

Slimme bril voor in de zorg

Als het gaat om **gebruik in de zorg**, dan zijn er spelregels voor slimme brillen. Waar bij consumentenstijlen vooral wordt gekeken naar design en batterijduur, draait het in de zorg voor 100% om **privacy (AVG/GDPR)**, **informatiebeveiliging (NEN 7510)** en **medische wetgeving**.

In de zorg verwerk je namelijk *bijzondere persoonsgegevens* (medische data en videobeelden van patiënten). Een misstap op het gebied van privacy kan direct leiden tot forse boetes van de Autoriteit Persoonsgegevens en tuchtrechtelijke problemen.

Welke brillen zijn absoluut NIET geschikt voor de zorg?

- **Consumentenbrillen (zoals de Ray-Ban Meta of Google Glass):**
Deze zijn **volledig ongeschikt** voor de zorg. De data stroomt vaak via Amerikaanse servers (Meta/Google), er kan geen AVG-verwerkersovereenkomst worden afgesloten en de data kan gebruikt worden voor het trainen van commerciële AI-modellen.

Wat is de BROWSER / PRIVACY-norm voor de zorg in Europa?

Voor een privacy-bestendige inzet in de Europese en Nederlandse zorg geldt dat **de hardware en de software gescheiden moeten worden beoordeeld**.

Een goede 'zorg-smart-glass' bestaat uit twee delen:

1. **Neutrale Enterprise Hardware** (geen consumentenmerk)
2. **Gecertificeerde Europese Zorgsoftware**

1. Welke Hardware is het beste qua privacy?

In de zorg wil je hardware die géén eigen consumenten-ecosysteem afdwingt en waarin je de camera en microfoon volledig onder controle hebt. De meest gebruikte en privacy-veilige hardware-opties in de Europese zorg zijn:

- **Vuzix (bijv. Vuzix M400 / M4000):** Erg populair in Nederlandse ziekenhuizen en de thuiszorg (bijv. bij wondzorg op afstand). Werkt op een afgeschermd Android-omgeving zonder Google Play Services.
- **RealWear (bijv. RealWear Navigator):** Robuust, veel gebruikt door maatschappen en medisch specialisten. De bril is volledig handsfree via spraak te bedienen en slaat lokaal niets op als dat niet mag.

2. Welke Software maakt het AVG-proof?

De bril zelf is slechts een camera en scherm; **de software bepaalt de privacy**. Om aan de AVG en de NEN 7510 te voldoen, moet de software-leverancier aan de volgende eisen voldoen:

- **Opslag in de EU:** De videostream of data mag Europa niet verlaten (geen Amerikaanse cloud servers i.v.m. de US Cloud Act).
- **NEN 7510 / ISO 27001 certificering:** De softwareleverancier moet aantoonbaar gecertificeerd zijn voor de Nederlandse zorg.
- **End-to-End Encrypted (E2EE):** Beelden van een operatie of wondbehandeling mogen alleen gestreamd worden naar de geautoriseerde arts/collega en mogen niet onbeveiligd worden opgeslagen.
- **Verwerkersovereenkomst:** De leverancier moet een medische verwerkersovereenkomst willen tekenen.

Veelgebruikte privacy-proof softwarecombinaties in NL:

Nederlandse zorginstellingen werken voor meekijken op afstand vaak met gespecialiseerde software zoals **Gemvision**, **1P8** of **Rods&Cones**. Deze software draait op de Vuzix- of RealWear-brillen en zorgt voor een AVG-veilige verbinding direct met het netwerk van het ziekenhuis of de thuiszorgorganisatie.

Waar moet je in de praktijk op letten (Privacy-checklist voor de zorg)?

1. **Toestemming van de patiënt (WGBO / AVG):** De patiënt moet (mondeling of schriftelijk) toestemming geven voordat de camera aangaat.
2. **Privacy van derden (omstanders):** Zorg dat de bril een duidelijk zichtbaar LED-lampje heeft dat brandt als de camera actief is, zodat collega's of bezoekers weten dat er gestreamd wordt.
3. **Geen lokale opslag:** Zorg dat foto's of video's nooit op het interne geheugen van de bril zelf blijven staan, maar direct via de beveiligde verbinding naar het EPD (Elektronisch Patiëntendossier) gaan of na de stream verdwijnen.

Conclusie: Kies voor de zorg **geen** bekend consumentenmerk, maar combineer een **Vuzix** of **RealWear** bril met een **gecertificeerde Nederlandse/Europese zorg-softwarepartner**. Dat is de enige manier om juridisch en ethisch veilig te werken.