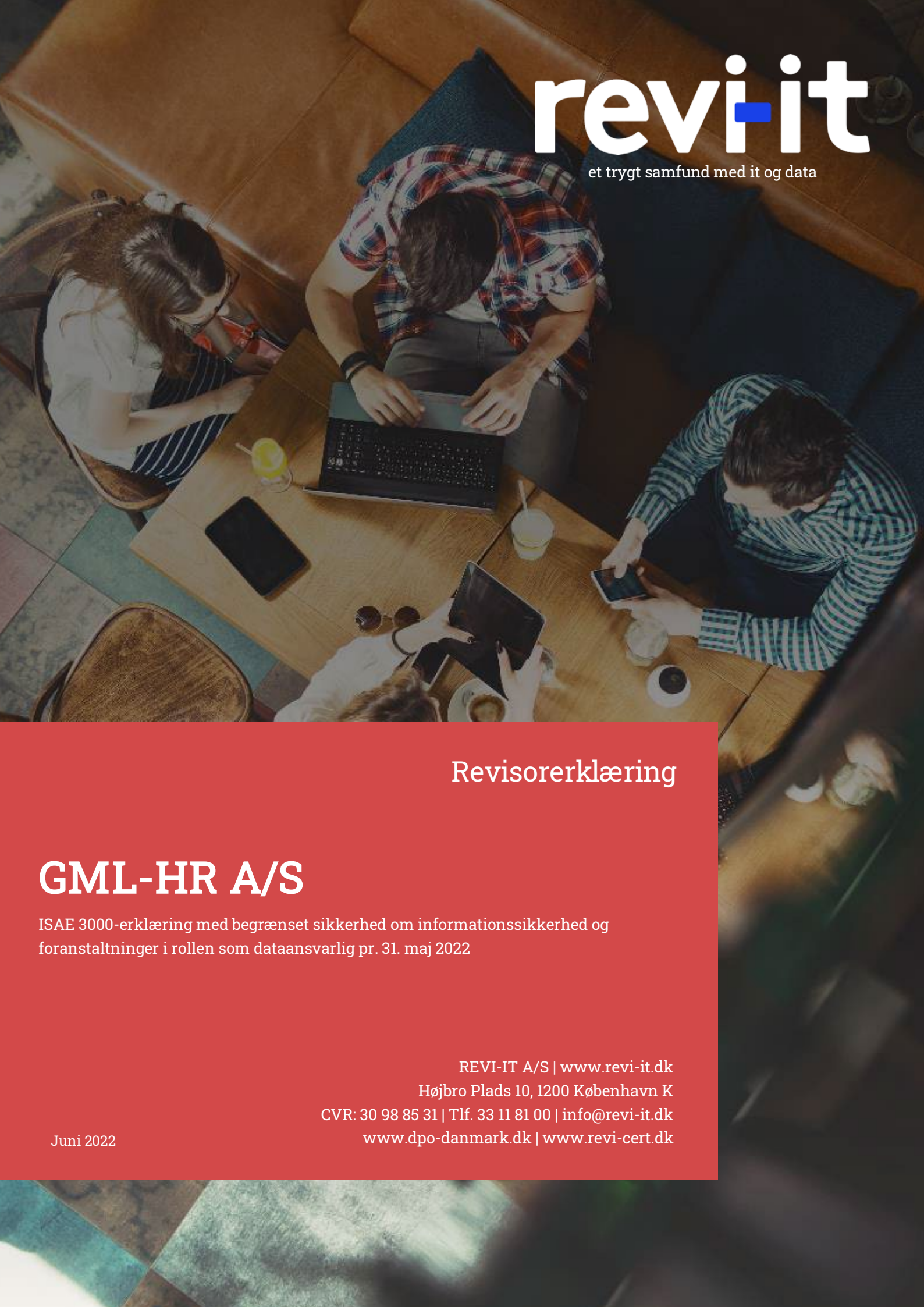

revi-it

et trygt samfund med it og data

Revisorerklæring

GML-HR A/S

ISAE 3000-erklæring med begrænset sikkerhed om informationssikkerhed og foranstaltninger i rollen som dataansvarlig pr. 31. maj 2022

