Dansk Revision Århus
godkendt revisionsaktieselskab
Tomsagervej 2
DK-8230 Åbyhøj
aarhus@danskrevision.dk
www.danskrevision.dk
Telefon: +45 89 36 12 12
Telefax: +45 89 36 12 00
CVR: DK 26 71 76 71
Bank: 6181 0007769555

Bleau A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Bleau A/S´ kunder.

Indholdsfortegnelse

1. Ledelsens udtalelse

Bleau A/S behandler personoplysninger på vegne af kunder (dataansvarlige) i henhold til indgåede databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Bleau A/S' ydelser, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Bleau A/S anvender underleverandøren og underdatabehandleren Microsoft Azure. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Bleau A/S' underleverandør og underdatabehandler. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i Bleau A/S' beskrivelsen af digitale services, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Bleau A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Bleau A/S bekræfter, at:

a) Den medfølgende beskrivelse, giver en retvisende beskrivelse af, hvordan Bleau A/S har behandlet personoplysninger på vegne af dataansvarlige pr. 30. maj 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Bleau A/S' processer og kontroller relateret til databeskyttelse var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede

- De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

- Kontroller, som vi med henvisning til Bleau A/S' ydelsers afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

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

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne 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 behandlingen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 30. maj 2023. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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

Risskov, den 12. juni

Robert G. Flintenborg

Adm. Direktør Bleau A/S

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Bleau A/S´ kunder relateret til ydelsen.

Til: Bleau A/S og Bleau A/S´ kunder relateret til ydelsen

Omfang

Vi har fået som opgave at afgive erklæring om Bleau A/S' beskrivelse af ydelser i relation til behandling af personoplysninger på vegne af dataansvarlige i henhold til databehandleraftale med Bleau A/S´ kunder i hele pr. 30. maj 2023 om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Bleau A/S anvender underleverandøren og underdatabehandleren Microsoft Azure. Denne erklæring omfat-ter ikke kontrolmål og tilknyttede kontroller hos Bleau A/S' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlernes kontroller, der forudsættes i desig-net af Bleau A/S´ kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos Bleau A/S.

Enkelte af de kontrolmål, der er anført i Bleau A/S' beskrivelse, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Bleau A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Vores konklusion udtrykkes med begrænset sikkerhed.

Bleau A/S' ansvar

Bleau A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 3, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Dansk Revision 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 Bleau A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på at opnå begrænset sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og implementeret.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af Bleau A/S' ydelser samt for kontrollernes udformning og implementering. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke implementeret. Vores handlinger har omfattet test af implementeringen af sådanne kontroller, som vi anser for nødvendige for at give begrænset 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 afsnit 3.

Omfanget af de handlinger vi har udført, er mindre end ved en erklæringsopgave med høj grad af sikkerhed. Som følge heraf er den grad af sikkerhed, der er for vores konklusion, betydeligt mindre end den sikkerhed, der ville være opnået, hvis der var udført en erklæringsopgave med høj grad af sikkerhed.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en dataansvarlig

Bleau 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 Bleau A/S' ydelser, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Under vores arbejde er vi ikke blevet bekendt med forhold, der giver os anledning til at konkludere,

(a) at beskrivelsen af Bleau A/S' ydelser, således som denne var udformet og implementeret pr. 30. maj 2023 ikke i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, ikke i alle væsentlige henseender var hensigtsmæssigt udformet pr. 30. maj 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Bleau A/S' digital services, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Åbyhøj, 12.juni 2023

Dansk Revision Århus
godkendt revisionsaktieselskab, CVR-nr. 26717671

Claus Guldborg Nyvold
registreret revisor

3. Beskrivelse af behandling

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

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

Karakteren af behandlingen

Bleau A/S' behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om Digitale services. Vi driver vores forretning ud fra følgende forudsætninger: At vi kan levere de produkter som vi tilbyder. At vi kan sende og modtage og opbevare informationer på vegne af kunders interessenter (beboere, borgere, ansatte, øvrige gæstebesøgende på hjemmeside)

- Levering, forbedring og tilpasning af den digitale service til Dataansvarlig
- Muliggørelse af dataansvarliges registrerede brugeres adgang til det integrerede IT-system
- Muliggøre dataansvarliges registrerede brugeres benyttelse af systemet.
- Foretage rapportering til Dataansvarlig
- Logning af offentlig indrapportering.
- Typer af databehandling omfatter herudover indsamling, opbevaring, sletning eller tilintetgørelse af data.

