehandleren en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.</p> <p>Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.</p> <p>Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelandes overførselsgrundlag og lignende.</p> <p>Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>

### 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.*

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
G.1	<p>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.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.</p> <p>Inspiceret ved en stikprøve på en enkelt dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	<p>Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret ved en stikprøve på en enkelt dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.



**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.*

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
H.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>
H.2	<p>Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.</p>	<p>Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> <li>• Udlevering af oplysninger</li> <li>• Rettelse af oplysninger</li> <li>• Sletning af oplysninger</li> <li>• Begrænsning af behandling af personoplysninger</li> <li>• Oplysning om behandling af personoplysninger til den registrerede.</li> </ul> <p>Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>

### Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> <li>• Awareness hos medarbejdere</li> <li>• Overvågning af netværkstrafik</li> <li>• Opfølgning på logning af adgang til personoplysninger</li> </ul>	<p>Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p> <p>Inspiceret dokumentation for, at netværkstrafikken overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv.</p> <p>Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	<p>Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p> <p>Forespurgt, om der har været konstateret sikkerhedsbrud hos underdatabehandlerne, og inspiceret, at disse er anført i oversigten over sikkerhedshændelser.</p>	Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.

**Kontrolmål I:**

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Disse procedurer skal indeholde anvisninger på beskrivelser af:</p> <ul style="list-style-type: none"> <li>• Karakteren af bruddet på persondatasikkerheden</li> <li>• Sandsynlige konsekvenser af bruddet på persondatasikkerheden</li> <li>• Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.</li> </ul>	<p>Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede anvisninger på:</p> <ul style="list-style-type: none"> <li>• Beskrivelse af karakteren af bruddet på persondatasikkerheden</li> <li>• Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden</li> <li>• Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.</li> </ul> <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p>	<p>Vores gennemgang har ikke givet anledning til væsentlige bemærkninger.</p>