Bijlage 15 Ritregistratie applicatie

Betreft aanbesteding:

Europese openbare aanbesteding 'Wagenpark lease'

Omgevingsdienst Haaglanden

De onderstaande eisen voor de ritregistratie applicatie zijn van toepassing en maken integraal deel uit van deze aanbesteding. Allereerst leest Opdrachtnemer de functionele eisen op hoofdlijnen. Daarna zijn de systeem eisen op een rijtje gezet.

Functionele eisen

Nr.	Omschrijving
1.	Alle ritten van alle kentekens moeten geregistreerd worden volgens de gegevens van de belastingdienst. Het ritregistratiesysteem heeft het keurmerk RRS (Keurmerk ritregistratiesystemen).
2.	De ritregistratie applicatie dienst het keurmerk RitRegistratieSystemen (RSS) te hebben.
3.	De ritregistratie applicatie dient BIO (Baseline Informatiebeveiliging Overheid) compliant te zijn.
4.	Opdrachtgever wenst te kunnen inloggen in de applicatie om real life na te kunnen gaan waar het voertuig zich bevindt en welke ritten er gemaakt zijn.
5.	Het systeem moet de volgende managementinformatie per voertuig genereren: • het aantal ritten per maand/kwartaal/jaar; • het aantal gereden kilometers per maand/kwartaal/jaar.

Systeem eisen

Nr.	Omschrijving
1.	Het onderhoud en ondersteuning op de door Opdrachtnemer aangeboden applicatie wordt tenminste gegarandeerd gedurende de looptijd van de overeenkomst.
2.	Voor alle overheidsopdrachten is de BIO van kracht. De beveiliging van de applicatie dient hieraan te voldoen. Op dit moment wordt er gewerkt aan de BIO 2.0. Omdat de BIO 2.0 pas eind 2024 van kracht wordt, is op 1 juni 2023 de handreiking BIO2.0-opmaat (https://bio-overheid.nl/category/producten?product=Handreiking_BIO2_0_opmaat) opgeleverd. In deze handreiking is de indeling van de controls, doelstellingen en overheidsmaatregelen in deel 2 van de BIO in lijn gebracht met de 2022-versie van de ISO-27002. Naast tekstuele wijzigingen, zijn ook een aantal overheidsmaatregelen geactualiseerd, vanwege nieuwe dreigingen, zoals ransomware. Naast de verhoging van de feitelijke veiligheid, wordt ook geanticipeerd op aanpassingen die in de BIO2.0 zullen worden doorgevoerd. Op deze Opdracht is het beveiligingsniveau **BBN2** van de BIO van toepassing. De oplossing dient de Opdrachtgever in staat te stellen hieraan te (blijven) voldoen zonder additionele kosten. Bij de uitvoering van de raamovereenkomst dient de Opdrachtnemer aantoonbaar te maken te voldoen aan BIO of diens opvolgers. Over de invulling hiervan maakt de Opdrachtnemer afspraken. Deze kan bijvoorbeeld bestaan uit derde partij Assurance met van toepassing zijnde scope, geldigheid en afgifte door erkende instantie. Voor meer informatie: https://bio-overheid.nl/category/producten#BIO.
3.	Indien persoonsgegevens in de zin van de Algemene Verordening Gegevensbescheming (AVG) worden verwerkt door een bewerker (derde) dient een Verwerkersovereenkomst te worden afgesloten. Onder Verwerking van Persoonsgegevens wordt verstaan: elke handeling of elk geheel van handelingen (o.a. verzamelen, bewaren en vernietigen) met betrekking tot Persoonsgegevens. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (bv. NAW-gegevens, foto's van personen, BSN-nummers. IP-nummers).
4.	Opdrachtnemer doet een melding aan Opdrachtgever van security en of privacy incidenten (datalek) binnen 24 uur na constatering en verstrekt alle details inclusief informatie over omvang, impact, betrokken data, en termijn van oplossen/verhelpen.

5.	De Leverancier van de ritregistratie applicatie dient zorg te dragen voor AVG compliancy van de software en van de gebruikte gegevens.
6.	Voor de duur van deze Overeenkomst wordt één verwerkersovereenkomst afgesloten. De verwerkersovereenkomst kan tijdens looptijd van de overeenkomst periodiek aangepast worden.
7.	Data (op transport, in verwerking en in rust) met classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.
8.	De door Forum Standaardisatie verplichte en aanbevolen standaarden moeten worden toegepast. (Relevante Standaardisatienormen zijn: * TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * STARTTLS en DANE *(beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen) *SAML (authenticatie en autorisatie))
9.	De data wordt binnen de E.U. en/of de Europese Economische Ruimte (EER) opgeslagen, in tenminste een Tier 2 datacenter. De aanbieder waar de hosting van de tool plaatsvindt valt onder de jurisdictie van de Europese Unie (EU) of de EEU., waarbij deze niet tevens valt onder een jurisdictie buiten de EU of de EER.
10.	Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn technologieonafhankelijk, onveranderbaar, integer en raadpleegbaar te worden opgeslagen en op aanwijzing van de CSC/data eigenaar te kunnen worden vernietigd (conform archiefwet).
11.	De onderlinge netwerkconnecties (koppelvlakken) in de keten van CSC naar CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.
12.	De clouddiensten architectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen CSC en CSP en biedt transparantie en overzicht van rand voorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.
13.	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
14.	De Leverancier werkt op eerste verzoek mee (maximaal 1 x per jaar) aan een audit en/of BIO onderzoek door de Auditdienst van de Opdrachtgever. Zie ook GIBIT art. 21. **of** De Leverancier overlegt jaarlijks een TPM verklaring door een onafhankelijke IT Auditor (RE).(zie art. 35 GIBIT)
15.	Leverancier toont aan dat beveiliging op orde is door het periodiek (laten) uitvoeren van een penetratietest (pentest).
16.	De gegenereerde data binnen de applicatie is eigendom van de Opdrachtgever. Dat betekent dat na het beëindigen van de dienstverlening dan wel de Nadere overeenkomst, de Opdrachtnemer deze data aan Opdrachtgever de moet overdragen, en wel binnen 10 dagen na contractbeëindiging.
17.	Gedurende de looptijd van de Raamovereenkomst zal de Opdrachtnemer het exit plan up-to-date houden
18.	Naast de inkoopvoorwaarden zijn de artikelen 20, 21, 22, 26, 28, 29, 30, 34, 34 35 en 36 van de GIBIT 2023 van toepassing op de overeenkomst.