Personoplysninger

- Almindelige personoplysninger, identifikationsoplysninger som navn og adresse, telefonnummer, e-mail.
- Andre personlige oplysninger, herunder oplysninger om boligforhold samt cpr. numre.

Følgende kategorier af registrerede personer er omfattet af databehandleraftalen:

- Borgere
- Ansøgere (bolig)
- Beboere
- Bestyrelsesmedlemmer (bolig)
- Ansatte hos Bleau kunde
- Pårørende til beboere og ansatte
- Gæstebesøgende

Instruks fra den dataansvarlige

Bleau handler alene efter instruks fra Dataansvarlig og må kun anvende dataene til de formål, der er angivet ovenfor eller andre formål skriftligt aftalt mellem parterne. Dette fremgår tydeligt igennem vores instruks i databehandleraftale med kunden samt i uddybende beskrivelse af Bleau A/S' håndtering af GDPR personlige data.

Databehandlingen skal ske i overensstemmelse med god databehandlingsskik.

Alle medarbejdere ved ansættelse bliver introduceret gennem sikkerhedspolitik vedr. kunde og personaleadministration og bliver løbende holdt opdateret omkring GDPR gennem vores læringshjul GDPR.

Bleau skal logge alle sine anvendelser af registreredes data. Registreringen indeholder oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Bleau skal på dataansvarliges vegne og efter dataansvarliges instruks opbevare data, herunder logfiler, i op til 6 måneder medmindre dataansvarlig giver Bleau instruks om en længere opbevaringstid for at sikre driften af dataansvarliges digitale løsninger.

Bleau har pligt til at fastsætte og uddybe, iværksætte og opretholde, organisatoriske, administrative og IT-tekniske sikkerhedsforanstaltninger, som forhindrer, at de behandlede data hændeligt eller ulovligt tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid mod lovgivningen.

Bleau skal fastsætte instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af IT-udstyr. Dette fremgår af vores sikkerhedspolitik vedr. kunde og personaleadministration.

Bleau skal sikre, at dennes medarbejdere er pålagt tavshedspligt med hensyn til persondata og behandler persondata fortroligt, herunder ikke-følsomme persondata.

Bleau kan lade databehandlingen ske helt eller delvist fra hjemmearbejdspladsen eller fra lokaler, som Bleau ikke fast driver virksomhed fra, men er forpligtet til at sikre kryptering af persondatakommunikation, der sker via åbne net.

Bleau skal på dataansvarliges anmodning give Dataansvarlig tilstrækkelige oplysninger til, at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet. Dette kan enten være i form af eget kontrolbesøg, eller gennem erklæring udført af uvildig kontrolinstans.

Risikovurdering

Bleau foretager løbende risikovurdering med en konsekvensvurdering på hvad der kan påvirke fortrolighed, tilgængelighed og integritet samt skøn for sandsynlighed og konsekvens. Med afsæt i risikovurderingen er der udarbejdet en sikkerhedspolitik som medarbejdere har modtaget instruks i.

Tekniske og organisatoriske kontrolforanstaltninger

Bleau har foretaget følgende praktiske tiltag, herunder såvel tekniske som organisatoriske, for at sikre overholdelse af krav i databehandleraftalen og for at beskytte persondata bedst muligt:

- It-sikkerhedspolitik og It-beredskabsplan
- Retningslinjer for medarbejdersikkerhed og samtykke
- Styring af aktiver, herunder kontrol af udlevering og returnering af aktiver ved ansættelser og fratrædelser
- Kryptering af data
- Tilsynsplan med underdatabehandler
- Styring af persondatassikkerhedsbrud og hændelseshåndtering
- Sikre etablering af databehandleraftaler med underdatabehandlere
- Sikre, at de krav, der pålægges i henhold til lovgivning eller af kunder via kontrakter og databehandler-aftaler tilsvarende pålægges underdatabehandlere
- Kontrol og opdatering af risikovurdering, politikker og procedurer
- Løbende oplæring af medarbejderne i GDPR
- Kontrol af adgangsforhold efter arbejdsbetinget behov

