

EU-verklaring van overeenstemming

Nederlands: EU-conformiteitsverklaring

Fabrikant	Eagle Software Consultancy B.V.
Adres	Kanteklaarpad 11, 3813 KR Amersfoort, Nederland
KVK-nummer	98050516
E-mail	info@eaglesc.nl
Website	www.eaglesc.nl

verklaart onder eigen verantwoordelijkheid dat onderstaand product voldoet aan de eisen van de hieronder genoemde EU-wetgeving:

Productnaam	Garbi Sein
Model	Garbi Sein v1
Productomschrijving	Wifi-verbonden notificatielampje dat, op basis van het ophaalschema van de door de gebruiker gekozen afvalinzamelaar, aangeeft welke afvalcontainer aan de straat gezet moet worden
Apparaat-identificatie	Elk exemplaar heeft een uniek 6-cijferig hexadecimaal apparaat-ID (afgeleid van het wifi-MAC-adres), zichtbaar op de statuspagina van het apparaat en gebruikt in de netwerknaam (<code>garbi-sein-XXXXXX</code>)

Toegepaste regelgeving

Cyber Resilience Act (Verordening (EU) 2024/2847)

Dit product is een "product met digitale elementen" in de zin van de Cyber Resilience Act (hierna: CRA) en valt, op basis van eigen beoordeling door de fabrikant, in de **standaardcategorie** (geen "belangrijk" of "kritiek" product in de zin van Bijlage III/IV) - het apparaat heeft geen beveiligings-, toegangscontrole- of infrastructuurfunctie. Op deze categorie is de interne-controleprocedure (Bijlage VIII, Module A) van toepassing: zelfbeoordeling door de fabrikant, zonder tussenkomst van een aangemelde instantie.

De fabrikant verklaart dat het product voldoet aan de essentiële eisen van **Bijlage I** van de CRA, met name:

- Het product wordt geleverd zonder bekende, exploiteerbare kwetsbaarheden op het moment van op de markt brengen.
- Het product wordt standaard met een veilige configuratie geleverd; waar een instelling niet standaard beveiligd kan worden ingesteld (zie de publieke samenvatting van de risicobeoordeling), is dit een bewuste, gedocumenteerde afweging met een zichtbare aanwijzing aan de gebruiker om dit zelf in te stellen.
- Toegang tot de instellingenpagina van het apparaat wordt beschermd door authenticatie (gebruikersnaam/wachtwoord, met gezouten en gehashte wachtwoordopslag) en CSRF-bescherming op alle statuswijzigende acties.
- Vertrouwelijkheid en integriteit van gegevens in transit worden beschermd door TLS met certificaatvalidatie tegen een vaste, gecureerde lijst van vertrouwde stamcertificaten (geen ongevalideerde/"insecure" verbindingen).
- Het apparaat beperkt het aanvalsoppervlak: alleen de netwerkfunctionaliteit die nodig is voor de werking (ophaalschema ophalen, software-updates, webinterface op het lokale netwerk) is aanwezig.
- Het product beschikt over een beveiligd update-mechanisme: firmware-updates worden opgehaald via een beveiligde (TLS) verbinding, **cryptografisch ondertekend en op het apparaat geverifieerd vóór installatie (Secure Boot V2), en het apparaat accepteert geen firmware die niet correct is ondertekend.**
- Beveiligingsrelevante gebeurtenissen worden vastgelegd (logboek, raadpleegbaar via de statuspagina van het apparaat) ten behoeve van diagnose.
- Gebruikers kunnen het apparaat terugzetten naar een schone staat (fabrieksreset) en kunnen zelf opgeslagen gegevens (adres, inloggegevens, wifi-gegevens) verwijderen.

De fabrikant voldoet daarnaast aan de kwetsbaarheidsverwerkingseisen van **Bijlage I, Deel II**, waaronder:

- Een gedocumenteerd, actueel overzicht van de in het product gebruikte software-componenten (Software Bill of Materials) - zie [SBOM](#).
- Een openbaar meldpunt en een gecoördineerd kwetsbaarheidsopenbaringsbeleid - zie [Coordinated-Vulnerability-Disclosure-Policy](#).
- Het zonder onnodige vertraging verhelpen van gemelde kwetsbaarheden en het kosteloos beschikbaar stellen van beveiligingsupdates gedurende de ondersteuningsperiode.
- Een ondersteuningsperiode van **minimaal 5 jaar** vanaf het moment dat dit productmodel voor het laatst op de markt is gebracht - zie [Product-Security-Support-Information](#) voor de precieze einddatum.

De fabrikant meldt actief misbruikte kwetsbaarheden en ernstige incidenten conform artikel 14 van de CRA aan ENISA via het daarvoor bestemde EU-meldplatform, binnen de daarvoor geldende termijnen (vroege waarschuwing binnen 24 uur, volledige melding binnen 72 uur, eindrapport binnen 14 dagen).

Radio-apparatuur (Richtlijn 2014/53/EU, "RED")

Dit product bevat de radiomodule DFR1117 (DFRobot "Beetle ESP32-C6"), waarvoor de eigen EU-conformiteitsverklaring van de fabrikant van die module (Zhiwei Robotics Corp.) reeds conformiteit met de RED aantoon, inclusief de daarin vervatte EMC-, gezondheids- en veiligheidseisen. Eagle Software Consultancy B.V.

verklaart, als apart document, dat de integratie van deze module in het Garbi Sein-product deze conformiteit niet beïnvloedt - zie [RED-EMC-Integratieverklaring](#).

RoHS (Richtlijn 2011/65/EU)

De radiomodule (DFR1117) is door de fabrikant van die module verklaard conform de RoHS-richtlijn. De overige door Eagle Software Consultancy B.V. toegevoegde onderdelen (drukknoppen, één WS2812-ledje, bedrading, behuizing) zijn standaard, RoHS-conforme elektronica-componenten.

Ondertekening

Deze verklaring wordt afgegeven onder de exclusieve verantwoordelijkheid van de fabrikant, Eagle Software Consultancy B.V.

Plaats	Amersfoort, Nederland
Datum	17-september-2026
Naam ondertekenaar	A.E. van Putten
Functie	DGA
Handtekening	Het door de ondertekenaar fysiek ondertekende origineel van dit document wordt intern gearcheveerd en is desgevraagd beschikbaar voor toezichthoudende autoriteiten; dit gepubliceerde exemplaar bevat bewust geen afbeelding van de handtekening zelf.

Laatst bijgewerkt: 2026-09-17.