Gemeente Eindhoven

Programma van Eisen – Handhavingssysteem

Colofon

Opdrachtgever	Gemeente Eindhoven, sector Stadsbedrijf, afdeling Stadsbeheer
Titel rapport	Programma van Eisen–Handhavingssysteem
Versie	1.0 (definitief)
Datum	27 september 2024

Inhoudsopgave

1 Inleiding 4
1.1 Algemeen 4
1.2 Doel 4
1.3 Opzet 4
1.4 Definities 4
2 Projectcontext 6
2.1 Huidige situatie 6
2.2 Randvoorwaarden en uitgangspunten 6
2.3 Ontwikkelingen 7
3 Organisatie van de werkzaamheden 8
3.1 Inbreng Opdrachtgever vs Opdrachtnemer 8
3.2 Overleg en rapportage 8
4 Eisen aan de dienstverlening 9
4.1 Eisen privacy en informatiebeveiliging 9
4.2 Algemene eisen handhavingssysteem 12
4.3 Eisen aan gebruikersbeheer en functioneel beheer 13
4.4 Administratiefrechtelijke handhaving parkeren 14
4.5 Brede handhaving – algemene eisen 16
4.6 Brede handhaving – eisen meldkamersoftware 17
4.7 Brede handhaving – eisen handhaaf-app 18
4.8 Brede handhaving – eisen back-office 19
4.9 Eisen aan koppelvlakken/interfaces 21
4.10 Eisen m.b.t. beschikbaarheid 22
5 Eisen aan de implementatie 23
5.1 Implementatie 23
5.2 Conversie 23
5.3 Informatie en training 23
5.4 Helpdesk – ondersteuning 24
5.5 Einde overeenkomst 25

1 Inleiding

1.1 Algemeen

Voor u ligt het Programma van Eisen met betrekking tot de levering van een Handhavingssysteem voor de afdeling Handhaving van Gemeente Eindhoven. Dit PvE geeft de beschrijving van de eisen die de Opdrachtgever stelt aan de levering van het systeem, alsmede de daaropvolgende instandhouding en technisch beheer van het geleverde systeem. Het te leveren systeem dient gedurende de gehele looptijd van de te sluiten overeenkomst volledig te voldoen aan de eisen die in dit PvE zijn opgenomen.

De gebruiksklare oplevering van het Handhavingssysteem dient uiterlijk 1 juli 2025 plaats te vinden. Voorafgaand dient de Opdrachtnemer de benodigde voorbereidingen te treffen en eventuele testen uit te voeren om per 1 juli 2025 volledig operationeel te zijn.

1.2 Doel

Dit PvE beschrijft de eisen aan en vormt het toetsingskader voor de levering van een Handhavingssysteem binnen gemeente Eindhoven. Met de aanbesteding van een Handhavingssysteem wordt beoogd dat de Gemeente Eindhoven de beschikking krijgt over een betrouwbaar, toekomstbestendig en flexibel systeem waarmee de gemeentelijke handhavers hun werk kunnen uitvoeren en datagestuurde handhaving mogelijk wordt gemaakt.
De Gemeente Eindhoven wenst door de Opdrachtnemer maximaal ondersteund te worden bij het dagelijks beheer van het systeem.

1.3 Opzet

In hoofdstuk 2 wordt de projectcontext geschetst. Daarbij wordt aangegeven met welke specifieke uitgangssituatie rekening gehouden met worden. Hoofdstuk 3 gaat in op de organisatie van de levering, hoofdstuk 4 op de daaraan gestelde technische en functionele eisen alsmede de te behalen prestatie-eisen.