Databeskyttelsesansvarlig (DPO)

Der ikke er krav til at der bliver udvalgt en DPO. Derimod er der valgt en ansvarlig for GDPR-området – Bleau har valgt adm. direktør som ansvarlig for GDPR, som dermed kan udføre sine opgaver uafhængigt af de enkelte ressortområder inden for organisationen. Adm. Direktør er tegningsberettiget for virksomheden, og kan som ansvarlig foretage nødvendige foranstaltninger af såvel sikkerhedsmæssig og økonomisk karakter.

Anvendelse af underdatabehandlere

Der føres årligt tilsyn med underdatabehandler med kontrol for at sikre at Bleau som dataansvarlig og databehandler, kan opretholde sine forpligtigelser gennem brug af underdatabehandlers tjenester.

- Underdatabehandler er oplyst i databehandleraftale mellem Bleau og Dataansvarlig. Her følges dataan-svarliges instruks for brug af underdatabehandler, der sikrer at de krav i henhold til lov, der pålægges Bleau som databehandler, ligeledes er pålagt og følges af underdatabehandler.
- Bleau er forpligtet til at underrette dataansvarlig i tilfælde af ændringer eller udskiftning af underdata-behandlere.

Overførsel af personoplysninger

Bleau må ikke overføre personoplysninger til tredjepart uden godkendelse af dataansvarlig. Der anvendes udelukkende EU/EAA baseret datacentre. Personoplysninger er krypteret i henhold til standard for kryptering.

De registreredes rettigheder

Vi oplyser de berørte registrerede om hvilke data vi som dataansvarlig eller databehandler i egenskab af vores drift af virksomhed, har brug for at behandle. For de registrerede, er der udarbejdet procedure for hvordan vi behandler deres persondata og deres rettigheder i forbindelse med behandlingen. Først og fremmest afgivelse af samtykke til dataansvarlig, de registreredes rettigheder, opbevaring af data, sletning af data og udlevering af data.

Håndtering af persondatasikkerhedsbrud

Bleau følger en It-beredskabsplan hvor der procedure for overvågning og drift samt en instruks ved en eventuelt sikkerhedsbrist for persondata.

- Bleau er forpligtet til straks/uden unødig forsinkelse at underrette Dataansvarlig om ethvert brud på persondatasikkerheden. Det gør vi ved at følge procedure i Beredskabsplan for databrud
- Såfremt Bleau modtager henvendelser fra en tredjepart vedrørende indholdet af data, der stammer fra dataansvarliges systemer eller kunder, skal Bleau videresende disse henvendelser eller henvise til in-struks fra Dataansvarlig (DBA) samt følge instruks for beredskabsplan for databrud.
- Dataansvarlig skal videresende henvendelser og oplysninger til Bleau, som angår Bleau konkrete databehandling.
- Bleau skal orientere Dataansvarlig om fravigelser af de givne instrukser vedrørende behandlingen. Sær-ligt skal afvigelser, der kan kompromittere datakorrekthed, oplyses.

- Hvis der er mistanke om, eller hvis der indtræffer hændelser, som indikerer et brud på persondatasikkerheden, skal dette straks meddeles til den anden part. Her følger procedure IT Beredskabsplan Bleau samt Beredskabsplan for databrud.

- Ved brud eller mistanke om brud på persondatasikkerheden, underretter Bleau Dataansvarlig herom uden unødigt ophold og senest 24 timer efter bruddet eller mistanken herom er konstateret, således at Dataansvarlig kan overholde sine forpligtelser om at vurdere og eventuelt anmelde sikkerhedsbruddet til Datatilsynet indenfor 72 timer.

Bleau må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, uden forudgående skriftlig aftale med Dataansvarlig om indholdet af en sådan kommunikation, medmindre Bleau har en retlig forpligtelse til sådan kommunikation.

