Niet-functionele Eisen

Datagestuurd reinigen van openbare buitenruimtes

26 juni 2026
Kenmerk 2026SB981
Versie 1.0
Definitief

bronversie Format A-302 v20221222

Inhoud

1.1 Architectuureisen

Eis 1. Het route- & planning informatiesysteem is een SAAS oplossing.

Eis 2. Toegang tot het route- & planning informatiesysteem is dwingend geregeld op basis van Single-Sign-On, (SSO) middels federatie op basis van Microsoft Azure Active Directory Federation

Eis 3. Voor data uitwisseling tussen camera software en route- & planning informatiesysteem wordt 2-zijdig TLS1.2 of hoger toegepast.

Eis 4. Authenticatie route- & planning informatiesysteem aansluiten op OpenID Connect Oauthv2; SAML 2 en provisioning op SCIMv2

Eis 5. Het gebruik van remote display en/of digitale workspace software om route- & planning informatiesysteem te benaderen is niet toegestaan behalve voor mobile device management betreffende security doeleinden

Eis 6. Het route- & planning informatiesysteem maakt geen gebruik van plug-in componenten.

Eis 7. Voor het functioneren van route- & planning informatiesysteem op het client device en/of in de webbrowser zijn geen verdere instellingen en/of installaties op het client device en/of in de browser benodigd.

Eis 8. Koppelingen van het route- & planning informatiesysteem met applicaties buiten de infrastructuur van de gemeente Utrecht (de SaaS applicaties Signalen en InPlanning) verloopt direct van de SaaS applicatie met de voorziening of SaaS applicatie.

Eis 9. De camera's moeten een zo breed mogelijk kijkvenster hebben én de beelden van de camera moeten geschikt zijn voor AI.

Eis 10. In 95% van alle gevallen is de levering van objectherkenning op basis van meta data betrouwbaar en volledig.

Eis 11. Er worden middels de camera's bevestigd op voertuigen van gemeente Utrecht beelden gemaakt van de publieke buitenruimte in de stad Utrecht. Hierbij kunnen passanten en kentekens van auto's onbedoeld in beeld komen waardoor deze persoonsgegevens worden verwerkt. De leverancier draagt er zorg voor dat op de beelden direct geblurred worden en objectdetectie plaatsvindt door het algoritme(S) in een voor medewerkers afgesloten omgeving en alle beelden daarna direct verwijderd worden. De afgesloten omgeving is zo dicht mogelijk bij de camera's/camerasysteem.

Eis 12. Objectdetectie wordt uitgevoerd door algoritmen zoals bijvoorbeeld RetinaNet, Mask R-CNN, SSD, YOLO, met specifieke prestatiecriteria zoals nauwkeurigheid, snelheid en ondersteunde objectcategorieën.

Eis 13. Het route- & planning informatiesysteem ontvangt uitsluitend het resultaat van het beeldherkenning algoritme, data van afvalsoort, datum en de locatie en omvang van afval (geen persoonsgegevens). Het is niet de intentie van deze verwerking om persoonsgegevens te verzamelen. De data is de enige output van het afgesloten camerasysteem.

1.2 Verwerkingslocaties

Eis 14. De verwerking vindt plaats in het camerasysteem op de voertuigen van de gemeente (dit is binnen de EER, in NL).

1.3 eigendom

Eis 15. De opdrachtgever, de gemeente is eigenaar van de resultaten van het beeldherkenning algoritme data: afvalsoort, datum en de locatie en omvang afval.

Eis 16. De opdrachtgever, de gemeente is eigenaar van alle data in het route- & planning systeem

1.4 Bewaartermijnen, naleving Archiefwet

Eis 17. De data over afval (locatie, afvalsoort, datum, tijdstip, volume inschatting) uit het beeldherkenning algoritme wordt direct na opname in het routeoptimalisatie- en planningssysteem vernietigd van de technische infrastructuur, de server(s) van opdrachtnemer. De bewaartermijn van deze data is max. 1 dag.

Eis 18. Alle data (afvalsoort, locatie, datum, tijdstip, voertuigen, materieel, functies, meldingen, hotspotkaarten, routes, etc.) in het routeoptimalisatie- en planningssysteem heeft de bewaartermijn van 7 jaar. De data wordt daarna door de opdrachtnemer vernietigd van de technische infrastructuur, de server(s) van opdrachtnemer. Dit betekent dat bewaartermijnen aan de data toegevoegd kunnen worden en dat er vernietigingslijsten opgesteld kunnen worden.