1.4 Definities

In dit Programma van Eisen wordt verstaan onder:

Combibon	Een in de Regeling modellen en formulieren ten behoeve van de handhaving Justitie, vastgesteld formulier, dat onder meer kan worden gebruik voor de volgende afdoenings-/sanctiemodaliteiten: - S: aankondiging van strafbeschikking - K: kennisgeving van bekeuring - A: aankondiging van beschikking (Mulder-feit) - B: beschikking (Mulder-feit)
Handhavingssysteem	Het door Inschrijver aan te bieden systeem, waarvan de daaraan te stellen eisen zijn opgenomen in dit Programma van Eisen.
Inschrijver	Een marktpartij die een Inschrijving indient in het kader van de aanbestedingsprocedure waardoor dit Programma van Eisen is opgesteld.
Mulder-feit	Een lichte verkeersovertreding (bijvoorbeeld foutparkeren), die valt onder de “Wet Mulder”; deze wet heet officieel Wet administratiefrechtelijke handhaving verkeersvoorschriften (WAHV).
Opdrachtgever	De rechtspersoon Gemeente Eindhoven, alsmede haar medewerkers en/of vertegenwoordigers.
Opdrachtnemer	De marktpartij welke na het doorlopen van de aanbestedingsprocedure de opdracht verwerft tot het uitvoeren van de gevraagde dienstverlening.

Service Level Agreement	De overeenkomst tussen Opdrachtgever en Opdrachtnemer, waarin afspraken zijn vastgelegd met betrekking tot de te realiseren kwaliteit van de dienstverlening.

2 Projectcontext

2.1 Huidige situatie

De Gemeente Eindhoven is een regie-organisatie, waarbij de uitvoeringstaken grotendeels zijn uitbesteed aan externe dienstverleners. Een uitzondering hierop wordt gevormd door de gemeentelijke handhavingstaken, uitgezonderd de handhaving van het fiscaalrechtelijk parkeren. Het fiscaalrechtelijk parkeren is sinds 1 januari 2024 ondergebracht bij een externe dienstverlener.

Voor de gemeentelijke handhavingstaken wordt sinds 2017 gebruik gemaakt van de gemeentelijke Handhavingssysteem BlueBrick van leverancier BrickYard, in combinatie met het informatiesysteem HEaPP van leverancier Ibou. In verband met de wijzigingen van het pakket aan gemeentelijke handhavingstaken van de openbare ruimte wordt gezocht naar een nieuwe Handhavingssysteem.

2.2 Randvoorwaarden en uitgangspunten

Visie Opdrachtgever

Gemeente Eindhoven beschouwt handhaving van de openbare ruimte als essentiële bouwsteen voor een gezonde, leefbare en veilige stad. Tegelijkertijd wil Eindhoven ook gastvrij zijn voor haar bezoekers.