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Juni 2022

Indholdsfortegnelse

Afsnit 1: GML-HR A/S' udtalelse

Erklæringen er udarbejdet til brug for GML-HR A/S' kunder, som har en tilstrækkelig forståelse til at vurdere beskrivelsen af test af kontroller sammen med anden information, herunder information om kontroller, som kunderne 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.

GML-HR A/S anvender underleverandørerne og underdatabehandlerne Dan Domain, DiscNordic, A&D Resources, Microsoft 365, Master samt Talentech ApS. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos GML-HR A/S' underleverandører og underdatabehandlere. Visse kontrolmål kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Test af kontroller omfatter ikke kontrolaktiviteter udført af underleverandører.

GML-HR A/S bekræfter, at:

a) Det medfølgende afsnit 3 om test af kontroller, giver en retvisende beskrivelse af, hvordan GML-HR A/S har behandlet personoplysninger pr. 31. maj 2022. Kriterierne anvendt for at give denne udtalelse var, at afsnit 3:

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

   - 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 kunder
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter kundens valg sker sletning eller tilbagelevering af alle personoplysninger til kunden, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, 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
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne HR-system til behandling af personoplysninger under hensyntagen til, at afsnit 4 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og derfor ikke kan omfatte ethvert aspekt ved HR-systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til kontrolmålene, var hensigtsmæssigt udformet og implementeret pr. 31. maj 2022, hvis relevante kontroller hos underleverandører var operationelt effektive pr. 31. maj 2022. Kriterierne anvendt for at give denne udtalelse var, at:

(i) De risici, der truede opnåelsen af kontrolmålene, var identificeret

(ii) De identificerede kontroller ville, hvis udført som beskrevet, give begrænset 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 relevante krav til dataansvarlige i henhold til databeskyttelsesforordningen.

Kolding, den 27. juni 2022
GML-HR A/S

Hanne Puggaard
Partner

Afsnit 2: Uafhængig revisors erklæring med begrænset grad af sikkerhed om informationssikkerhed og foranstaltninger i rollen som dataansvarlig pr. 31. maj 2022

Til GML-HR A/S

Omfang

Vi har fået til opgave at afgive erklæring om GML-HR A/S' HR-system i rollen som dataansvarlig pr. 31. maj 2022 og b) om udformningen og implementeringen af kontrolmålene.

GML-HR A/S anvender underleverandørerne og underdatabehandlerne Dan Domain, DiscNordic, A&D Resources, Microsoft 365, Master samt Talentech ApS. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos GML-HR A/S' underleverandører og underdatabehandlere. Visse kontrolmål kan kun nås, hvis underdatabehandlernes kontroller, der forudsættes i designet af GML-HR A/S ´ kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos GML-HR A/S.

Vores konklusion udtrykkes med begrænset sikkerhed.

GML-HR A/S' ansvar

GML-HR A/S er ansvarlig for udarbejdelsen af udtalelsen i "Afsnit 1", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen er præsenteret; for leveringen af de ydelser, afsnit 3 omfatter, for at anføre kontrolmålene samt for at udforme og implementere kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

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

REVI-IT A/S anvender international standard om kvalitetsstyring, ISQC 1[1] , og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og krav ifølge lovgivning og øvrig regulering.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om GML-HR A/S' udformning af kontroller, der knytter sig til de kontrolmål, der er anført i afsnit 3.