Eis 19. Alle data in het routeoptimalisatie- en planningssysteem heeft versiebeheer en mogelijkheden voor het zoeken naar informatie door de gebruiker, de opdrachtgever.

Eis 20. Voor de data die bewaard moet worden geldt dat de lijst voorkeursformaten van het Nationaal Archief moet worden gebruikt: https://www.nationaalarchief.nl/archiveren/kennisbank/lijst-voorkeursformaten. En voldoet bij voorkeur aan MDTO standaard.

Eis 21. Algoritmen voor beeldherkenning en in Routeoptimalisatie- en planningssysteem wordt door leverancier bewaart gedurende contractduur, dit geldt ook voor alle versies gedurende de looptijd van het contract.

Eis 22. De geblurde camerabeelden, die niet voor trainingsdoeleinden gebruikt worden, worden direct vernietigd. De beperkte set van geblurde beelden die wordt gebruikt voor training doeleinden en feedback op het algoritme door aanbieder en eventueel kwaliteitscontrole door opdrachtgever, wordt bewaard voor de periode van 1 maand en daarna aantoonbaar verwijderd.

1.5 Bescherming persoonsgegevens, naleving AVG

Eis 23. Persoonsgegevens worden real-time bij de bron (camera-hardware/software) geblurd (geanonimiseerd) en niet voor verdere verwerking opgeslagen.

Eis 24. Een beperkte set van de herkende data (afvalsoort, locatie, datum, tijdstip, omvang) wordt regelmatig door de leverancier steekproefwijs gecontroleerd/getoetst. Indien dit afwijkt van de norm wordt dit besproken met opdrachtgever en issues/afwijkingen worden door opdrachtnemer verholpen conform de eisen in de SLA. Hier worden echter geen persoonsgegevens voor gebruikt of verwerkt.

Eis 25. De gemeente (opdrachtgever) kan de beperkte set van de herkende data (voor kwaliteitsdoeleinden) opvragen incl. het bijhorend resultaat van het algoritme voor controle doeleinden

Eis 26. Onderdeel van de overeenkomst met de leverancier is de eis om met blurring methodiek/algoritme te werken in de meest recente versie (minimaal 1 x per jaar uit te werken in een SLA). De functionele en technische omschrijvingen van het algoritme(s) en de toepassing daarvan is volledig beschreven in een Dossier van Afspraken en Procedures de zogenaamde DAP.

Eis 27. Door het implementeren van een autorisatiematrix voor beheerders van de opdrachtnemer van camerasysteem met blurring-methodiek en algoritme(s), krijgen alleen de beheerders toegang tot de configuratie van het systeem (deze bevatten geen persoonsgegevens). Er wordt contractueel vastgelegd hoe de leverancier om mag gaan met toegang tot en gebruik van de configuratie en inrichting.

Eis 28. Er zal geen opslag plaatsvinden van persoonsgegevens. Na het real-time blurren van persoonsgegevens en objectdetectie door algoritme omzetten in metadata, worden de geblurde beelden onmiddellijk verwijderd van het camera systeem.

Eis 29. Onderdeel van de overeenkomst tussen opdrachtgever en opdrachtnemer is de eis om de gebruikte blurring algoritme bij te werken naar de meest recente versie met betrekking tot afvalherkenning. In de SLA en in de DAP (Dossier Afspraken en Procedures) als onderdeel van de overeenkomst wordt het update en upgrade beleid opgenomen.

Eis 30. De opdrachtneremer levert technische documentatie waarin aangetoond wordt dat de informatiesystemen aan alle eisen voldoen, uitleg over de werking van de algoritmen. Duidelijke informatie over de werking en het doel van de informatiesystemen en algoritmen voor de gebruikers.

Eis 31. Logbestanden (Logging): automatische logging en registratie van gebeurtenissen in software camera’s en route- & planningsysteem voor traceerbaarheid door de opdrachtnemer en verstrekt aan de opdrachtgever. De logging moet minimaal zes maanden bewaard worden door de opdrachtnemer.