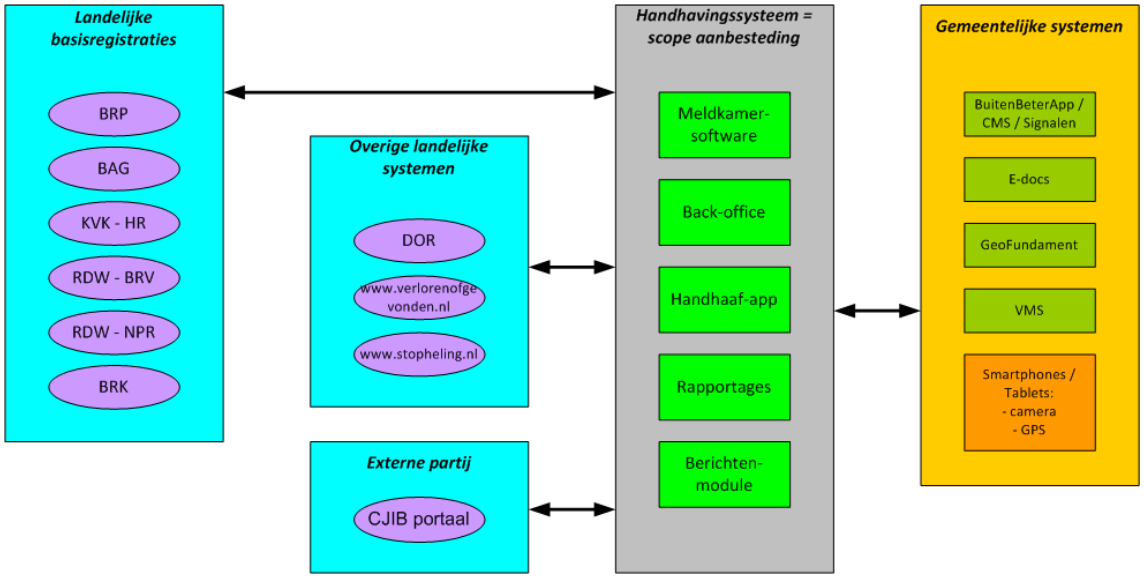
Wet en Regelgeving

Alle door de Opdrachtnemer bij de levering, alsmede het beheer en onderhoud, van de applicatie in te zetten middelen dienen te voldoen aan alle in Nederland geldende wet- en regelgeving, waaronder ARBO- en veiligheidsregels en NEN-normeringen. De verwerking van gegevens binnen de applicatie dient middels een DPIA te worden getoetst aan AVG en WPG en de gemeentelijke uitgangspunten ten aanzien van privacy, security en safety.

Projectomvang

De globale omvang van deze opdracht behelst:

- Het gebruiksklaar opleveren van één Handhavingsapplicatie (SaaS) voor de gemeentelijke handhavingstaken binnen de openbare ruimte, uitgezonderd de fiscale parkeerhandhaving, inclusief bijbehorende koppelingen met gemeentelijke systemen en systemen van derden (zie figuur 1 en bijlage 1).
- Het beschikbaar stellen van één Handhavingsapplicatie voor 150 gebruikers na implementatie. Gedurende de gehele looptijd van de overeenkomst is het voor gemeente Eindhoven mogelijk het aantal gebruikers te laten toenemen en afnemen o.b.v. de eventuele groei of krimp van het aantal gebruikers.
- Het gedurende 10 jaar (als gebruik wordt gemaakt van alle verlengingsmogelijkheden) na oplevering verzorgen van het technisch beheer van de Handhavingsapplicatie, opdat deze blijvend correct functioneert.
- Het gedurende 10 jaar (als gebruik wordt gemaakt van alle verlengingsmogelijkheden) na oplevering verzorgen updates en upgrades van de Handhavingsapplicatie, opdat deze blijvend voldoet aan wet- en regelgeving.
- Het beschikbaar stellen van managementinformatie ten behoeve van de Opdrachtgever.
- Het gedurende 10 jaar (als gebruik wordt gemaakt van alle verlengingsmogelijkheden) leveren van ondersteuning/consultancy als dit nodig wordt geacht door Opdrachtgever.
- Het migreren van bestaande gegevens uit de huidige oplossingen.



Figuur 1: Schematisch overzicht scope aanbesteding inclusief te koppelen systemen

Tot dit project behoort niet:

- Het functioneel en operationeel beheer van het Handhavingssysteem
- Het leveren en/of beheren van mobiele devices
- Het leveren en/of beheren van (mobiele) printers
- Het leveren van ANPR-camera's en VMS
- Het inrichten van werkplekken ten behoeve van backoffice werkzaamheden

Randvoorwaarden

De volgende randvoorwaarden zijn van toepassing:

- Het handhavingssysteem dient 1 juli 2025 gebruiksklaar en volledig ingericht te worden opgeleverd.
- Na opdrachtverlening levert Opdrachtgever een DPIA aan, waarbij Opdrachtnemer de voor hem relevante of specifiek voor zijn Inschrijving geldende zaken dient aan te vullen. Deze zaken betreft die onderdelen van de DPIA die uitsluitend Opdrachtnemer kan invullen. Opdrachtnemer dient de volledig ingevulde DPIA binnen 14 dagen aan Opdrachtgever te retourneren.
- Opdrachtnemer mag werkzaamheden door Derden uit latenvoeren, doch uitsluitend na schriftelijke goedkeuring daarvan door Opdrachtgever. Opdrachtnemer behoudt te allen tijde de volledige eindverantwoordelijkheid voor de kwaliteit en het resultaat van de uitgevoerde werkzaamheden.