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 kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om udformningen af kontroller hos en dataansvarlig omfatter udførelse af handlinger for at opnå bevis for den dataansvarliges udformning af kontroller. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at afsnit 3 ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. Vores handlinger har omfattet test af implementeringen af sådanne kontroller, som vi anser for nødvendige for at give begrænset sikkerhed for, at kontrolmålene, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af egnetheden af de anførte mål samt egnetheden af de kriterier, som den dataansvarlige 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 dataansvarlig

GML-HR A/S' erklæring er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og omfatter derfor ikke nødvendigvis alle de aspekter ved HR-systemet, som hver enkelt kunder måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en dataansvarlig 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 dataansvarlig 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 HR-systemet, således som denne var udformet og implementeret pr. 31. maj 2022, ikke i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til kontrolmålene, ikke i alle væsentlige henseender var hensigtsmæssigt udformet pr. 31. maj 2022

Beskrivelse af test af kontroller

De specifikke kontroller, der blev vurderet (ved analyse og forespørgsel), samt arten og resultater af disse tests, fremgår i afsnit 3.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, afsnit 3, er udelukkende tiltænkt kunder, der har anvendt GML-HR A/S' HR-system som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som kunderne selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 27. juni 2022

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Basel Rimon Obari
Partner, CISA, CISM

Michael Marseen
Statsautoriseret revisor

Afsnit 3: Kontrolmål, kontrolaktivitet, vurdering og resultater heraf

Vores arbejde er udført i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores vurdering af funktionaliteten har omfattet de kontrolmål, der er udvalgt af ledelsen, og som fremgår af kontrolmålene nedenfor. Vores vurdering har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå begrænset sikkerhed for, at de anførte kontrolmål blev nået pr. 31. maj 2022.

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos GML-HR A/S' underleverandører og underdatabehandlere.

Vi har udført vores tests af kontroller hos GML-HR A/S via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos GML-HR A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Den registreredes rettigheder

Artikel	*GML-HR A/S' kontrolmål*	*REVI-IT A/S' udførte vurdering (ved analyse og forespørgsel)*	*Resultat af vurdering*
13 – Oplysningspligt ved indsamling af personoplysninger hos den registrerede	Der efterleves procedurer og kontroller, som sikrer, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer.	Vi har forespurgt til procedurer vedrørende oplysningspligt ved indsamling af personoplysninger hos den registrerede. Vi har inspiceret, at der foreligger en skabelon der sikrer oplysningspligten. Vi har inspiceret at der foreligger et årshjul der sikrer at de interne kontroller udføres jf. planen.	Ingen afvigelser konstateret.
12 + 15-20 – De registreredes rettigheder.	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til indsigt, sletning, dataeksport, berigtigelse og begrænsning i forhold til behandling af egne registrerede personoplysninger og behandlingen heraf er overholdt.	Vi har forespurgt til proceduren for de registreredes rettigheder. Vi har inspiceret, at der foreligger en procesbeskrivelse vedrørende persondatahenvendelser. Vi har inspiceret, at der foreligger en log til registrering af persondatahenvendelser. Vi har forespurgt hvordan persondatahenvendelser omkring sletning håndteres.	Ingen afvigelser konstateret.

Dataansvarlig og databehandler

Artikel	*GML-HR A/S' kontrolmål*	*REVI-IT A/S' udførte vurdering (ved analyse og forespørgsel)*	*Resultat af vurdering*
25 - Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.	Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse er implementeret gennem design og standardindstillinger i virksomhedens tekniske og organisatoriske sikringsforanstaltninger.	Vi har forespurgt til proceduren for databeskyttelse. Vi har forespurgt om der anvendes testdata.	Vi er blevet oplyst, at der ikke anvendes testdata, idet der ikke foretages udvikling på systemet. Ingen afvigelser konstateret.

