Vipindi

Blue Idea

Inspektionsrapport vedr. databehandleraftale med Blue Ideas kunder

28. september 2020

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 de henførbare data. Dette er vurderet ud fra at der er meget få, og kun almindelige, henførbare personoplysninger og oplysningerne er afgivet af den registrerede selv. Loginoplysninger er registreret af den dataansvarlige. Der registreres ikke følsomme oplysninger 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. 28. september 2020 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

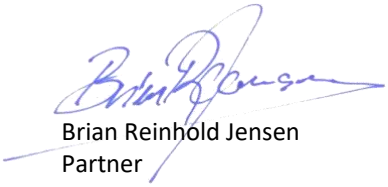
Vores ansvar er at inspicere og rapportere Blue Ideas implementering af forhold der er beskrevet i databehandleraftalen, herunder generelle forpligtelser for databehandlere, tekniske sikkerhedsforanstaltninger og organisatoriske sikkerhedsforanstaltninger.

Inspektionen omfatter bla. interviews, stikprøver og tests, og er udført med udgangspunkt i almindeligt accepterede metoder og politikker for interne audits.

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

Silkeborg den 28. september 2020

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 drejer sig primært almindelige personoplysninger.

Personoplysninger

Almindelige personoplysninger, herunder: Navn, E-mailadresse, adresse, telefonnummer.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Dataansvarliges medarbejdere.
- Dataansvarliges kunder og samarbejdspartnere.

Praktiske tiltag

Der er implementeret passende tekniske og organisatoriske foranstaltninger til at sikker behandling af person-oplysninger.

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 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 afvigelser konstateret. Der findes ikke log over udførte tilsyn, men ledelsen fremviste dokumentation for gennemført tilsyn i perioden.
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 afvigelser konstateret.
1.4	Der er udarbejdet intern instruks for underretning af dataansvarlige i tilfælde af brud på datasikkerheden.	Inspiceret instruks for underretning i forbindelse med databrud. Instruksen er en del af personalehåndbogen som alle medarbejdere er bekendte med.	Ingen afvigelser konstateret.
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 procedurer, for at behandling af personoplysninger udelukkende sker når der foreligger instruks.	Ingen afvigelser konstateret. (Indgåelse af databehandleraftale er en integreret del af kontraktindgåelsen, og der foreligger derfor ikke en særskilt instruks).
1.6	Databehandleren har foretaget en risikovurdering. Risikovurderingen opdateres jævnligt, og mindst en gang årligt.	Inspiceret risikovurdering og opdateringer.	Ingen afvigelser konstateret. Jf. risikovurderingen er der meget få personoplysninger opbevaret i systemet, hvorfor risikovurdering ikke foretages med fastlagte intervaller, men ved ændringer i behandling af personoplysninger.

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.	Inspiceret at antivirus er aktivt og opdateret på arbejdsstationer. Interviewet ledelsen vedr. serverkonfiguration der sikrer mod afvikling af skadevoldende kode.	Ingen afvigelser konstateret.

	Antivirus opdateres løbende.		
2.2	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall. Der er opdateret politik/instruks for konfiguration af firewall	Forespurgt til infrastruktur på hostingplatformen, herunder konfiguration af firewall og inspiceret tilhørende instrukser.	Ingen afvigelser konstateret.
2.3	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Interview af ledelsen vedr. håndtering af adgang til personoplysninger. Grundet organisationens størrelse varetager alle medarbejdere funktioner der kræver adgang til personoplysninger for at kunne servicere kunderene.	Ingen afvigelser konstateret. (Det er noteret at alle medarbejdere har arbejdsbetinget behov for adgang.)
2.4	Der anvendes krypteret forbindelse mellem klient og server	Inspiceret at adgang til dk.sms-service.dk sker med krypteret forbindelse.	Ingen afvigelser konstateret.
2.5	Adgangskoder opbevares krypteret	Inspiceret at adgangskoder er krypteret i databasen.	Ingen afvigelser konstateret.
2.6	Driftsmiljøet er adskilt fra udviklings- og testmiljøer	Forespurgt til adskillelse af drifts og udviklings-/testmiljøer.	Ingen afvigelser konstateret.
2.7	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form.	Forespurgt til pseudonymisering/anonymisering af data til test og lignende.	Ingen afvigelser konstateret. I forbindelse med test af dataudveksling med operatører hentes "live-data" fra operatørernes databaser.

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.	Forespurgt at der foreligger procedurer for oprettelse og nedlæggelse af brugernes adgang til systemer. Forespurgt at medarbejderes adgange til systemer, er godkendt, og at der er et arbejdsbetinget behov. Forespurgt at fratrådte medarbejderes brugerkonti er deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret. Ingen afvigelser konstateret. Ingen afvigelser konstateret. Der findes ikke log over udførte kontroller med tildelte brugeradgange. Jf. pkt. 2.3, har alle aktive ansatte arbejdsbetinget behov for adgang til personoplysningerne.

3.2	Der er fastlagt procedurer for sletning af dataansvarliges data, ved opsigelse/ophør af abonnement.	Inspiceret at procedurer for sletning af dataansvarliges data er aftalt i standardkontrakterne.	Ingen afvigelser konstateret
3.4	Der er udarbejdet databeskyttelsespolitik. Politikken er kommunikeret til medarbejderne. Politikken revurderes årligt.	Inspiceret at der er udarbejdet databeskyttelsespolitik. Forespurgt til medarbejdernes kendskab til politikken. Inspiceret at politikken gennemgås	Ingen afvigelse konstateret Politiken er indeholdt i personalehåndbogen. Der er ikke udarbejdet procedurer for review af politikken, men det blev konstateret at personalehåndbogen er gennemgået og tilrettet jævnligt i de seneste 12 måneder.
3.5	Alle medarbejdere er underlagt tavshedspligt. Tavshedspligten er også gældende efter medarbejderens fratrædelse.	Inspiceret virksomhedens fortrolighedserklæring, der indgås med alle medarbejdere.	Ingen afvigelser konstateret.
3.6	Ved fratrædelse er der implementeret processer, der sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Forespurgt til procedurer for inddragelse af brugerens adgange efter fratrædelse.	Ingen afvigelser konstateret. Alle adgange styres via AD
3.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Forespurgt til gennemførelse af løbende awareness-træning. Det oplyses at træningen gennemføres løbende på personalemøder.	Der føres ikke log over gennemført træning, men ledelsen oplyste om at der fremadrettet vil blive ført referat fra møderne hvor træningen bliver dokumenteret.