2.3 Ontwikkelingen

Het handhavingssysteem wordt gebruikt door de afdeling Handhaving, welke onderdeel gaat vormen van de sector Veiligheid en Handhaving. De verwachting is dat het aantal handhavers de komende jaren sterk zal groeien, zowel voor de bestuursrechtelijke als de strafrechtelijke handhaving, met circa 5 tot 10% per jaar.

3 Organisatie van de werkzaamheden

3.1 Inbreng Opdrachtgever vs Opdrachtnemer

3.1.1 Opdrachtgever stelt de volgende zaken ter beschikking:

- Mobiele devices (smartphones en tablets, voorzien van besturingssoftware Android of iOS) ten behoeve van de handhavers
- Exportbestand van de huidige APV-regelgeving plus feitcodes en boetebedragen

3.1.2 Voor zover dn benodigd zijn voor de gebruiksklare oplevering en/of de instandhouding van de applicatie, maar niet in bovenstaand overzicht zijn opgenomen, dient Opdrachtnemer deze voor eigen rekening in te brengen.

3.2 Overleg en rapportage

3.2.1 Ieder kwartaal wordt de gang van zaken met betrekking tot de Overeenkomst en de kwaliteit van de geleverde dienstverlening geëvalueerd ten kantore van de Opdrachtgever. De gespreksonderwerpen worden in overleg tussen de Opdrachtgever en de Opdrachtnemer vastgesteld en nader bepaald.

3.2.2 Gedurende het 1e jaar na implementatie kan op initiatief van de Opdrachtgever een hogere overlegfrequentie dan elk kwartaal worden aangehouden.

3.2.3 In geval van calamiteiten of wanneer Opdrachtgever en/of Opdrachtnemer aanleiding ziet om in extra overleg te treden, dienen beide partijen hier hun medewerking aan te verlenen.

3.2.4 De Opdrachtnemer stelt een vast contactpersoon (en vervanger) aan waarmee alle communicatie tussen de Opdrachtgever en de Opdrachtnemer kan plaatsvinden.

3.2.5 Op zowel operationeel, tactisch als strategisch niveau kan (zowel structureel of op verzoek van Opdrachtgever/Opdrachtnemer) overleg plaatsvinden tussen de betrokken medewerkers op het betreffende onderwerp indien dat leidt tot een betere/snellere en/of meer efficiënte werkwijze. Hier worden na gunning afspraken over gemaakt inclusief communicatiematrix en mandatering.

3.2.6 De Opdrachtnemer verzorgt maandelijks standaard managementrapportages op strategisch, tactisch en operationeel niveau. Gedurende de eerste periode na implementatie wordt gezamenlijk bepaald op welke wijze welke informatie wordt gepresenteerd. Bij de Inschrijving dienen voorbeeldrapportages te worden meegestuurd.

3.2.7 Geautoriseerde gebruikers van Opdrachtgever kunnen zelfstandig managementrapportages genereren op basis van vrij instelbare query's/selecties. Deze query's, selecties en rapportages beperken zich tot datgene waarvoor betreffende gebruiker is geautoriseerd en zijn uitsluitend toegankelijk voor gebruikers met gelijke autorisatie.

3.2.8 Data uit het handhavingssysteem dient geëxporteerd te kunnen worden naar gangbare bestandstypen, minimaal naar PDF, Excel en/of naar csv. Dit geldt ook voor 1 op n relaties ten behoeve van verwerking buiten het handhavingssysteem.

4 Eisen aan de dienstverlening

4.1 Eisen privacy en informatiebeveiliging

4.1.1 Opdrachtnemer dient ISO27001, dan wel aantoonbaar gelijkwaardig, gecertificeerd te zijn. Dit geldt tevens voor eventuele onderaannemers van Opdrachtnemer.

