Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov
07-07-2018 til 31-05-2019

ISAE 3000

Lector ApS

CVR-nr.: 10 02 16 18

Juli 2019

Indholdsfortegnelse

Lector ApS' udtalelse

Denne erklæring vedrører Lector ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

Vi bekræfter, at vi, efter vores opfattelse, i al væsentlighed har overholdt ovennævnte kriterier for perioden 07-07-2018 til 31-05-2019.

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.

Charlottenlund, 5. juli 2019

Lector ApS

Tue Villum Sørensen
Adm. direktør

Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov

Til Lector ApS' ledelse, selskabets kunder og disses revisorer.

Omfang

Vi har efter aftale, for perioden 07-07-2018 til 31-05-2019, undersøgt Lector ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov i forbindelse med Lector ApS' generelle arbejdsgange for behandling af personoplysninger, og desuden understøttelsen af teknisk overensstemmelse for applikationerne TeamShare og ESS.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er alene udarbejdet til brug for Lector ApS' ledelse, selskabets kunder og disses revisorer til vurdering af de tilrettelagte forretningsgange, og kan ikke anvendes til andre formål end til de ovennævnte processer og leverancer.

Ledelsens ansvar

Ledelsen i Lector ApS har ansvaret for at implementere og sikre opretholdelsen af forretningsgange som krævet af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

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 databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

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 databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov**.**

Det er vores opfattelse, at Lector ApS, i alle væsentlige henseender, lever op til ovennævnte kriterier for perioden 07-07-2018 til 31-05-2019.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har været omfattet af Lector ApS' generelle arbejdsgange for behandling af personoplysninger og kunder der har anvendt applikationerne TeamShare og ESS, og deres revisorer, 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, 5. juli 2019

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 Lector ApS har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov. 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 for perioden 07-07-2018 til 31-05-2019 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 databeskyttelseslovens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos Lector ApS' 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 Lector ApS 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
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 håndtering af samtykke for brugere af systemerne, så skriftligt samtykke kan indhentes og efterfølgende dokumenteres, og vi har inspiceret de implementerede muligheder for TeamShare og ESS. Vi har forespurgt til overblik over hvilket samtykke der indgås, og vi har inspiceret loggen for TeamShare og ESS.	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, letilgængelig og forståelig form til den registrerede.	Vi har forespurgt til dokumentation for, at virksomheden skriftlige procedurer for håndtering af persondataanmodninger, og vi har inspiceret proceduren for persondataanmodninger. Yderligere har vi forespurgt til dokumentation for at proceduren, er blevet opdateret i perioden, og vi har inspiceret dokumentation for løbende opdatering af proceduren.	Ingen væsentlige afvigelser konstateret.

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
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 procedure for håndtering af retten til indsigt, og vi har inspiceret proceduren for håndtering af persondataanmodninger. Vi har forespurgt til periodisk opdatering af procedurerne, og vi har inspiceret dokumentation for periodisk vurdering, herunder ledelsesgodkendelse. Vi har forespurgt til dokumentation for, at virksomheden teknisk kan efterkomme de registreredes rettigheder i forhold til indsigt, og vi har inspiceret dokumentation for, at ovenstående kan gennemføres for TeamShare og ESS. Vi har forespurgt til håndtering af indsigtsanmodninger, og vi har stikprøvevis inspiceret dokumentation for håndteringen.	Vi har ikke haft mulighed for at teste proceduren, da vi har fået oplyst, at virksomheden ikke har haft anmodninger om indsigt i perioden. Ingen væsentlige afvigelser konstateret i øvrigt.
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 procedure for håndtering af retten til berigtigelse, og vi har inspiceret proceduren for håndtering af persondataanmodninger. Vi har forespurgt til periodisk opdatering af procedurerne, og vi har inspiceret dokumentation for periodisk vurdering, herunder ledelsesgodkendelse. Vi har forespurgt til dokumentation for, at virksomheden teknisk kan efterkomme de registreredes rettigheder i forhold til berigtigelse, og vi har inspiceret dokumentation for, at ovenstående kan gennemføres for TeamShare og ESS. Vi har forespurgt til håndtering af berigtigelsesanmodninger, og vi har stikprøvevis inspiceret dokumentation for håndteringen.	Vi har ikke haft mulighed for at teste proceduren, da vi har fået oplyst, at virksomheden ikke har haft anmodninger om berigtigelse i perioden. Ingen væsentlige afvigelser konstateret i øvrigt.

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 procedure for håndtering af retten til sletning, og vi har inspiceret proceduren for håndtering af persondataanmodninger. Vi har forespurgt til periodisk opdatering af procedurerne, og vi har inspiceret dokumentation for periodisk vurdering, herunder ledelsesgodkendelse. Vi har forespurgt til dokumentation for, at virksomheden teknisk kan efterkomme de registreredes rettigheder i forhold til sletning, og vi har inspiceret dokumentation for, at ovenstående kan gennemføres for TeamShare og ESS. Vi har forespurgt til håndtering af sletteanmodninger, og vi har stikprøvevis inspiceret dokumentation for håndteringen.	Vi har ikke haft mulighed for at teste proceduren, da vi har fået oplyst, at virksomheden ikke har haft anmodninger om sletning i perioden. Ingen væsentlige afvigelser konstateret i øvrigt.
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 procedure for håndtering af retten til begrænsning, og vi har inspiceret proceduren for håndtering af persondataanmodninger. Vi har forespurgt til periodisk opdatering af procedurerne, og vi har inspiceret dokumentation for periodisk vurdering, herunder ledelsesgodkendelse. Vi har forespurgt til dokumentation for, at virksomheden teknisk kan efterkomme de registreredes rettigheder i forhold til begrænsning, og vi har inspiceret dokumentation for, at ovenstående kan gennemføres for TeamShare og ESS. Vi har forespurgt til håndtering af begrænsningsanmodninger, og vi har stikprøvevis inspiceret dokumentation for håndteringen.	Vi har ikke haft mulighed for at teste proceduren, da vi har fået oplyst, at virksomheden ikke har haft anmodninger om begrænsning i perioden. Ingen væsentlige afvigelser konstateret i øvrigt.