Samtykke og oplysningspligt

Bleau indhenter samtykke fra de registrerede på vegne af de dataansvarlige. Derudover er på vegne af dataansvarlige udarbejdet procedure og kontroller for de registreredes samtykke ved besøg på hjemmeside og ved login for brug af dataansvarliges tjenester som kræver samtykke og som er en del af Bleau databehandling.

Fortegnelse

Bleau føre fortegnelse over databehandling på vegne af kunder indenfor vores branchevertikaler. Fortegnelserne holdes løbende opdateret ved ændringer til databehandling.

Fortegnelsen indeholder følgende:

1) Kontaktoplysninger Bleau. Hvem der er Databeskyttelsesrådgiver. Hvem der er dataansvarlige.
2) Behandlingens formål
3) Kategorier af registrerede og kategorier over deres personoplysninger
4) Oplysninger om overførsel til tredjeland(e)
5) Sletning
6) En generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger.

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

Komplementerende kontroller hos de dataansvarlige

- Dataansvarlig er dataansvarlig for de personoplysninger, som Dataansvarlig instruerer Bleau om at behandle. Der skal derfor foreligge en underskrevet databehandleraftale
- Dataansvarlig har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Lov nr. 502 af 23/05/2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven).
- Dataansvarlig er pligtig til at sikre at eventuelle tredjeparter, der optræder på dataansvarliges vegne, efterlever de samme forpligtelser som Dataansvarlig selv. Dette foregår gennem instruks i databehandleraftale.
- Dataansvarlig er pligtig til at sikre, at der ikke foretages indgreb eller handlinger, som kan kompromittere eller besværliggøre Bleau A/S' databehandling uden forudgående godkendelse fra Bleau. Dette foregår gennem instruks i databehandleraftale.

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 indgående databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt, om der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har forespurgt om, hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget.	Ingen anmærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har forespurgt om, hvordan ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks, og vi har vurderet hensigtsmæssigheden heraf.	Ingen anmærkninger.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har forespurgt, om der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har forespurgt, om der forligger formaliserede procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	Ingen anmærkninger. Der har ikke været behov for underretninger i perioden, hvorfor vi ikke har kunnet teste implementeringen af kontrollen.