Artikel	*GML-HR A/S' kontrolmål*	*REVI-IT A/S' udførte vurdering (ved analyse og forespørgsel)*	*Resultat af vurdering*
24 – Dataansvarlig. 28 – Databehandler. 29 - Behandling, der udføres for den dataansvarlige eller databehandleren.	Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, at databehandler har overholdt de tekniske og organisatoriske sikringsforanstaltninger, som er etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven, samt sikrer beskyttelse af den registreredes rettigheder, samt at behandling af personoplysninger er foretaget i overensstemmelse med den dataansvarliges instruks.	Vi har forespurgt til proceduren for behandling af personoplysninger sikrer at dette alene sker i henhold til en kontrakt eller databehandleraftale. Vi har stikprøvevis inspiceret at databehandleraftalerne er underskrevet og indeholder godkendelse af anvendte underleverandører. Vi har forespurgt til den løbende kontrol af at databehandler har overholdt tekniske og organisatoriske sikringsforanstaltninger. Vi har inspiceret, at der er foretaget tilsyn af underleverandører.	Ingen afvigelser konstateret.
30 - Fortegnelse over behandlingsaktiviteter.	Der foreligger hos den dataansvarlige en fortegnelse over kategorier af behandlingsaktiviteter.	Vi har inspiceret fortegnelsen over behandlingsaktiviteter og dataflow. Vi har inspiceret at fortegnelsen er godkendt og gennemgået i perioden.	Ingen afvigelser konstateret.
32 – Behandlingssikkerhed.	Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af, eller adgang til, personoplysninger.	Vi har forespurgt til proceduren for behandlingssikkerhed. Vi har inspiceret at risikovurderingen har fokus på konsekvenser for den registrerede. Vi har inspiceret informationssikkerhedspolitikken. Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere. Vi har stikprøvevis inspiceret, at brugeroprettelser følger proceduren. Vi har forespurgt til procedure for logning.	Ingen afvigelser konstateret.

Artikel	GML-HR A/S' kontrolmål	REVI-IT A/S' udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
		Vi har inspiceret at brugere med adgang til personoplysninger er begrænset til medarbejdere med et arbejdsbetinget behov. Vi har inspiceret, at der er foretaget gennemgang af brugere med adgang til personoplysninger, i perioden. Vi har stikprøvevis inspiceret, at logs indeholder ID, type af aktivitet samt et datostempel. Vi har stikprøvevis inspiceret, at der er opsat antivirus og at denne er opdateret. Vi har inspiceret dokumentation der viser, at der anvendes 2-faktor autentifikation. Vi har forespurgt hvordan persondatahenvendelser omkring sletning håndteres.	
33 - Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden. 34 - Underretning om brud på persondatasikkerheden til den registrerede.	Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden, samt underretning til de registrerede.	Vi har forespurgt til proceduren for håndtering af persondatasikkerhedsbrud. Vi har forespurgt om der har været nogen persondatasikkerhedsbrud i perioden.	Vi er blevet oplyst, at der ikke har været nogen persondatasikkerhedsbrud i perioden, hvorfor vi ikke har kunnet teste effektiviteten af kontrollen. Ingen afvigelser konstateret.

Overførsel af personoplysninger til tredjelande eller internationale organisationer			
Artikel	*GML-HR A/S' kontrolmål*	*REVI-IT A/S' udførte vurdering (ved analyse og forespørgsel)*	*Resultat af vurdering*
44 - Generelt princip for overførsel. 45 - Overførsel baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet. 46 - Overførsler omfattet af fornødne garantier. 47 - Bindende virksomhedsregler. 48 - Overførsel eller videregivelse uden hjemmel i EU-retten. 49 - Undtagelser i særlige situationer. 50 - Internationalt samarbejde om beskyttelse af personoplysninger.	Der efterleves procedurer og kontroller, som sikrer, at der alene sker overførsel af personoplysninger til et tredjeland eller en international organisation, hvis Kommissionen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation, har et tilstrækkeligt beskyttelsesniveau.	Vi har forespurgt til proceduren for overførsel til tredjelande. Vi har inspiceret at der foreligger et gyldigt overførselsgrundlag for anvendelse af en underleverandør med hosting i USA.	Ingen afvigelser konstateret.