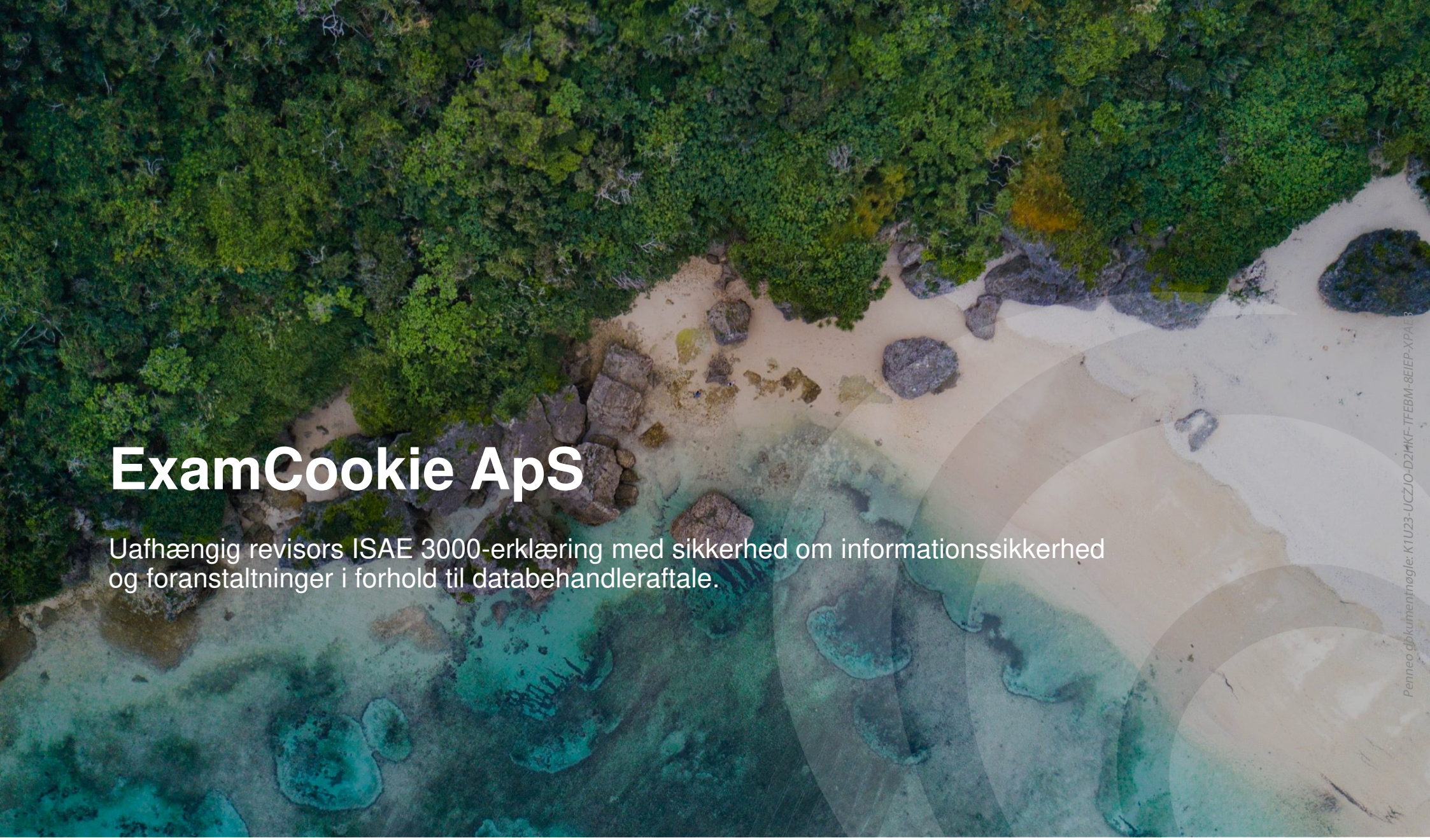
