Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af persondataforordningen (GDPR) pr. 25-05-2018

ISAE 3000-I

GML-HR A/S

CVR-nr.: 33 07 66 49

Maj 2018

Indholdsfortegnelse

GML-HR A/S' udtalelse

Denne erklæring vedrører GML-HR A/S' overholdelse af persondataforordningen (GDPR).

Pr. dags dato bekræfter vi, at vi, efter vores opfattelse, i al væsentlighed har overholdt ovennævnte kriterier, pr. dags dato, d. 25-05-2018.

Vi bekræfter herudover, at revisor har haft adgang til al information og materiale, som har været nødvendig for erklæringsafgivelsen.

På den baggrund er det vores vurdering, at vi, i al væsentlighed, har udført en hensigtsmæssig drift og administration for vores ydelser.

Kolding, 25. maj 2018

GML-HR A/S

Hanne Puggaard

Partner

Uafhængig revisors erklæring om overholdelse af persondataforordningen (GDPR) pr. 25-05-2018

Til GML-HR A/S' ledelse, selskabets kunder og disses revisorer

Vi har efter aftale undersøgt GML-HR A/S' overholdelse af persondataforordningen (GDPR) pr. dags dato, 25-05-2018.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er alene udarbejdet til brug for GML-HR A/S' ledelse, selskabets kunder og disses revisorer til vurdering af de tilrettelagte forretningsgange, og kan ikke anvendes til andre formål.

Ledelsens ansvar

Ledelsen i GML-HR A/S har ansvaret for at implementere og sikre opretholdelsen af forretningsgange som krævet af persondataforordningen (GDPR).

Revisors ansvar

Det er vores ansvar, på grundlag af det udførte arbejde, at udtrykke en konklusion om, hvorvidt selskabet overholder de krav, der er nævnt i persondataforordningen (GDPR).

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 høj grad af sikkerhed for vores konklusion.

REVI-IT A/S er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

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

Vores arbejde har omfattet forespørgsler, observationer samt vurdering og stikprøvevis undersøgelse af den information, vi har modtaget.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke afdækkes af vort arbejde. Endvidere vil en anvendelse af vor konklusion på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, ændring i kravene til behandling af oplysninger eller i selskabets overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion eventuelt ikke længere vil være gældende.

Konklusion

Denne konklusion er udformet på grundlag af forståelsen af de kriterier, som der er redegjort for i erklæringens indledende afsnit, og som bygger på kravene i persondataforordningen (GDPR).

Det er vores opfattelse, at GML-HR A/S, i alle væsentlige henseender, lever op til ovennævnte kriterier, pr. dags dato, 25-05-2018.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i det efterfølgende afsnit.

København, 25. maj 2018

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, CIPP/E, CRISC, adm. direktør

Kontrolmål, udførte kontroller, test og resultater heraf

Den følgende oversigt er udformet for at skabe et overblik over de kontroller, som GML-HR A/S har implementeret i henhold til overholdelse af persondataforordningen (GDPR). Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte artikler pr. 25-05-2018 er efterlevet.

De krav, som fremgår direkte af forordningen eller loven kan ikke fraviges. Derimod kan der justeres på, hvordan sikkerheden implementeres, da sikkerhedskravene i forordningen på flere punkter er af mere generel og overordnet karakter, som bl.a. skal tage hensyn til formål, behandlingens karakter, kategorien af personoplysninger mv. Herudover kan der være konkrete krav i de enkelte kundekontrakter, der kan have en rækkevidde, der går ud over persondataforordningens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos GML-HR A/S' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

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

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv udført – eller har observeret – en genudførelse af kontroller med henblik på at verificere, at kontrollen fungerer som forventet

2: Principper

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
5 - Principper for behandling af personoplysninger	Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.	Vi har forespurgt til dokumentation for indsamling, behandling og opbevaring af personoplysninger sker efter klare principper, og for at virksomheden løbende foretager kontrol af principperne.	Ingen væsentlige afvigelser konstateret.
6 - Lovlig behandling	Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.	Vi har forespurgt til dokumentation for, at behandling sker på et lovligt grundlag, og at virksomheden løbende udfører kontrol af, om behandling er sket på et lovligt grundlag.	Ingen væsentlige afvigelser konstateret.
7 - Betingelser for samtykke 8 - Betingelser for et barns samtykke i forbindelse med informationssamfundstjenester	Der efterleves procedurer og kontroller, som sikrer, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger.	Vi har forespurgt til dokumentation for, at når behandling er baseret på samtykke, at samtykket opfylder betingelserne for samtykke.	Ingen væsentlige afvigelser konstateret.
9 - Behandling af særlige kategorier af personoplysninger 10 - Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser	Der efterleves procedurer og kontroller, som sikrer, at behandling af særlige kategorier af personoplysninger alene sker under hensyntagen til fastlagte kriterier, betingelser og de fornødne garantier.	Vi har forespurgt til dokumentation for, at virksomheden har identificeret personoplysninger af særlig kategori. Vi har desuden sikret, at virksomheden har lovlig hjemmel til at behandle personoplysninger, og der løbende foretages kontrol af behandlingsgrundlaget.	Ingen væsentlige afvigelser konstateret.
11 - Behandling, der ikke kræver identifikation	Der efterleves procedurer og kontroller, som sikrer, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet.	Vi har forespurgt til dokumentation for, at virksomheden har procedurer for at sikre, at personoplysninger, som kun er påkrævet til identifikation af den registrerede, kun opbevares, så længe identifikation er påkrævet.	Ingen væsentlige afvigelser konstateret.

