**Onderbouwing AVG en OWASP**

Om te voldoen aan de eisen van de **AVG (Algemene Verordening Gegevensbescherming)** en de beveiligingsrichtlijnen van de **OWASP Top 10**, zijn in de ontwikkeling van deze applicatie de volgende maatregelen genomen:

**Privacy (AVG)**

* De applicatie verwerkt alleen de strikt noodzakelijke gegevens, zoals naam, e-mailadres (voor inloggen) en quizresultaten.
* Wachtwoorden worden veilig opgeslagen via Laravel’s ingebouwde hashingfunctie (bcrypt).
* Alleen geautoriseerde gebruikers (admins) kunnen beheertaken uitvoeren. Dit is geregeld via middleware en rollen.
* Er worden geen gegevens gedeeld met externe partijen en alle gebruikersdata blijft binnen het systeem.
* Gegevens die niet meer nodig zijn worden verwijderd of geanonimiseerd.

**Beveiliging (OWASP Top 10)**

* **SQL-injectie wordt voorkomen** door gebruik te maken van Laravel’s Eloquent ORM en Query Builder.
* **Cross-Site Scripting (XSS)** wordt voorkomen doordat alle dynamische inhoud in Blade automatisch wordt ontsnapt met {{ }}.
* **Cross-Site Request Forgery (CSRF)** wordt afgevangen door Laravel’s ingebouwde CSRF-bescherming (@csrf token in forms).
* **Authenticatie en autorisatie** worden gecontroleerd via Laravel’s Auth-systeem en middleware.
* Foutmeldingen en validatiefeedback geven **geen gevoelige informatie prijs**.
* Alle gebruikersinvoer wordt gevalideerd op de server met Laravel Form Requests of validate()-methoden.

Deze maatregelen zorgen ervoor dat de applicatie veilig en privacybewust is opgezet en voldoet aan zowel de AVG als de OWASP-veiligheidsrichtlijnen.