Tilsynsrapport

Vedr. databehandleraftale med:
Blue Idea
Borgergade 2
8600 Silkeborg

14. november 2022

Indholdsfortegnelse

Ledelsens udtalelse

Blue Idea behandler personoplysninger på vegne dataansvarlige i henhold til databehandleraftale indgået mellem parterne.

Medfølgende beskrivelse og inspektionsrapport er udarbejdet til brug for den dataansvarlige, der har anvendt Blue Ideas platform, 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.

Blue Idea bekræfter, at nedenstående beskrivelse, giver en retvisende beskrivelse af Blue Idea, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i henhold til den indgåede databehandleraftale.

Vurdering

Blue Idea har vurderet en samlet lav risiko i forbindelse med behandlingen af personhenførbare data. Dette er vurderet ud fra at der er meget få, og kun almindelige, personoplysninger og oplysningerne er afgivet af den registrerede selv. Loginoplysninger er registreret af den dataansvarlige. Der registreres ikke følsomme eller fortrolige personoplysninger i systemet.

Inspektørens udtalelse

Omfang

Vi har fået som opgave at inspicere og rapporterer vedr. Blue Ideas beskrivelse af ydelsen i henhold til indgåede databehandleraftaler med kunder, pr. 14. november 2022 og om udformningen og funktionen af kontroller, der knytter sig til databehandleraftalen.

Inspektionen udføres for at sikre at databehandlingen efterlever de tekniske og organisatoriske sikkerhedsforanstaltninger der er angivet i databehandleraftalen samt databehandlerens generelle forpligtelser.

Ansvar og fremgangsmåde

Vores ansvar er at inspicere og rapportere Blue Ideas implementering af forhold der er beskrevet i databehandleraftalen, herunder generelle forpligtelser for databehandlere, tekniske sikkerhedsforanstaltninger og organisatoriske sikkerhedsforanstaltninger.

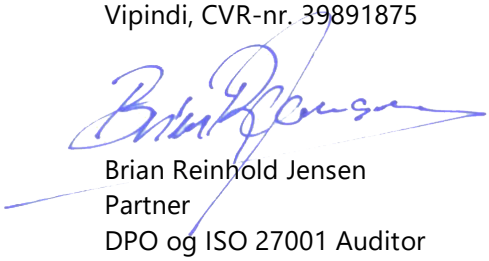
Metoder anvendt til test er beskrevet nedenfor:

Metode	**Overordnet beskrivelse**
Interview	Forespørgsel af udvalgt personale hos virksomheden vedr. kontroller.
Observation	Observation af, hvordan funktionen og kontrollen håndteres/udføres.
Inspektion	Gennemgang af dokumenter, rapporter og logs, der indeholder angivelser vedr. udførelsen af kontrollen. Det vurderes om funktionen overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrol	Vi har selv udført, eller har observeret, en genudførelse af kontroller med henblik på verifikation af kontrollen og at den fungerer som forventet.

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

Silkeborg den 14. november 2022

Vipindi, CVR-nr. 39891875



Brian Reinhold Jensen
Partner
DPO og ISO 27001 Auditor

Beskrivelse af behandling og omfang

Den Dataansvarlige anvender systemet SMS-Service, som ejes og administreres af Blue Idea, til at udsende SMS-beskeder.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige omhandler udelukkende almindelige personoplysninger.

Kategorier af personoplysninger

Almindelige personoplysninger, i form af Navn, E-mailadresse, adresse og telefonnummer.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Dataansvarliges medarbejdere
- Dataansvarliges kunder

Praktiske tiltag

Der er implementeret passende tekniske og organisatoriske foranstaltninger til at sikker behandling af personoplysninger.

Kontrolforanstaltninger

Der henvises til afsnittet "Kontrolaktivitet og resultat", hvor de konkrete kontrolaktiviteter er beskrevet.