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
12 - Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder	Der efterleves procedurer og kontroller, som sikrer, at oplysninger om behandlingen af personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.	Vi har forespurgt til dokumentation for, at persondataanmodninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede, og at virksomheden løbende fører kontrol med dette.	Ingen væsentlige afvigelser konstateret.
	Der efterleves procedurer og kontroller, som sikrer, at udøvelsen af den registreredes rettigheder sker rettidigt, herunder besvarelse af den registreredes anmodninger og begrundelse for eventuelt afslag.	Vi har forespurgt til dokumentation for, at persondataanmodninger fra en registreret sker rettidigt og korrekt, og at virksomheden løbende fører kontrol med dette.	Ingen væsentlige afvigelser konstateret.
13 - Oplysningspligt ved indsamling af personoplysninger hos den registrerede 14 - Oplysningspligt, hvis personoplysninger ikke er indsamlet 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 dokumentation for, at virksomheden, når den indsamler oplysninger om den registrerede, giver den registrerede tilstrækkeligt med oplysninger til at opfylde oplysningspligten, og at virksomheden løbende fører kontrol med dette.	Ingen væsentlige afvigelser konstateret.
	Der efterleves procedurer og kontroller, som sikrer, at den registrerede har modtaget oplysning om retten til indsigt, berigtigelse eller sletning af personoplysninger samt begrænsning af behandlingen.	Vi har forespurgt til dokumentation for, at virksomheden løbene kontrollerer, at den registrerede er blevet oplyst om retten til indsigt, berigtigelse eller sletning af personoplysninger samt begrænsning af behandlingen, og at virksomheden fører løbende kontrol med dette.	Ingen væsentlige afvigelser konstateret.
15 - Den registreredes indsigtsret	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til indsigt i egne registrerede personoplysninger og behandlingen heraf er overholdt.	Vi har forespurgt til dokumentation for, at virksomheden har en skriftlig procedure for indsigtsanmodninger fra den registrerede, som løbende kontrolleres.	Ingen væsentlige afvigelser konstateret.
16 - Ret til berigtigelse 19 - Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til berigtigelse af egne registrerede personoplysninger er overholdt, herunder berigtigelse hos modtagere af personoplysningerne.	Vi har forespurgt til dokumentation for, at virksomheden har skriftlige procedurer for berigtigelse af personoplysninger, herunder underretning af databehandlere og modtagere af personoplysningerne, som løbende kontrolleres af virksomheden.	Ingen væsentlige afvigelser konstateret.

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
17 - Ret til sletning ("retten til at blive glemt") 19 - Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til sletning af egne registrerede personoplysninger er overholdt, herunder sletning hos modtagere af personoplysningerne.	Vi har forespurgt til dokumentation for, at virksomheden har skriftlige procedurer for sletning af personoplysninger, når virksomheden modtager en anmodning fra en registreret, og at databehandlere bliver underrettet om at slette persondata, samt dokumentation for, at proceduren løbende bliver kontrolleret.	Ingen væsentlige afvigelser konstateret.
18 - Ret til begrænsning af behandling 19 - Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til begrænsning af behandling af egne registrerede personoplysninger, er overholdt, herunder begrænsning hos modtagere af personoplysningerne.	Vi har forespurgt til dokumentation for, at virksomheden har skriftlige procedurer for begrænsning af personoplysninger, når virksomheden modtager en anmodning fra en registreret, og at databehandlere bliver underrettet om at begrænse persondata, samt dokumentation for, at proceduren løbende bliver kontrolleret.	Ingen væsentlige afvigelser konstateret.
20 - Ret til dataportabilitet	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til at overføre egne registrerede personoplysninger til en anden dataansvarlig, er overholdt.	Vi har forespurgt til dokumentation for, at virksomheden har skriftlige procedurer for dataportabilitet af personoplysninger, når virksomheden modtager en anmodning fra en registreret, og at databehandlere er forpligtet til at bistå virksomheden, samt dokumentation for, at virksomheden løbende fører kontrol med proceduren.	Ingen væsentlige afvigelser konstateret.
21 - Ret til indsigelse 22 - Automatiske individuelle afgørelser, herunder profilering	N/A – kravene er dækket af kontrolmålet i artikel 6.	Vi har desuden fået oplyst, at virksomheden ikke foretager automatisk profilering.	-
23 - Begrænsninger	N/A – området er ikke relevant i forhold til kontrolmål for en erklæring.	*Ikke relevant.*	-