Eis 32. Opdrachtnemer moet voldoen aan de ISO27001 norm en de VVT (Verklaring Van Toepasselijkheid) is van toepassing op hun dienstverlening. Veranderingen in de VVT worden proactief aan de opdrachtgever gecommuniceerd.

Eis 33. De afvalstoffenverordening van de gemeente dient aangepast te worden als rechtsgrond voor gegevensverwerkingen. Dit is een randvoorwaarde voor gunning. Indien de afvalstoffenverordening niet op dit punt is aangepast, kan de gemeente niet tot gunning van deze aanbesteding overgaan.

Eis 34. De opdrachtnemer zal minimaal 1x per jaar een Penetratie test laten uitvoeren op de op het gehele systeem van applicatie en installatie inclusief koppelingen welke van toepassing zijn voor gemeente Utrecht. Dit dient door een onafhankelijke en gespecialiseerde auditor plaats te vinden. Eventuele bevindingen in de pentest die als critical worden aangemerkt moeten binnen 2 weken worden verholpen. Er dient voor in productie name van het systeem een pentest te worden uitgevoerd en de eventuele criticals zijn weggenomen cq gemitigeerd met doeltreffende maatregelen.

Eis 35. De opdrachtnemer zal 1x per 2 jaar een Privacy compliance audit laten uitvoeren, met als doel om te onderzoeken of het technische proces nog voldoet aan de laatste stand van privacyregelgeving, waaraan de Gemeentelijke overheid dient te voldoen. Deze audit dient door een onafhankelijke en gespecialiseerde auditor te worden uitgevoerd

Eis 36. Het uitvoeren van de hierboven genoemde audits [Eis 28 en Eis 29] dient aantoonbaar te worden gemaakt door de opdrachtnemer d.m.v. een gecertificeerde In Control Statement, bijv accountantsverklaring, SOC 2 Type II rapport of anders. Deze beide audits mogen eventueel door eenzelfde partij, tegelijkertijd worden uitgevoerd. De volledige inhoud van deze ICS zal door de opdrachtnemer worden gedeeld met de opdrachtgever.

Eis 37. De opdrachtnemer laat beide audits de eerste maal uitvoeren [eis 20 en 29] voordat de applicatie in productie wordt genomen en vanaf dan iedere 2 jaar (Privacy Compliance Audit) en ieder jaar (penetratietest).

Eis 38. Opdrachtnemer beschikt over:

- ISO 27001-certificaat (scope dekkend voor gecontracteerde dienst - niet alleen hoofdvestiging) ISMS conform ISO 27001;
- Óf gelijkwaardige zekerheid als alternatief voor ISO 27001: SOC 2 Type II (werking, niet enkel opzet/bestaan) of ISAE 3000 / NBA Richtlijn 3000-verklaring — mits scope dekkend;
- SOC 2 Type II-rapport (gescoped op de specifieke dienst - aanvullend op ISO 27001, met name voor cloud) voor de gecontracteerde dienst.

Eis 39. Opdrachtnemer zorgt voor volledige ketentransparantie door toeleveranciers aan de opdrachtgever bekend te maken, de eisen van de opdrachtgever door te leggen aan deze toeleveranciers, aantoonbaar inzicht te bieden in de beveiliging van de gehele leveranciersketen, en een helder subverwerkersbeleid te voeren waarin wordt vastgelegd welke derden data verwerken en waarin tijdige kennisgeving bij wijzigingen (met name bij SaaS- en Cloud toepassingen) is geborgd.

Eis 40. Gedurende de looptijd geeft de opdrachtnemer de veranderingen in de keten van toeleveranciers door aan de opdrachtgever, inclusief risico’s daarin.

Eis 41. Opdrachtnemer verplicht het gebruik van role-based access volgens het least-privilege-principe, zorgt ervoor dat multi-factor authenticatie (MFA) verplicht is voor beheeraccounts en alle vormen van remote access, en borgt dat toegang tot de ICT-prestatie dwingend is ingericht via Single Sign-On (SSO) op basis van federatie met Microsoft Azure Active Directory.

Eis 42. De ICT-prestatie van de opdrachtnemer hanteert een authenticatiemechanismen op basis van OpenID Connect (OAuth2), SAML 2 en provisioning via SCIM v2.

Eis 43. De ICT- prestatie van de opdrachtnemer waarborgt aantoonbaar dat alle data zich binnen de EU/EER bevindt, inclusief een contractuele garantie die ook van toepassing is op alle ingeschakelde subverwerkers.