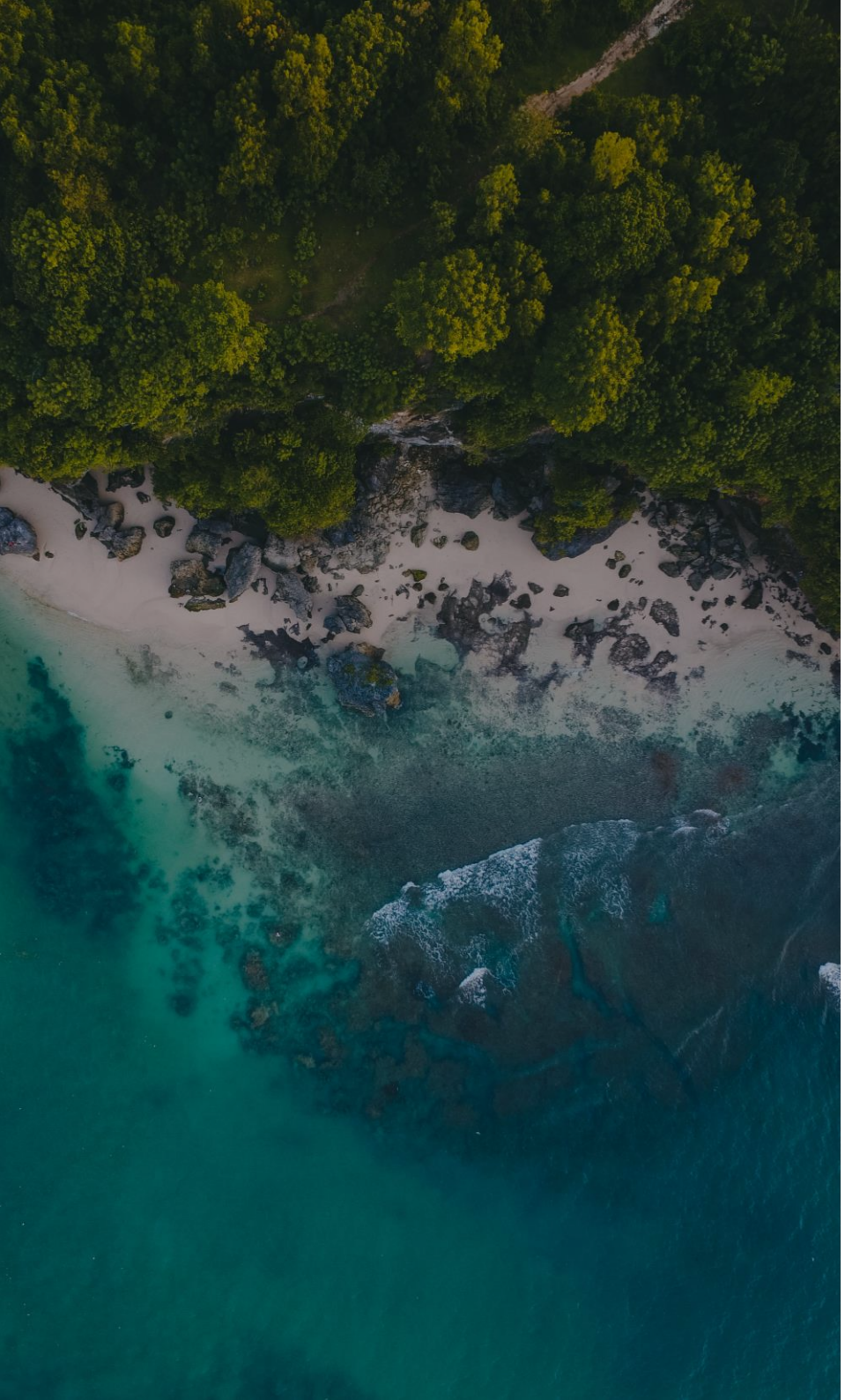


