Revisorerklæring

GML-HR A/S

ISAE 3000-erklæring med begrænset sikkerhed om informationssikkerhed og foranstaltninger i rollen som dataansvarlig pr. 12. marts 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

April 2024

Indholdsfortegnelse

Sektion 1: GML-HR A/S' udtalelse

Medfølgende udtalelse og erklæring er udarbejdet til brug for GML-HR A/S' kunder som har en tilstrækkelig forståelse til at vurdere testen 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 Talentech ApS, Master A/S, Summit A/S, Master A/S, Microsoft, DISCnordic, Mentor IT og DanDomain. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos GML-HR A/S' underleverandører og underdatabehandlere. Visse kontrolmål i sektion 3 kan kun nås, hvis underleverandørernes og underdatabehandlernes kontroller, der forudsættes i designet af vores kontroller, er passende designet og operationelt effektive. Sektion 3 omfatter ikke kontrolaktiviteter udført af underleverandører.

GML-HR A/S bekræfter, at:

a) Den medfølgende test af kontroller, Sektion 3, giver et retvisende billede af, hvordan GML-HR A/S har behandlet personoplysninger pr. 12. marts 2024. Kriterierne anvendt for at give denne udtalelse var, at Sektion 3:

   (i) Redegør for, hvordan GML-HR A/S' processer og kontroller relateret til databeskyttelse var designet 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 underleverandører.
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter kundens valg sker sletning eller tilbagelevering af alle personoplysninger til kunden, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at der kan foretages 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) er udarbejdet for at opfylde de almindelige behov til en bred kreds af kunder og derfor ikke kan omfatte ethvert aspekt ved HR-system Talent Recruiter, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i sektion 3, var passende designet og implementeret pr. 12. marts 2024, hvis relevante kontroller hos underdatabehandlere var operationelt effektive, som forudsættes i designet af GML-HR A/S pr. 12. marts 2024. Kriterierne anvendt for at give denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i Sektion 3, var identificeret, og

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

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde relevante krav i henhold til databeskyttelsesforordningen.

København, den 5. april 2024
GML-HR A/S

Hanne Puggaard
Partner

Sektion 2: Uafhængig revisors erklæring med begrænset sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler pr. 12. marts 2024

Til GML-HR A/S i rollen som dataansvarlig og GML-HR A/S' kunder

Omfang

Vi har fået som opgave at afgive erklæring om a) GML-HR A/S' i rollen som dataansvarlig pr. 12. marts 2024 og b) om udformningen og implementeringen af kontrolmålene.

GML-HR A/S anvender underleverandørerne og underdatabehandlerne Talentech ApS, Master A/S, Summit A/S, Master A/S, Microsoft, DISCnordic, Mentor IT og DanDomain. 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 operationelt effektive sammen med de relaterede kontroller hos GML-HR A/S.

Konklusion udtrykkes med begrænset sikkerhed.

GML-HR A/S' ansvar

GML-HR A/S er ansvarlig for udarbejdelsen af ledelsens udtalelse i Sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen er præsenteret; for leveringen af de ydelser, for at anføre kontrolmålene samt for designet og implementeringen af operationelt effektive kontroller for at opnå de anførte kontrolmål.

Grant Thorntons 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.

Grant Thornton 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.

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 Sektion 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 passende designet og implementeret.

En erklæringsopgave med sikkerhed om at afgive erklæring om designet og implementeringen 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 Sektion 3 ikke er retvisende, og at kontrollerne ikke er passende designet eller ikke implementeret. Vores handlinger har ved analyse og forespørgsel omfattet vurdering af implementeringen af sådanne kontroller, som vi anser for nødvendige for at give begrænset grad af sikkerhed for, at kontrolmålene blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af egnetheden af de heri anførte mål samt egnetheden af de kriterier, som er specificeret og beskrevet i Sektion 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 databehandler

Sektion 3 er udarbejdet for at opfylde de almindelige behov til en bred kreds af kunder og omfatter derfor ikke nødvendigvis alle de aspekter ved HR-system Talent Recruiter som hver enkelt kunde 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-system Talent Recruiter således som dette var udformet og implementeret pr. 12. marts 2024, ikke i alle væsentlige henseender er retvisende, og

(b) at kontrollerne hos GML-HR A/S som knytter sig til de kontrolmål, der er anført i sektion 3, ikke i alle væsentlige henseender var hensigtsmæssigt udformet pr.12. marts 2024

Beskrivelse af vurdering af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og vurdering af kontroller i det efterfølgende afsnit, Sektion 3, er udelukkende tiltænkt kunder, der har anvendt GML-HR A/S HR-system Talent Recruiter, 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 5. april 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Isabella Ørgaard Jensen
Director, CISA

Sektion 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 implementeringen har omfattet de kontrolmål og tilknyttede kontroller, 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. 12. marts 2024.

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

Vi har udført vores vurdering 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. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
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*	*Grant Thorntons 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 procedure 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

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

Artikel	*GML-HR A/S' kontrolmål*	*Grant Thorntons 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 om procedure for databeskyttelse. Vi har forespurgt om der anvendes testdata.	Vi er blevet informeret om, at der ikke anvendes testdata, hvorfor vi ikke har kunnet teste implementeringen af kontrollen. Ingen afvigelser konstateret.
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 inspiceret, at der foreligger en procedure, der indeholder krav om, at behandling af personoplysninger alene sker i henhold til kontrakt eller databehandleraftale. Vi har inspiceret at senest indgåede databehandleraftale er underskrevet og indeholder godkendelse af anvendte underdatabehandlere. Vi har forespurgt om hvorvidt den løbende kontrol af at databehandler har overholdt tekniske og organisatoriske sikringsforanstaltninger. Vi har inspiceret et eksempel på, at der er foretaget tilsyn af en underdatabehandler.	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.

Artikel	*GML-HR A/S' kontrolmål*	*Grant Thorntons vurdering (ved analyse og forespørgsel)*	*Resultat af vurdering*
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 procedure 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. 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. 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.	Ingen afvigelser konstateret.
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 om proceduren for håndtering af persondatasikkerhedsbrud. Vi har forespurgt om der har været nogen persondatasikkerhedsbrud.	Vi er blevet informeret om, at der ikke har været nogen persondatasikkerhedsbrud, hvorfor vi ikke har kunnet teste implementeringen af kontrollen. Ingen afvigelser konstateret.

Overførsel af personoplysninger til tredjelande eller internationale organisationer			
Artikel	*GML-HR A/S' kontrolmål*	*Grant Thorntons vurdering (ved forespørgsel og analyse)*	*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 underdatabehandler med hosting i USA.	Ingen afvigelser konstateret.

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."

Hanne Lynnerup
Underskriver 1
Serienummer: aa6e354e-4a37-4bc0-9e11-f73581888c60
IP: 85.191.xxx.xxx
2024-04-05 17:54:38 UTC

Isabella Ørgaard Jensen
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serienummer: 43ade1e0-a323-4e29-b02d-ffc8946d896b
IP: 77.241.xxx.xxx
2024-04-05 17:55:53 UTC

Jacob Helly Juell-Hansen
Underskriver 3
Serienummer: d606b7c0-b84a-4f0d-b549-9db5ea2e79c4
IP: 83.93.xxx.xxx
2024-04-06 04:57:06 UTC