Eis 44. De accounts in de ICT-prestatiezijn zijn te allen tijde herleidbaar tot een persoon of een apparaat en worden door de opdrachtnemer ten minste halfjaarlijks beoordeeld.

Eis 45. Alle geleverde en beheerde sensoren en camera's door de opdrachtnemer voldoen aan de vereisten voor hardening (waarbij default-accounts worden verwijderd en overbodige services zijn uitgeschakeld), beschikken over up-to-date patchmanagement en zijn voorzien van adequate malwarebescherming.

Eis 46. De camera's authentiseren zich uniek aan het IoT-netwerk door middel van een device-ID. Hiervoor zorgt de opdrachtnemer.

Eis 47. Camerabeelden worden onmiddellijk geautomatiseerd van de apparatuur verwijderd nadat zij zijn verwerkt door de opdrachtnemer.

Eis 48. Alle koppelingen met Route- & planningsysteem verlopen via beveiligde verbindingen voor de data-uitwisseling met gemeentelijke applicaties: Signalen, InPlanning en Tableau/PowerBI. Alle koppelingen zijn gebaseerd op standaard REST-API-services (zie Forum Standaardisatie).

Eis 49. De Route- & planningsysteem is een SaaS-applicatie en borgt aantoonbare tenant-segmentatie op de infrastructuur, de servers, waarbij data strikt logisch is geïsoleerd van andere huurders, en levert jaarlijks bewijs van deze scheiding conform de overeengekomen zekerheidsniveaus.

Eis 50. Encryptie wordt geborgd doordat bij data-uitwisseling tussen camera's en het route- en planningsinformatiesysteem en de aangrenzende applicaties van d egemeente, te weten Signalen, InPlanning en Tableau (Server) wederzijdse authenticatie via TLS 1.2 of hoger wordt toegepast, en voor externe communicatie gebruik wordt gemaakt van PKI-certificaten.

Eis 51. Toegang tot camera's en applicaties moet door opdrachtgever, functioneel beheerder, kunnen worden geregistreerd, waarbij alle toegangsactiviteiten aantoonbaar worden vastgelegd en tevens alle wijzigingen in autorisaties en software worden gelogd. Vastleggingen worden minimaal 12 maanden bewaard.

Eis 52. Het route- en planningsinformatiesysteem ondersteunt een SOC-koppeling via het standaard syslog-formaat en zorgt ervoor dat beveiligingsmonitoringdata exporteerbaar is ten behoeve van integratie met het SIEM-systeem van de opdrachtgever.

Eis 53. Opdrachtnemer heeft een incidentproces dat voorziet in detectie, melding, analyse, mitigatie en periodieke rapportage aan de opdrachtgever.

Eis 54. Opdrachtnemer beschikt over een recovery- en incident responseplan dat is afgestemd met de opdrachtgever, waarbij jaarlijkse tests verplicht zijn en de resultaten hiervan periodiek aan de opdrachtgever worden gerapporteerd.

Eis 55. Er geldt een verplicht incidentproces voor de opdrachtnemer waarin significante incidenten zo snel mogelijk en uiterlijk binnen 24 uur als eerste melding (early warning) aan opdrachtgever worden gemeld, gevolgd door een nadere inhoudelijke incidentmelding inclusief impactanalyse binnen 72 uur en een eindrapport binnen één maand, en dat daarnaast voorziet in detectie, analyse, mitigatie en periodieke rapportage aan de opdrachtgever.

Eis 56. Wijzigingen zullen door de opdrachtnemer vooraf worden aangekondigd, waarbij voor substantiële wijzigingen een minimaal aankondigingstermijn van 30 dagen geldt.

Eis 57. Opdrachtnemer heeft een gedocumenteerd kwetsbaarheidsbeheerproces ingericht dat voorziet in ontdekking, registratie, beoordeling en herstel van kwetsbaarheden met aantoonbare doorlooptijden, waarbij een verplichte patchprocedure met prioritering wordt toegepast, de opdrachtnemer een volledig logboek bijhoudt van alle patches (inclusief niet-uitgevoerde patches), en jaarlijks een pentestrapport met betrekking tot de apparatuur aan de opdrachtgever wordt verstrekt.