ExamCookie ApS

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i forhold til databehandleraftale.

bakertilly

Now, for tomorrow



Indholdsfortegnelse

1. Ledelsens udtalelse

ExamCookie ApS, CVR-nr. 29 55 34 91, behandler personoplysninger på vegne af de dataansvarlige i henhold til indgåede databehandleraftaler, dækkende den konkrete softwareløsning til uddannelsesinstitutioner, mere specifikt monitorering under eksamen, der leveres til den enkelte dataansvarlige.

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt ExamCookie ApS' software i forbindelse med deres prøver og eksamener, 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. ExamCookie ApS bekræfter, at:

a) Den medfølgende beskrivelse, side 7 - 9, giver en retvisende beskrivelse af de softwareløsninger og informationer ExamCookie indsamler, hvor der har været behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden 23. august 2023 til 22. august 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan softwareløsningen 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

1. Ledelsens udtalelse (fortsat)

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

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

ii. Indeholder relevante oplysninger om ændringer ved databehandlerens softwareløsning til behandling af personoplysninger foretaget i perioden 23. august 2023 til 22. august 2024.

iii. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne softwareløsning 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 den leverede softwareløsning, 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 efter vores vurdering hensigtsmæssigt udformet og fungerede i hele perioden 23. august 2023 til 22. august 2024. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

iii. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 23. august 2023 til 22. august 2024.

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.

Aalborg, den 4. september 2024

Direktion

Morten Claudius Jakobsen

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med ExamCookie ApS' kunder relateret til ydelsen.

Til: ExamCookie ApS og ExamCookie ApS' kunder relateret til ydelsen.

Omfang
Vi har fået som opgave at afgive erklæring om ExamCookie ApS' beskrivelse af ydelsen i henhold til databehandleraftale med dataansvarlige, i hele perioden 23. august 2023 til 22. august 2024, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

ExamCookie ApS´ ansvar
ExamCookie ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse, 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
Baker Tilly Denmark Godkendt Revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Revisors ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om ExamCookie ApS' 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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af ydelsen samt for kontrollernes udformning og funktionalitet. 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 fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet.

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

2. Uafhængig revisors erklæring (fortsat)

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

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

a) at beskrivelsen af ydelsen, således som denne var udformet og implementeret i hele perioden 23. august 2023 til 22. august 2024, i alle væsentlige henseender er retvisende, og
b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 23. august 2023 til 22. august 2024, og
c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret i hele perioden 23. august 2023 til 22. august 2024.

Beskrivelse af test af kontroller
De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår på side 13-28.

Tiltænkte brugere og formål
Denne erklæring og beskrivelsen af test af kontroller på side 13-28 er udelukkende tiltænkt dataansvarlige, der har anvendt ExamCookie ApS' ydelse, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 4. september 2024

Baker Tilly Denmark
Godkendt Revisionspartnerselskab
CVR-nr. 35 25 76 91

Michael Brink Larsen
statsautoriseret revisor
MNE-nr. mne23256

3. Beskrivelse af behandling

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at overholde de gældende eksamensregler udstedt af Undervisningsministeriet i eksamensbekendtgørelsen. Mere specifikt gøres dette ved, at den dataansvarlige kan anvende ExamCookie til at monitorere elever i tidsrummet for prøven, og i den forbindelse kan der forekomme behandling af personoplysninger.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om at kunne identificere samt sikre indsamlet data fra prøver gennem kryptering og pseudonymisering, således at den dataansvarlige kan gennemgå data, om nødvendigt, for at sikre, at den afholdte prøve er sket for elevens vedkommende uden brug af ikke tilladte hjælpemidler. Der anvendes fra databehandleren Microsoft Azure som underdatabehandler som beskrevet i de indgåede databehandleraftaler.