Kontrolmål A **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Vi har vurderet, om det er sandsynligt, at der vil ske underretning af den dataansvarlige hvis instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt, om der foreligger formaliserede procedurer, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres. Vi har forespurgt om, hvornår procedurer er opdateret.	Ingen anmærkninger.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der	Vi har forespurgt, om den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Ingen anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har forespurgt databehandler om, hvilke tekniske foranstaltninger der er implementeret, og hvordan disse sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Vi har inspiceret dokumentation for, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med en enkelt udvalgt dataansvarlig.	
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har forespurgt om der på systemer og databaser der anvendes, til behandling af personoplysninger er installeret antivirus. Vi har forespurgt om antivirus programmer løbende opdateres.	Ingen anmærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har forespurgt om adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall. Vi har forespurgt om den er passende konfigureret.	Ingen anmærkninger.
B.5	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har forespurgt, om der foreligger formaliserede procedurer for begrænsning af brugernes adgang til personoplysninger. Vi har forespurgt, om der foreligger formaliserede procedurer for periodisk opfølgning på, at	Ingen anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		brugernes adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Vi har inspiceret udtræk fra systemet over brugere med adgang til personoplysninger, er begrænset til medarbejdernes arbejdsbetingede behov.	
B.6	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har forespurgt, om der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen anmærkninger.
B.7	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har forespurgt, om der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Vi har forespurgt, om teknologiske løsninger til kryptering har været tilgængelige og aktiveret pr. erklæringsdatoen. Vi har inspiceret opsætning af enkelt tilfældigt udvalgt transmissionsvej at kryptering er effektiv.	Ingen anmærkninger.
B.8	Der er etableret logning i systemer og databaser.	Vi har forespurgt, om der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af	Ingen anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås i forbindelse med fejlsøgning.	personoplysninger, herunder gennemgang og opfølgning på logs. Vi har forespurgt om logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, har været konfigureret og aktiveret i hele erklæringsperioden. Vi har forespurgt, om opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning. Vi har inspiceret ud fra en tilfældigt udvalgt dags logning, at logfiler har det forventede indhold i forhold til opsætning.	
B.9	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har forespurgt, hvordan det sikres, at anvendelsen af testdata alene sker i pseudonymiseret eller anonymiseret form. Vi har inspiceret ved for en tilfældigt udvalgt udviklings- henholdsvis testdatabase, at personoplysninger heri er pseudonymiseret eller anonymiseret.	Ingen anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.10	Ændringer til systemer og databaser følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har forespurgt, om der foreligger formaliserede procedurer for håndtering af ændringer til systemer og databaser, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.	Ingen anmærkninger.
B.11	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger.	Vi har forespurgt, om der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har inspiceret for 2 ud af 2 tiltrådte medarbejder, at adgange til systemer og databaser, er godkendt, og at der er et arbejdsbetinget behov. Vi har inspiceret for 1 ud af 1 fratrådt medarbejder, at dennes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.	Ingen anmærkninger.
B.12	Adgang til systemer og databaser, hvori der sker behandling af dataansvarliges personoplysninger, sker som minimum ved anvendelse af to-faktor autentifikation.	Vi har forespurgt, om der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved adgang til behandling af dataansvarliges personoplysninger. Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen anmærkninger.
B.13	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, om der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Ingen anmærkninger.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har forespurgt, om der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har forespurgt om, hvordan informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen anmærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret ved en repræsentativ databehandleraftale, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen anmærkninger.
C.3	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har, for 2 ud af 2 nyansatte medarbejdere i erklærings-perioden inspiceret, at den pågældende medarbejder har underskrevet en fortrolighedsaftale og er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen anmærkninger.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.4	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har forespurgt, om der foreligger procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har, for 1 uf af 1 fratrådt medarbejder i erklærings-perioden inspiceret, at rettigheder er inaktiveret, samt forespurgt på at aktiver er inddraget.	
C.5	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har forespurgt, om der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen anmærkninger.
C.6	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har forespurgt, om databehandleren udbyder awareness-træ-ning til medarbejderne omfattende generel it-sikkerhed og be-handlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført awareness-træning.	Ingen anmærkninger.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.7	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver og bliver inddraget i relevante områder.	Vi har forespurgt, om der foreligger en vurdering af behov for en databeskyttelsesrådgiver.	Ingen anmærkninger. Databehandleren har ikke pligt til at udpege en officiel DPO, men har udpeget en databeskyttelsesansvarlig i virksomheden for at sikre fokus på compliance.
C.8	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige. Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige indeholder: • Navn og kontaktoplysninger på databehandleren, de dataansvarlige, den dataansvarliges eventuelle repræsentanter og databeskyttelsesrådgivere • De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige • Når det er relevant, oplysninger om overførsel til et tredjeland eller en international organisation samt dokumentation for passende garantier • Hvis det er muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger.	Vi har inspiceret, at der foreligger fortegnelser, over behandlingsaktiviteter på vegne af kunder. Vi har inspiceret, at fortegnelser indeholder: • Navn og kontaktoplysninger på databehandleren, de dataansvarlige, den dataansvarliges eventuelle repræsentanter og databeskyttelsesrådgivere • De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige • Når det er relevant, oplysninger om overførsel til et tredjeland eller en international organisation samt dokumentation for passende garantier	Ingen anmærkninger.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		• Hvis det er muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger.	

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*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt, om der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har forespurgt om, hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget.	Ingen anmærkninger.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har forespurgt, om de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens op-bevaringsperioder og sletterutiner.	Ingen anmærkninger.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har forespurgt, om der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har forespurgt om der har været nogle ophørte databehandlinger.	Ingen anmærkninger. Vi er blevet informeret om, at der ikke har været nogle ophørte databehandlinger, hvorfor vi ikke har kunnet teste implementeringen af kontrollen.