Eis 58. Back-ups worden door de opdrachtnemer zodanig ingericht dat minimaal drie versies beschikbaar zijn en jaarlijks een restoretest wordt uitgevoerd om de herstelbaarheid te verifiëren.

Eis 59. Er is een Business Continuity Plan voor de geleverde dienst opgesteld door de opdrachtnemer, dat aantoonbaar is getest en waarin de recovery time objective (RTO) en recovery point objective (RPO) zijn gedocumenteerd.

Eis 60. Er geldt een beschikbaarheids- en uptime-SLA van minimaal 99% voor de opdrachtnemer, waaraan financiële consequenties zijn verbonden bij het niet behalen van dit serviceniveau.

Eis 61. Opdrachtnemer voorziet in verplichte security awareness-trainingen voor haar personeel, waarbij personeel met toegang tot systemen of data minimaal wordt gescreend door middel van een Verklaring Omtrent Gedrag (VOG) en, voor gevoelige segmenten, een Verklaring van Geen Bezwaar (VGB) vereist is.

Eis 62. Er is een jaarlijks auditrecht voor de opdrachtgever vastgelegd, waarbij tevens is toegestaan dat de opdrachtgever penetratietesten uitvoert.

Eis 63. Remote access tot apparatuur door beheerders van de opdrachtnemer wordt uitsluitend tijdelijk verleend, volledig gelogd en na gebruik automatisch afgesloten.

Eis 64. Transparantie over wijzigingen in de dienst of het product wordt geborgd door de opdrachtnemer doordat vooraf kennisgeving plaatsvindt, het wijzigingsbeheerproces inzichtelijk is, en elke wijziging wordt voorzien van een risicoanalyse en een mogelijkheid tot rollback.

Eis 65. Data blijft te allen tijde eigendom van de opdrachtgever, waarbij bij beëindiging van de overeenkomst wordt geborgd dat de data overdraagbaar is en aantoonbaar veilig wordt verwijderd.

1.6 Naleving van de wetgeving, de AI Act

Bij de levering van dit systeem, dient de opdrachtnemer te voldoen aan de vereisten van de AI Act (Artificial Intelligence Regulation) zodra deze wet is aangenomen en geïmplementeerd in Nederland. Het AI-systeem voor camera's met beeldherkenning software met aanverwante algoritmes wordt beschouwd als een hoog risicosysteem, vanwege het filmen in de openbare ruimte.

In het kader van de AI-act draagt de leverancier specifieke verantwoordelijkheden en vervult expliciete rollen om naleving te garanderen. Specifieke verplichtingen en eisen voor de leverancier omvatten:

Eis 66. Opdrachtnemer zorgt voor datamanagement: de beperkte dataset met geblurde camerabeelden wordt beveiligd opgeslagen, alleen medewerkers die toegang hebben voor training van algoritme komen in aanraking met de data. Data wordt beperkt bewaard, na training verwijderd. De beperkte dataset met geblurde camerabeelden wordt aan gemeente verstrekt voor kwaliteitsdoeleinden zodra er om wordt gevraagd.

Eis 67. Opdrachtnemer zorgt voor risico beheersysteem en data kwaliteitssysteem

Eis 68. Opdrachtnemer zorgt voor automatische logging van het gebruik en van de AI-systeem beeldherkenning en het route- & planningsysteem zelf waarmee bijv. oneigenlijk toegang en gebruik kan worden opgespoord

Eis 69. De outputdata van het beeldherkenning algoritme blijft eigendom van de gemeente (door route- en planning systeem gebruikt). Dit geldt ook voor tijdelijk bewaarde geblurde camerabeelden voor trainingsdoeleinden. De input- en outputdata van het route- & planningsysteem blijft eigendom van de gemeente

Eis 70. De Opdrachtnemer voldoet aan de exit strategie afspraken: de output data van beeldherkenning wordt door de opdrachtnemer kosteloos overgedragen aan de opdrachtgever (gemeente) incl. alle logbestanden. De opdrachtnemer zorgt voor de verwijdering van bedrijfsdata uit informatiesystemen en zorgt voor overdracht van logbestanden. De input- en output data van route- & planningsysteem incl. logbestanden worden door opdrachtnemer kosteloos aan opdrachtgever (gemeente) overgedragen voordat het contract eindigt.