Personoplysninger

Data, der behandles af Databehandleren i ExamCookie, er elevdata tilknyttet den enkelte institution (den dataansvarlige) og kan opdeles i 2 kategorier:

Personoplysninger kategori A: Indsamlet data fra elevens computer gennem ExamCookie klienten.

Der indsamles under prøver, og udelukkende i den tidsramme prøven er angivet til, af uddannelsesinstitutionen. Disse opbevares i op til 1-3 måneder efter prøvedatoen, afhængig af den specifikke indgåede databehandleraftale, derefter bliver data automatisk slettet. Indsamlet data fra elevens computer er:

- Relevante skærmbilleder
- Procesliste
- Ny kopieret tekst og billeder i computerens clipboard
- Programmer anvendt i front på computeren
- URL-adresser anvendt under eksamen

Eksamensdata indsamlet fra klienten er pseudonymiseret, således data ikke kan tilkobles den konkrete person, data er indsamlet fra. Derudover er alt indsamlet data krypteret med en unik krypteringsnøgle.

3. Beskrivelse af behandling (fortsat)

Personoplysninger kategori B: Data indsamlet fra STIL, Tilslutning.stil.dk.

Der oprettes en tilslutningsaftale, mere specifikt en UNI-Sync mellem pakke, gennem tilslutning.stil.dk. Denne anvendes alene til at oprette og identificere den enkelte elev tilknyttet institutionen i ExamCookie, for at sikre der ikke indsamles data før eller efter prøvers tidsrum. Data indsamlet gennem tilslutningsaftalen er:

- Kursistens fulde navn
- Kursistens klasse samt eventuelle hold på institutionen
- Kursistens skole & årgang
- Kursistens eksamensplan
- Kursistens UNI-Login, bruger ID, til identificering af hver kursist som unik bruger (password er krypteret)
- Kursistens personnummer, hvor dette behandles under pseudonymisering og ikke er synligt i backenden
- Personoplysninger opbevares krypteret og pseudonymiseret som en ekstra sikkerhedsforanstaltning, hvor krypteringsnøgler (HASH nøglen) kun er tilgængelig for én betroet medarbejder i ExamCookie.

Data er opdelt i to kategorier, eksamensdata indsamlet fra klienten samt registreringsdata fra UNI-sync aftalen. Disse er krypteret med separate krypteringsnøgler. Alt data er krypteret både i 'in transmission', 'in rest' og 'in motion'. Data i klar tekst er derfor ikke tilgængelig for underdatabehandler, Microsoft Azure. Adgang til denne data kræver et login gennem 2-faktor-godkendelse, krypteringsnøglen (HASH nøglen) samt én specifik IP-adresse, hvor det kun er én betroet medarbejder, der har adgang til disse.

Praktisk tiltag

Direktionen i ExamCookie ApS, som er ansvarlig for IT-sikkerheden, sørger for, at der til stadighed er etableret procedurer og systemer, der understøtter overholdelsen af den til enhver tid gældende informations- og IT-sikkerhedspolitik, og at denne lever op til de krav, som er aftalt i de indgåede databehandleraftaler.

Tiltagene indenfor IT-sikkerhed omfatter både organisatoriske samt tekniske tiltag, eksempelvis:

- Procedurer til håndtering af ansættelser, fratrædelser og tildeling og inddragelse af rettigheder
- Fortrolighed og tavshedspligt for alle medarbejdere, partnere samt eventuelle freelancere / konsulenter er indgået før et samarbejde eller ansættelse kan starte
- Awareness-træning
- Databehandlerens medarbejdere arbejder udelukkende med den dataansvarliges systemer og data fra udstyr udleveret og administreret af databehandleren
- Udstyret er beskyttet af kryptering af harddisken, at brugerne ikke er lokal administrator og at databehandlerens sikkerhedsløsninger indeholdende antivirus, SecureDNS og automatiseret opdatering

