iVISION

Inspektionsrapport vedr. databehandleraftale med iVISIONs kunder

31. oktober 2020

Indholdsfortegnelse

Ledelsens udtalelse

iVISION 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 iVISIONs 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.

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

Vurdering

iVISION har vurderet en samlet middel risiko i forbindelse med behandlingen af de henførbare data. Dette er vurderet ud fra at der er få, men muligvis fortrolige (og i sjældne tilfælde følsomme) oplysninger noteret i den dataansvarliges sager.

Inspektørens udtalelse

Omfang

Vi har fået som opgave at inspicere og rapporterer vedr. iVISIONs beskrivelse af ydelsen i henhold til indgåede databehandleraftaler med kunder, pr. 31. oktober 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

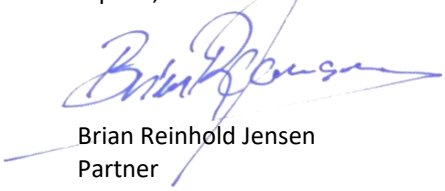
Vores ansvar er at inspicere og rapportere iVISIONs implementering af forhold der er beskrevet i databehandleraftalen, herunder generelle forpligtelser for databehandlere, tekniske sikkerhedsforanstaltninger og organisatoriske sikkerhedsforanstaltninger.

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

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

Silkeborg den 31. oktober 2020

Vipindi, CVR-nr. 39891875



Brian Reinhold Jensen
Partner
DPO og ISO 27001 Auditor

Beskrivelse af behandling og omfang

Den Dataansvarlige anvender systemet Legis 365, som ejes og administreres af iVISION eller underdatabehandlere, til sags- og dokumenthåndtering.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om registreringer i forbindelse med håndtering af sager for den dataansvarliges klienter.

Personoplysninger

Almindelige personoplysninger, herunder: Navn, E-mailadresse, uddannelse og erhverv.

Fortrolige og følsomme oplysninger relateret til den dataansvarliges klienter.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- medarbejdere hos Dataansvarlig
- Dataansvarliges kunder/klienter

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 føres årligt tilsyn med underdatabehandlere.	Inspiceret listen over underdatabehandlere og tilhørende underdatabehandlere. Forespurgt til udførte tilsyn med underdatabehandlere.	Ingen væsentlige afvigelser konstateret Der findes ikke log over udførte tilsyn, men ledelsen foreviste dokumentation for fremtidige, planlagte og regelmæssige, tilsyn.
1.2	Der er udarbejdet fortegnelse over dataansvarlige, til brug for information i tilfælde af brud på datasikkerheden.	Inspiceret fortegnelsen over dataansvarlige	Ingen afvigelser konstateret
1.3	Der er udarbejdet intern instruks for underretning af dataansvarlige i tilfælde af brud på datasikkerheden.	Inspiceret den interne instruks for håndtering (og underretning) af databrud.	Ingen afvigelser konstateret
1.4	Alle medarbejdere er instrueret i beskyttelsen af personoplysninger	Interview med ledelsen og inspektion af interne instrukser.	Ingen afvigelser konstateret

2. Tekniske sikkerhedsforanstaltninger			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
2.1	SSL krypteret forbindelse mellem klient og server. (Extended Validation)	Inspiceret ssl-kryptering af forbindelse og kontrolleret certifikat.	Ingen afvigelser konstateret
2.2	Adgangskode opbevares krypteret	Inspiceret at passwords opbevares krypteret i databasen.	Ingen afvigelser konstateret
2.3	Driftsmiljø er adskilt fra udviklings- og testmiljøer	Inspiceret at databaser for drifts-, udviklings- og testmiljøer er adskilte	Ingen afvigelser konstateret
2.4	Al data i systemet behandles og opbevares på to seperate lokationer inden for EU i Vest- og Nordeuropa.	Inspiceret konfiguration af hostingmiljø.	Ingen afvigelser konstateret
2.5	Der er etableret dokumenterede backuprutiner.	Inspiceret backuprutinerne og tilhørende dokumentation.	Ingen afvigelser konstateret
2.6	Kundedata slettes 3 måneder efter aftalens ophør.	Inspiceret slettepolitik og procedurer vedr. kundedata.	Ingen væsentlige afvigelser konstateret. Det blev konstateret at der i enkelte tilfælde blev opbevaret data i længere tid end de tre måneder. Primært efter kundens ønske i forbindelse med test af andet system.

2.7	Der føres log over login og loginforsøg på platformen	Inspiceret log over login og loginforsøg.	Ingen afvigelser konstateret. Systemet er bygget så den dataansvarlige selv har adgang til loggen fra systemet.

4. Organisatoriske sikkerhedsforanstaltninger			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
4.1	Adgang til personoplysninger er begrænset til få nøglepersoner	Inspiceret opsætning af rettigheder vedr. adgang til personoplysninger.	Ingen afvigelser konstateret.
4.2	Der er fastlagt interne procedurer for håndtering af sikkerhedsbrud	Inspiceret instruks for brud på datasikkerhed.	Ingen afvigelser konstateret.
4.3	Alle medarbejdere har tavshedspligt og har underskrevet fortrolighedserklæringer.	Inspiceret standardaftalen for medarbejdere, vedr. fortrolighed og hemmeligholdelse.	Ingen afvigelser konstateret.

5. Fysiske sikkerhedsforanstaltninger			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
5.1	Kontorer og bygninger aflåses, når de forlades	Inspiceret medarbejderinstruks vedr. aflåsning af kontorer.	Ingen afvigelser konstateret.