Bijlage XX Telematica eisen en randvoorwaarden

Randvoorwaarden

- De Veiligheidsregio referentie architectuur (VeRa) is van toepassing (zie https://www.veraonline.nl)
- De geboden oplossingen moeten aan kunnen sluiten op de bestaande ICT- en informatievoorzieningen van de VNOG (op aanvraag kunnen de hard- en software standaarden die gelden binnen de VNOG worden geleverd).

Eisen

- Voertuig- en sensor data moet 24/7 beschikbaar zijn, zowel live- als historische data.
- Zowel de toegang tot de data als het beheer moet middels een API uitgevoerd kunnen worden (er hoeft geen user interface geleverd te worden).
- Aanpassen en wijzigen van bestaande data en sensoren moet in eigen beheer door de VNOG kunnen worden uitgevoerd.
- Nieuwe sensoren toevoegen en nieuwe data ontsluiten moet mogelijk zijn eventueel in samenwerking met de leverancier.
- De lokale configuratie dient op afstand vanaf een centraal punt door middel van een enkele actie (niet per voertuig) ingericht kunnen worden.
- De uitwisseling van de voertuig- en sensor data moet zowel realtime als achteraf plaats kunnen vinden. Waarbij de keuze aan de VNOG is.
- De data moet ook in oorspronkelijk formaat (conform Vera IA.4)) beschikbaar zijn.
  Er moet zoveel mogelijk gebruik gemaakt worden van data die door de systemen van en in het voertuig geleverd wordt, bijvoorbeeld GPS locatie data die al vanuit het voertuigvolgsysteem voorhanden is.
- Er moet zoveel mogelijk gebruik gemaakt worden van de binnen de VNOG reeds beschikbare infrastructuur.
- Zonder verbinding dient de op dat moment verzamelde data bewaard te blijven, deze dient te worden gesynchroniseerd bij het weer beschikbaar komen van de verbinding
    - Bij voorkeur is de data lokaal benaderbaar via de API, ook als er geen verbinding voor handen is.
- De oplossing mag op geen enkele wijze het operationele proces belemmeren.

- Eis is een proof of concept (POC) waarin duidelijk wordt:
    - Hoe de oplossing werkt door middel van een beschrijving van zowel de API en minimaal een schematische weergave van de werking.
    - Hoe de uitbreidbaarheid geregeld is
    - Hoe de beveiliging geregeld is
    - Hoe de opslag van de data geregeld is
    - Wat de keuzemogelijkheden zijn, bijvoorbeeld ten aanzien van operating systemen en databases
    - Hoe de data uitwisseling tussen sensoren en de centrale opslag geregeld is.
    - Er is een database schema beschikbaar

- **Security eisen**
    - Zorg voor gesegmenteerde datastromen
    - Gebruik gestandaardiseerde marktconforme protocollen
    - Datastromen zijn niet afluisterbaar, een vorm van beveiliging is aanwezig, welke van toepassing is op het protocol wat gebruikt wordt. Deze beveiliging voldoet aan de wettelijk gestelde eisen (BIO = Baseline Informatiebeveiliging overheid)

- **Eigenaarschap van data**
    - In het kader van de verwerking van beschikbare gegevens bepaalt de verantwoordelijke het doel van de gegevensverwerking, in dit geval dus de VNOG.
    - De data zal worden opgeslagen in een databank die eigendom is van de VNOG, de leverancier stemt hiermee in dat het databank recht voor hem komt te vervallen, ongeacht de intrinsieke waarde van de data
    - De verwerking wordt vastgelegd in een verwerkersovereenkomst.

- De applicatie betreft een saas oplossing.
- De applicatie dient minimaal te voldoen aan de wet- en regelgeving op het gebied van informatiebeveiliging, vertrouwelijkheid en privacy.
- De verbinding is beveiligd met een certificaat van een vertrouwde certificeringsinstantie
- De data, gegevens van de VNOG, bevindt zich alleen in datacenters in de Europese Economische Ruimte (EER) of in een door Europese Unie erkent “veilig land”. Indien er bedrijven betrokken zijn die onder de Amerikaanse wetgeving vallen dan moet dit bedrijf een actieve EU-U.S. Privacy Shield Framework hebben.
- De applicatie is redundant over meerdere datacenters geografisch gescheiden van elkaar.
- Hosting van het systeem vindt plaats in een beveiligde omgeving en voldoet aan alle in Nederland geldende wet- en regelgeving.
- De datacenters zijn ISO 27001 gecertificeerd. De Inschrijver dient aan te geven op welke onderdelen het certificaat is geaccrediteerd.
- Er wordt minimaal één keer in de twee jaar een pentest uitgevoerd, de uitkomsten hiervan worden gedeeld met de Aanbestedende Dienst.
- Er vindt periodiek een backup plaats van de applicatie en de inhoud, de backup blijft minimaal 10 dagen beschikbaar.
- Er is een acceptatieomgeving van de applicatie beschikbaar die vergelijkbaar is met de productieomgeving.
- De data is 24/7 beschikbaar:
    - Uptime garantie van 99.86% of beter (=< 12 uur per jaar)
    - 4 Maintenance Windows (MTW) van max. 3 uur per stuk per jaar
        - Uptime incl. MTW en verstoringen buiten MTW 99,7% (<=24 uur per jaar)
- De Inschrijver verzorgt alle updates en waarborgt dat de VNOG steeds met de nieuwste, succesvol geteste software werkt, zonder dat dit ten koste gaat van de beschikbaarheid en bruikbaarheid van de software.
- De Inschrijver zorgt voor het technisch beheer.
- Er wordt een SLA afgesproken tussen Aanbestedende Dienst en Inschrijver waarin de volgende zaken worden geregeld:
    - Live monitoring / Proactieve monitoring / Reactieve monitoring
    - Eerste response binnen 30 min
    - Call to Fix / Call to response uitleg
- De Inschrijver beschikt over een professionele Nederlandstalige helpdesk met een vast aanspreekpunt (accountmanager).
- De Inschrijver beschikt over een storingsdienst, welke buiten kantoortijden beschikbaar is en Prio 1 incidenten kan aannemen binnen de SLA
- De beschikbaarheid van de data is gegarandeerd door een ESCROW regeling.
- Per release, upgrade en fix wordt een volledig overzicht meegeleverd van de inhoud van de release, upgrade en fix.

Inschrijver onderhoudt documentatie voor beheerders (beheerdocumentatie) en draagt er zorg voor dat deze altijd up-to-date is met de gebruikte versie van de software.