3. Beskrivelse af behandling (fortsat)

- Fjernopkobling til databehandlerens systemer sker ved anvendelse af krypterede forbindelser og adgangen er beskyttet af 2-faktor sikkerhed
- I det omfang den dataansvarlige har tilladt fjernopkobling til den dataansvarliges systemer via databehandlerens standardløsning hertil, sker dette via krypterede forbindelser og med anvendelse af 2-faktor sikkerhed
- Databehandlerens centrale systemer er placeret i et ISAE3402 certificeret datacenter med sikringsforanstaltninger baseret på ISO27002 standarden, som bl.a. indeholder sikring mod strømsvigt, brand og overophedning
- Databehandleren har udarbejdet politikker for passwordsikkerhed og skærmlåse samt generel IT-sikkerhed, herunder sikker bortskaffelse af brugt udstyr
- Foranstaltningerne revurderes og kontrolleres efter en fast proces og er omfattet af revision og erklæring
- Databehandlerens lokationer er sikret fysisk med låse og alarmer.

Risikovurdering

ExamCookie ApS har vurderet og revurderer løbende den generelle risiko forbundet med persondatabehandlingen for de dataansvarlige som en del af en fast proces og fastlægger i samarbejde med de dataansvarlige de kontrolforanstaltninger, der er nødvendige for at beskytte de registreredes rettigheder via en afvejning af risici i forhold til de forholdsregler, der bliver truffet for at beskytte disse rettigheder.

Generelt vurderes risikoen for de registreredes rettigheder som lav, for så vidt angår den behandling ExamCookie ApS foretager henset til, at data opbevares sikkert hos underdatabehandler, der har foretaget de nødvendige tekniske og organisatoriske tiltag samt anskaffet diverse certificeringer. Ydermere sker persondatabehandling gennem kryptering og pseudonymisering og kan kun tilgås gennem 2-faktor-login.

Til trods for at risikoen generelt vurderes lav, opretholder ExamCookie ApS altid et sikkerhedsniveau, der efter ExamCookie ApS' vurdering som minimum kan understøtte en mellem risiko.

Kontrolforanstaltninger

De etablerede kontrolforanstaltninger tager udgangspunkt i ExamCookie ApS' informations- og IT-sikkerhedspolitik, hvor følgende hovedpunkter indgår:

- Risikovurdering og håndtering
- Informationssikkerhed
- Organisering af informationssikkerhed

3. Beskrivelse af behandling (fortsat)

- Informationssikkerhed
- Organisering af informationssikkerhed
- Styring af aktiver
- Medarbejdersikkerhed
- Adgangsstyring
- Kryptering
- Fysisk sikkerhed
- IT- og netværksdrift
- Anskaffelse, udvikling og vedligehold af systemer
- Styring af sikkerhedshændelser

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

Komplementerende kontroller hos de dataansvarlige

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

- Stillingtagen til dataminimering samt dataopbevaring. Der skal aktivt vælges opbevaringsperiode, som standard er 1 måned, men kan forlænges op til 3 måneder samt eventuelle fravalg for dataindsamling gennem klienten.

3. Beskrivelse af behandling (fortsat)

- Stillingtagen til dataminimering samt dataopbevaring. Der skal aktivt vælges opbevaringsperiode, som standard er 1 måned, men kan forlænges op til 3 måneder samt eventuelle fravalg for dataindsamling gennem klienten
- Sikre, at personoplysninger, indsendt data til tilslutning.stil.dk gennem de studieadministrative systemer, er ajourførte
- Opsætning og styring af egne brugere i ExamCookie, herunder eksamensansvarlige, IT-personale samt eventuelle lærere samt at brugerne er ajourførte
- Sikring af, at personfølsomme oplysninger ikke medsendes i eventuelle supportsager til ExamCookie ApS
- Stillingtagen og vurdering af eventuelle konsekvenser i relation til persondatabeskyttelse samt at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen

Stillingtagen til, at instruksen er lovlig, set i forhold til den til enhver tid gældende persondataretlige regulering.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Formål og omfang

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 – Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores test af kontrollernes design, funktionalitet og implementering har omfattet kontroller, som vi har vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte forhold jf. afsnit 4.3 er efterlevet i hele perioden 23. august 2023 til 22. august 2024. Yderligere kontrolmål- og aktiviteter hos tilsluttede virksomheder omfattes ikke af vores testhandlinger.