Kontrolmål E **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt, om der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har forespurgt om, hvornår procedurer er opdateret.	Ingen anmærkninger.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har forespurgt, om databehandleren har et overblik over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Vi har inspiceret, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen anmærkninger.

Kontrolmål F **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt, om der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har forespurgt om, hvornår procedurer er opdaterede, og hvilke opdateringer der eventuelt er foretaget.	Ingen anmærkninger
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har forespurgt, om databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har, for alle underdatabehandler fra databehandlerens oversigt over underdatabehandlere inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige (specifikt eller indirekte).	Ingen anmærkninger.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække	Vi har forespurgt, om der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.	Ingen anmærkninger. Vi er blevet informeret om, at der ikke har væ-ret nogen ændringer i anvendelse af underda-tabehandlere, hvorfor vi ikke har

Kontrolmål F **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.		kunnet teste implementeringen af kontrollen.
F.4	Databehandleren har, som minimum, pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har forespurgt, om der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Vi har inspiceret, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	I en enkelt databehandleraftale med en kunde er der angivet en yderligere underleverandør ud over Microsoft Azure. Det er oprindeligt en fejl at underleverandøren er blevet angivet i databehandleraftalen, da denne ikke behandler persondata på vegne af Bleau. Databehandleraftalen med pågældende underleverandør er derfor annulleret og kunden er informeret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har forespurgt, om databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Vi har inspiceret, at oversigten indeholder de krævede oplysninger.	Ingen anmærkninger.

Kontrolmål F **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har forespurgt, om der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Vi har inspiceret dokumentation for, at der er foretaget en risikovurdering af underdatabehandlere. Vi har inspiceret dokumentation for, at der er udført tilsyn med underdatabehandlere i henhold til resultatet af risikovurderingen.	Ingen anmærkninger.

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*	*Revisors udførte test*	*Resultat af revisors test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har stikprøvevis inspiceret, at databehandleraftaler beskriver proceduren for overførsler til tredjelande. Vi har forespurgt til, om der overføres personoplysninger til tredjelande, og vi har inspiceret oversigten over lokation for data.	N/A – ingen overførsler til tredjelande, da de data der opbevares hos Microsoft Azure på EU servere ligger i en krypteret lock box som ikke kan tilgås af Microsoft.

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*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt, om der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har forespurgt om, hvornår procedurer er opdateret.	Ingen anmærkninger.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har forespurgt om de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vi har vurderet, om det er sandsynligt, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen anmærkninger.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har forespurgt, om der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har forespurgt om, hvornår procedurer er opdateret.	Ingen anmærkninger.
I.2	Databehandleren har etableret kontroller for identifi-kation af eventuelle brud på persondatasikkerheden.	Vi har forespurgt om databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Vi har inspiceret dokumentation for, at der foreligger et lærings-hjul som omhandler GDPR samt læring omkring sikkerhedsbrud.	Ingen anmærkninger.
I.3	Databehandleren har ved eventuelle brud på person-datasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har forespurgt, om databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har forespurgt, om der har været persondatasikkerhedsbrud indenfor det seneste år.	Ingen anmærkninger. Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud indenfor det seneste år, hvorfor vi ikke har kunnet teste implementeringen af kontrollen.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden	Vi har forespurgt om de foreliggende procedurer for underretning af de dataansvarlige ved brud	Ingen anmærkninger.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
	• Sandsynlige konsekvenser af bruddet på persondata-sikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	på persondatasikkerheden indeholder detalje-rede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på person-datasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at hånd-tere bruddet på persondatasikkerheden. Vi har vurderet om det er sandsynligt, at de fore-liggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	

PENNEO

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

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

Robert Møller Filtenborg
Adm. direktør
Serienummer: b50087b2-5fa0-4961-aee1-9751ad9c7093
IP: 152.115.xxx.xxx
2023-06-12 08:51:04 UTC

MitID

Claus Guldborg Nyvold
Registreret revisor
Serienummer: CVR:26717671-RID:1077207344095
IP: 188.120.xxx.xxx
2023-06-12 08:54:43 UTC

NEM ID

Penneo dokumentnøgle: 4MFVP-P77V6-UXNSC-SHYHP-GHLHF-KSAI3