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
24 - Den dataansvarliges ansvar	Der efterleves procedurer og kontroller, som sikrer, at dataansvarliges tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige.	Vi har forespurgt til dokumentation for, at virksomheden har udarbejdet procedurer og kontroller, som sikrer, at virksomhedens tekniske og organisatoriske foranstaltninger til sikring af den registreredes persondata, herunder rollefordeling, password-kontrol, logning af aktivitet osv., og at virksomheden løbende fører kontrol med dette.	Ingen væsentlige afvigelser konstateret.
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 dokumentation for, at virksomheden, under hensyn til det aktuelle tekniske niveau, har taget stilling til implementeringsomkostninger og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene. Desuden at virksomheden har taget stilling til og har implementeret databeskyttelse gennem design og databeskyttelse via standardindstillinger, og at disse løbende kontrolleres.	Ingen væsentlige afvigelser konstateret.
26 - Fælles dataansvarlige 27 - Repræsentanter for dataansvarlige og databehandlere, der ikke er etableret i Unionen	N/A – områderne er ikke relevante i forhold til kontrolmål for en erklæring	*Ikke relevant.*	-
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.	Vi har forespurgt til dokumentation for, at virksomheden har indgået databehandleraftaler med sine behandlere, og at disse aftaler lever op til forordningens krav til databehandlere, herunder underdatabehandlere, og disse løbende kontrolleres.	Ingen væsentlige afvigelser konstateret.
30 - Fortegnelse over behandlingsaktiviteter	Der efterleves procedurer og kontroller, som sikrer, at virksomheden fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.	Vi har forespurgt til dokumentation for, at virksomheden har udarbejdet en fortegnelse over alle behandlingsaktiviteter, og at fortegnelsen løbende bliver opdateret og kontrolleret.	Ingen væsentlige afvigelser konstateret.

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
31 - Samarbejde med tilsynsmyndigheden	N/A – området er ikke relevant i forhold til kontrolmål for en erklæring.	*Ikke relevant.*	-
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 dokumentation for, at virksomheden har udarbejdet nødvendige procedurer og tekniske foranstaltninger, herunder bl.a., sikring mod ændring, uautoriseret adgang til personoplysninger, aktivitetslog mv., som løbende kontrolleres af virksomheden.	Ingen væsentlige 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, hvis personoplysninger er omfattet af bruddet.	Vi har forespurgt til dokumentation for, at virksomheden har en procedure for anmeldelse af persondatasikkerhedsbrud til Datatilsynet, og at virksomheden også underretter de påvirkede registrerede, samt løbende fører kontrol med proceduren.	Ingen væsentlige afvigelser konstateret.
35 - Konsekvensanalyse vedrørende databeskyttelse	Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges konsekvensanalyse vedrørende databeskyttelse, inden der foretages behandling af personoplysninger, samt at der foretages en fornyet konsekvensanalyse ved ændring i den risiko, som behandlingsaktiviteterne udgør.	Vi har forespurgt til dokumentation for, at virksomheden har udarbejdet en konsekvensanalyse eller argumenter for ikke at udarbejde en analyse, som løbende kontrolleres.	Ingen væsentlige afvigelser konstateret.
36 - Forudgående høring	Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges høring hos tilsynsmyndigheden, såfremt konsekvensanalysen viser, at behandlingen af personoplysninger vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.	*Ikke relevant.*	-

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
37 - Databeskyttelsesrådgiver	Der efterleves procedurer og kontroller, som sikrer, at der - i de tilfælde, hvor det er krævet - er udpeget en databeskyttelsesrådgiver, som opfylder krav om tilstrækkelige kompetencer, og som er anmeldt til tilsynsmyndigheden.	*Ikke relevant - GML-HR er ikke underlagt krav om at have en DPO.*	-
38 - Databeskyttelsesrådgiverens stilling	Der efterleves procedurer og kontroller, som sikrer databeskyttelsesrådgiverens stilling, herunder at en databeskyttelsesrådgiver ikke modtager instrukser vedrørende udførelsen af dennes opgaver, samt at en databeskyttelsesrådgiver ikke udfører opgaver eller har andre pligter, som kan medføre interessekonflikt.	*Ikke relevant, idet GML-HR ikke har en DPO.*	-
39 - Databeskyttelsesrådgiverens opgaver	Der efterleves procedurer og kontroller, som sikrer, at databeskyttelsesrådgiveren er bekendt med omfanget af sine opgaver, inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger samt rapporterer direkte til ledelsen hos den dataansvarlige eller hos databehandleren.	*Ikke relevant, idet GML-HR ikke har en DPO.*	-
40 - Adfærdskodekser 41 - Kontrol af godkendte adfærdskodekser 42 - Certificering 43 - Certificeringsorganer	N/A – områderne er ikke relevante i forhold til kontrolmål for en erklæring.	*Ikke relevant.*	-

5: Overførsel af personoplysninger til tredjelande eller internationale organisationer

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
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 dokumentation for, at virksomhedens overførsel til tredjeland eller international organisation sker med lovlig hjemmel, og at virksomheden har indgået databehandleraftaler med databehandlere, som overfører persondata til tredjeland eller international organisation.	Ingen væsentlige afvigelser konstateret.