Forordningens krav og regler kan ikke fraviges, men forordningen skal omfatte og tage hensyn til formål, behandlingens karakter samt kategorien af personoplysninger mv. på alle niveauer, og den er som følge heraf af mere generel og overordnet karakter på flere områder. Implementeringen af sikkerheden kan således efter partnernes valg tilpasses til den enkelte aftale. Enkelte kundekontrakter kan således også have en rækkevidde, der går ud over databeskyttelsesforordningens eller databeskyttelseslovens almindelige krav. Sådanne yderligere krav er ikke omfattet af nedenstående.

4.2 Udførte testhandlinger

Vi har i forbindelse med udførelsen af tests af kontrolaktiviteter udført følgende handlinger:

Metode	Beskrivelse
Forespørgsler	Egnet personale er forespurgt om udførelsen af væsentlige kontrolaktiviteter.
Inspektion	De af kunden fastsatte procedurer, politikker samt dokumentation, er gennemgået og blevet taget stilling til, med henblik på at vurdere, hvorvidt de konkrete kontroller er designet og implementeret, så de må forventes at blive effektive. Vi har i de tekniske platforme, heri databaser, netværkskomponenter mv, testet den specifikke systemsætning, for at påse om hvorvidt kontrollerne er designet, implementeret og effektive. Dertil er det vurderet om hvorvidt kontrollerne er overvåget tilstrækkeligt samt i passende intervaller.
Observation	Observation af kontrollernes udførelse.
Genudførelse af kontrol	Vi har selv udført eller observeret en gentagen udførelse af kontrollen, med det formål at verificere, at kontrollen fungerer som antaget.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

4.3 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	Baker tillys udførte test	Resultat af test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Ingen anmærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på 2 behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Inspiceret ved en stikprøve på 2 databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Ingen anmærkninger.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen anmærkninger.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker tillys 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 firewall er konfigureret i henhold til intern politik herfor.	Ingen anmærkninger.
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.	Ingen anmærkninger.
B.6	Adgang til personoplysninger er isoleret til brugere med 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 brugeres 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 2 brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen anmærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Enheder • Systemer • Databaser	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at der ved en stikprøve på 2 alarmer er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	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. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret på erklæringstidspunktet. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger på erklæringstidspunktet, samt om de dataansvarlige er behørigt orienteret herom.	Ingen anmærkninger.

B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold:
	
	• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
	• Sikkerhedshændelser omfattende:
	  • Ændringer i logopsætninger, herunder de-aktivering af logning
	  • Ændringer i systemrettigheder til brugere
	  • Fejlede forsøg på log-on til systemer, databaser og netværk
	
	Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.
		Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs.
		
		Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.
		
		Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.
		
		Inspiceret ved en stikprøve på 1 dages logning, at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser.
		
		Inspiceret ved en stikprøve på 1 dages logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.
			Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker tillys 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 1 udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret. Inspiceret ved en stikprøve på 1 udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Ingen anmærkninger.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Ingen anmærkninger.
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.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved en stikprøve på 2 medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve på 1 fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt de-aktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte bruger-adgange.	Ingen anmærkninger.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen anmærkninger.
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.	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. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, på erklærings-tidspunktet.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
C.1	Databehandlerens ledelse har godkendt en skriftlig in-formationssikkerhedspolitik, 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.	Inspiceret, at der foreligger en informations-sikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at 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.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på 4 databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen anmærkninger.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af data-behandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på 1 databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af data-behandlerens procedurer for efterprøvning.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret ved en stikprøve på 1 nyansat medarbejder på erklæringstidspunktet, at den pågældende medarbejder har under-skrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på 1 nyansat medarbejder på erklæringstidspunktet, at den pågældende medarbejder er blevet in-troduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen anmærkninger.
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 medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på 1 fratrådt medarbejder på erklæringstidspunktet, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen anmærkninger.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	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 1 fratrådt medarbejder på erklæringstidspunktet, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen anmærkninger.
C.7	Der gennemføres løbende awareness-træning af data-behandlerens 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.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