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
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 procedure for håndtering af retten til dataportabilitet, og vi har inspiceret proceduren for håndtering af persondataanmodninger. Vi har forespurgt til periodisk opdatering af procedurerne, og vi har inspiceret dokumentation for periodisk vurdering, herunder ledelsesgodkendelse. Vi har forespurgt til dokumentation for, at virksomheden teknisk kan efterkomme de registreredes rettigheder i forhold til udtræk, og vi har inspiceret dokumentation for, at ovenstående kan gennemføres for TeamShare og ESS. Vi har forespurgt til håndtering af dataportabilitetsanmodninger, og vi har stikprøvevis inspiceret dokumentation for håndteringen.	Vi har ikke haft mulighed for at teste proceduren, da virksomheden ikke har haft anmodninger om dataportabilitet. Ingen væsentlige afvigelser konstateret i øvrigt.

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
24 - Den dataansvarliges ansvar	Der efterleves procedurer og kontroller, som sikrer, at tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige.	Vi har forespurgt til procedure, som sikrer, at virksomheden har implementeret tekniske og organisatoriske foranstaltninger til sikring af den registreredes persondata, herunder rollefordeling, password-kontrol, logning af aktivitet osv., og vi har inspiceret proceduren. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedurer, og vi har inspiceret kontrollen.	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, at virksomheden har taget stilling til og har implementeret databeskyttelse gennem design og databeskyttelse via standardindstillinger, samt at disse løbende kontrolleres, og vi har inspiceret kontroller herfor.	Ingen væsentlige afvigelser konstateret.

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
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 databehandlere, samt at disse aftaler lever op til forordningens krav til databehandlere, herunder underdatabehandlere, og vi har stikprøvevis inspiceret dokumentationen. Vi har forespurgt til periodisk kontrol for, at databehandleraftalerne er opdaterede, og vi har inspiceret kontrollen.	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 vi har inspiceret fortegnelsen. Vi har forespurgt til kontrol for, at fortegnelsen løbende opdateres og evalueres, og vi har inspiceret dokumentation for gennemgang i periode, samt tilhørende kontrol. Vi har forespurgt til ledelsesgodkendelse af fortegnelsen, og vi har inspiceret dokumentation for ledelsesgodkendelse.	Ingen væsentlige afvigelser konstateret.

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
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 kontrol for periodisk gennemgang af virksomhedens risikobillede og de dertilhørende tekniske og organisatoriske foranstaltninger, og vi har inspiceret kontrollen og den udarbejdede risikoanalyse. Vi har forespurgt til udarbejdelse af en informationssikkerhedspolitik, og vi har inspiceret informationssikkerhedspolitikken, samt dokumentation for ledelsens gennemgang i perioden. Vi har forespurgt til udarbejdelsen af nødvendige procedurer og tekniske foranstaltninger, herunder bl.a. sikring mod ændring, uautoriseret adgang til personoplysninger, aktivitets-log mv., og vi har inspiceret procedurerne. Vi har stikprøvevis inspiceret de implementerede tekniske og organisatoriske foranstaltninger på baggrund af ovenstående procedurer for TeamShare og ESS.	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 virksomhedens procedure for håndtering af persondatasikkerhedsbrud, og vi har inspiceret proceduren. Vi har forespurgt til periodisk gennemgang af proceduren, og vi har inspiceret kontrollen. Vi har forespurgt til sikkerhedsbrud i perioden, og vi har inspiceret dokumentation for håndtering af sikkerhedsbrudende.	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 ledelsens vurdering af nødvendigheden af at gennemføre egne konsekvensanalyser på hele eller dele af databehandlingen for den enkelte dataansvarlige, og vi har inspiceret vurderingen. Vi har forespurgt til kontrol for periodisk gennemgang af stillingtagen til behovet for udarbejdelse af en konsekvensanalyse, og vi har inspiceret kontrollen.	Vi har observeret, at virksomheden ikke er underlagt krav til udarbejdelse af en konsekvensanalyse. Ingen væsentlige afvigelser konstateret i øvrigt.

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.	Vi har forespurgt til dokumentation for ledelsens vurdering af nødvendigheden af at udpege en databeskyttelsesrådgiver, og vi har inspiceret vurderingen. Vi har forespurgt til periodisk kontrol for stillingtagen til nødvendigheden af at udpege en databeskyttelsesrådgiver.	Vi har konstateret, at virksomheden ikke er underlagt krav om at have en databeskyttelsesrådgiver. Ingen væsentlige afvigelser konstateret i øvrigt.

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 overførsel af personoplysninger til 3. lande, og vi har stikprøvevis inspiceret dokumentation for at data opbevares i EU.	Ingen væsentlige afvigelser konstateret.