# Figlo Beveiligings-maatregelen

Versie 1-7-2017

## Figlo Beveiligingsmaatregelen

Figlo kent voor zijn SAAS-dienstverlening als leverancier en als verwerker van persoonsgegevens een aantal (wettelijke) verantwoordelijkheden met betrekking tot de beveiliging van klantdata. Eén van die verantwoordelijkheden is het adequaat beveiligen van die data. Met dit document wil Figlo een overzicht geven van de beveiligingsmaatregelen die genomen zijn.

Voor de beveiliging van de applicatie Figlo Advisor gehost bij Microsoft Azure zijn de volgende beveiligingsmaatregen van toepassing:

- Voor de ontwikkeling en implementatie van de Software is een zogenaamde OTAP-straat ingericht. Dit houdt in dat de software alvorens in productie wordt genomen een strikt traject volgt met verschillende fases zodat de kwaliteit van de ontwikkelde software gewaarborgd wordt. De fase zijn ‘Ontwikkeling’, ‘Test’, ‘Acceptatie’ en ‘Productie’.
- Toegangsrechten van de Figlo applicatie en systemen zijn beschreven en via protocollen gedefinieerd en gewaarborgd;
- De software van Figlo wordt jaarlijks op inherente veiligheid getest door een externe deskundige partij. Deze externe deskundige test de software op beveiligingskwetsbaarheden doormiddel van een ‘hackerstest’, ‘penetratietesten’ ‘code review’ en een algemene ‘Vulnerability assessment’ op applicatie én systeem.
- De hosting van de applicatie in de cloud wordt verzorgd door Microsoft Azure die ISO 27001, HIPAA, FedRAMP, SOC 1 en SOC 2 gecertificeerd zijn.
- (Persoons)gegevens worden alleen binnen Europese Vrije Ruimte verwerkt.
- Toegang tot data is alleen mogelijk via een geldige sessie. Opzetten van een sessie is alleen mogelijk met geldig username/password.
- Wachtwoorden zijn ‘gehashed’ en versleuteld in de database opgeslagen.
- Wachtwoorden worden via ‘one way hashing’ gecontroleerd op correctheid.
- Al het verkeer tussen front-end en backend is beveiligd met een beveiligde verbinding door middel van HTTPS met geldig SSL-certificaat.
- Een SQL-database Firewall en Firewall op server niveau is geïnstalleerd.
- Database en applicatie zijn redundant uitgevoerd.
- Er is een back-up beleid waarin is vastgelegd dat er een dagelijkse back-up wordt gemaakt van alle klantgegevens;
- De gegevens van een klant is logisch gescheiden van gegevens van andere klanten. Het is onmogelijk om vanuit organisatie A, klantgegevens te kunnen bekijken van organisatie B.
- Alle data die ge-exporteert worden vanuit de Productieomgeving is altijd geanonimiseerd.