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	Baker tillys udførte test	Resultat af test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen anmærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • *Dataejeren skal senest 30-90 dage inden Hovedaftalens ophør skriftligt meddele databehandler, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til dataejeren. I det tilfælde, hvor personoplysningerne tilbageleveres til dataejeren, skal databehandler ligeledes slette eventuelle kopier. Databehandler skal sikre, at eventuelle underdatabehandlere ligeledes efterlever dataejerens meddelelse.* • *Sletning af personoplysninger ved databehandleraftalens ophør.*	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på 4 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på 4 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte 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	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret ved en stikprøve på 1 ophørte databehandlinger på erklæringstidspunktet, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål E:

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

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den data-ansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret.	Ingen anmærkninger.
E.2	Databehandlerens databehandling inklusiv opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på 4 databehandlinger 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.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

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	Baker tillys udførte test	Resultat af test
F.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den data-ansvarlige. Der foretages løbende – og mindst en 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.	Ingen anmærkninger.
F.2	Databehandleren anvender alene underdatabe-handlere 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 2 underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	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 persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af data-behandlerens oversigt. Inspiceret ved en stikprøve på 2 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databe-handleraftalerne mellem de dataansvarlige og databehandleren.	Ingen anmærkninger.
F.5	Databehandleren har en oversigt over godkendte under-databehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.	Ingen anmærkninger.
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 revisions-erklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlings-sikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen anmærkninger

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

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	Baker tillys udførte test	Resultat af test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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. Inspiceret, at procedurerne er opdateret.	Ingen anmærkninger.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved en stikprøve på 2 dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Ingen anmærkninger.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på 2 dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandler-aftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Microsoft benyttes, som under-databehandler. Selskabet er registreret i EU – US Data Privacy Framework. Ingen øvrige anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

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	Baker tillys udførte test	Resultat af test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne 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.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen anmærkninger

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på per-sondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen anmærkninger.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af tilgang til personoplysninger	Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker tillys udførte test	Resultat af test
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden på erklæringstidspunktet Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 24 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen anmærkninger.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen anmærkninger.

Baker Tilly GDPR ansvarlig partner

Michael Brink Larsen
Partner, statsautoriseret revisor
+45 4041 5068
mbl@bakertilly.dk

Now, for tomorrow

Baker Tilly Denmark
Godkendt Revisionspartnerselskab

København
Poul Bundgaards Vej 1, 1. sal, 2500 Valby
T: +45 3345 1000

Sorø
Storgade 24A, 4180 Sorø
T: +45 3345 1000

Odense
Hjallesevej 126, 5230 Odense M.
T: +45 6613 0730

bakertilly.dk

PENNEO

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

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

Morten Claudius Jakobsen
Direktion
På vegne af: ExamCookie ApS
Serienummer: 0780c4c5-ce70-424b-8a1d-6b9d74dcf20d
IP: 45.10.xxx.xxx
2024-10-30 11:18:37 UTC

Mit ID

Michael Brink Larsen
BAKER TILLY DENMARK GODKENDT REVISIONSPARTNERSELSKAB CVR: 35257691
Statsautoriseret revisor
På vegne af: Baker Tilly Denmark Godkendt Revisionsp…
Serienummer: f0c28aad-9c66-4dd4-9020-15bb8d0b4494
IP: 80.209.xxx.xxx
2024-10-30 11:36:02 UTC

Mit ID