Kontrolaktivitet og resultat

1. Generelle principper for databehandlere			
Nr.	Kontrolpunkt	Udført test	Resultat af test
1.1	Der er udarbejdet en fortegnelse over virksomhedens behandlingsaktiviteter i rollen som databehandler.	Inspiceret virksomhedens fortegnelse i rollen som databehandler.	Ingen væsentlige afvigelser konstateret.
1.2	Der er indgået underdatabehandleraftaler og føres årligt tilsyn med underdatabehandlere.	Inspiceret aftaler og kontrol med underdatabehandlere. Forespurgt til planlagte kontroller	Ingen væsentlige afvigelser konstateret. I perioden er implementeret nyt system til årshjul for GDPR-relaterede kontroller. Ikke alle planlagte kontroller er oprettet i systemet på tilsynsdagen.
1.3	Der er udarbejdet fortegnelse over dataansvarlige, til brug for information i tilfælde af brud på datasikkerheden.	Inspiceret oversigt over dataansvarlige og kontaktinformationer.	Ingen væsentlige afvigelser konstateret.
1.4	Der er udarbejdet intern instruks for underretning af dataansvarlige i tilfælde af brud på datasikkerheden.	Forespurgt, at der foreligger instruks for underretning af dataansvarlige i tilfælde af brud på datasikkerheden. Inspiceret, at dataansvarlige er underrettet i tilfælde hvor der har været databrud.	Ingen væsentlige afvigelser konstateret. Der har ikke været registrerede databrud i perioden.
1.5	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.	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 væsentlige afvigelser konstateret.
1.6	Databehandleren har foretaget en risikovurdering.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler	Ingen væsentlige afvigelser konstateret.

	Risikovurderingen opdateres jævnligt, or mindst en gang årligt.	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.	
1.7	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.	Ingen væsentlige afvigelser konstateret.

2. Tekniske sikkerhedsforanstaltninger			
Nr.	Kontrolpunkt	Udført test	Resultat af test
2.1	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, eller andre foranstaltninger der forhindrer afviklingen af skadevoldende kode. Antivirus opdateres løbende.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret på en computer via stikprøve	Ingen væsentlige afvigelser konstateret.
2.2	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.	Ingen væsentlige afvigelser konstateret.
2.3	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	Ingen væsentlige afvigelser konstateret.

		i overensstemmelse med deres arbejdsbetingede behov.	
2.4	Der anvendes krypteret forbindelse mellem klient og server	Inspiceret, at forbindelsen mellem klient og server er krypteret.	Ingen væsentlige afvigelser konstateret.
2.5	Adgangskoder opbevares krypteret	Inspiceret, at adgangskoder opbevares krypteret.	Ingen væsentlige afvigelser konstateret.
2.6	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.	Forespurgt, 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.	Ingen væsentlige afvigelser konstateret.
2.7	Der er fastlagt procedurer for sletning af dataansvarliges data, ved opsigelse/ophør af abonnement.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret ved en stikprøve på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen væsentlige afvigelser konstateret.

3. Organisatoriske sikkerhedsforanstaltninger			
Nr.	Kontrolpunkt	Udført test	Resultat af test
3.1	Der er udarbejdet forretningsgange for oprettelse og nedlæggelse af medarbejderes adgang til personoplysninger. Medarbejdernes adgang til, og arbejdsbetingede behov for, personoplysninger revurderes regelmæssigt.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af medarbejdernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Forespurgt til fratrædelser i perioden og tilhørende off-boarding procedure.	Ingen væsentlige afvigelser konstateret.
3.2	Der er udarbejdet databeskyttelsespolitik. Politikken er kommunikeret til medarbejderne.	Inspiceret personalehåndbogen. Forespurgt til procedurer for kommunikation til medarbejdere og årlige review af politikken.	Ingen væsentlige afvigelser konstateret.

	Politikken revurderes årligt.		
3.3	Alle medarbejdere er underlagt tavshedspligt. Tavshedspligten er også gældende efter medarbejderens fratrædelse. Alle medarbejdere er introduceret for databeskyttelsespolitikken.	Forespurgt ved en stikprøve på 1 nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Forespurgt ved en stikprøve på 1 nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen væsentlige afvigelser konstateret.
3.4	Ved fratrædelse er der implementeret processer, der sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Forespurgt til procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Forespurgt ved en stikprøve på 2 fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen væsentlige afvigelser konstateret.
3.5	Der gennemføres løbende awarenes-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awarenes-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 væsentlige afvigelser konstateret. Virksomheden har i perioden indført et onlinesystem til gennemførelse af awareness-aktiviteter.