4.1.2 Het volledige Handhavingssysteem inclusief bijbehorende koppelingen dienen te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) alsmede Wet politiegegevens (Wpg). Indien een medewerker werkt in een proces dat valt onder de reikwijdte van Wpg, dient dit voor de medewerker duidelijk zichtbaar te zijn in de handhaaf-app en/of backoffice-omgeving.

4.1.3 Opdrachtnemer dient actief bij te dragen aan het doorlopen van het gemeentelijke DPIA-proces en daaruit voortvloeiende noodzakelijke aanpassingen aan de software en/of koppelingen door te voeren.

4.1.4 Het volledige Handhavingssysteem inclusief bijbehorende koppelingen dienen te zijn ontwikkeld conform de principes van Security- en Privacy-by-Design alsmede Security- en Privacy-by-Default.

4.1.5 Het volledige Handhavingssysteem dient de functionele en technische mogelijkheden te hebben, zodat de Opdrachtgever kan voldoen aan de Baseline Informatie Beveiliging Nederlandse Gemeenten (BIG)/Baseline Informatiebeveiliging Overheid (BIO).

4.1.6 Opdrachtnemer dient te beschikken over een interne procedure met betrekking tot ‘Responsible Disclosure’. Onder Responsible Disclosure wordt verstaan dat wanneer een persoon die beroepsmatig of bij toeval een kwetsbaarheid tegen komt in een applicatie en dit meldt bij Opdrachtnemer, deze de kwetsbaarheid adequaat oplost voordat deze bekend wordt.

4.1.7 De hosting van het Handhavingssysteem dient plaats te vinden bij een provider die niet onder de US Patriot Act valt en op servers die zijn gevestigd binnen de Europese Economische Ruimte.

4.1.8 Opdrachtnemer dient medewerking te verlenen aan audits op verzoek van Opdrachtgever (‘right to audit’).

4.1.9 Voor zover (delen van) de applicatie als een clouddienst wordt aangeboden, dient hiervoor periodiek, minimaal 1 keer per jaar, een Grey box pentest (inclusief kwetsbaarheidsscan), uit te voeren door een onafhankelijke gecertificeerde partij, te worden doorlopen. De resultaten van deze pentest, de opvolging van de testresultaten en de oplossing, inclusief oplossingstermijn, van ‘high risk’ bevindingen dienen te worden gerapporteerd aan Opdrachtgever. De kosten voor deze test zijn voor rekening van Opdrachtnemer.

4.1.10 Alle dataverbindingen tussen onderdelen van het Handhavingssysteem dienen beveiligd te zijn.

4.1.11 Opdrachtgever is eigenaar van alle data die met behulp van het Handhavingssysteem wordt vergaard door gebruikers van Opdrachtgever. Opdrachtnemer mag deze data gebruiken voor zover dit noodzakelijk is voor de uitvoering van de dienstverlening.

4.1.12 Het kopiëren, muteren of verwijderen van data is niet toegestaan zonder expliciete schriftelijke toestemming van Opdrachtgever.

4.1.13 Voor zover (delen van) het Handhavingssysteem toegankelijk dienen te zijn voor geautoriseerde medewerkers van Opdrachtgever, dienen deze gebruikt te kunnen worden met minimaal de laatste 3 versies van de browser Microsoft Chromium - Edge. Daarbij is het niet toegestaan dat lokaal plug-ins of andersoortige (installatie)bestanden opgeslagen dienen te worden.

4.1.14 Geautoriseerde medewerkers van Opdrachtgever of Opdrachtnemer dienen uitsluitend toegang te kunnen verkrijgen tot (delen van) het Handhavingssysteem middels een persoonsgebonden login en 2-factor authenticatie.

4.1.15 Geautoriseerde medewerkers van Opdrachtgever dienen toegang te kunnen verkrijgen tot (delen van) de applicatie middels Single-Sign-On, waarbij de Microsoft Azure Active Directory protocollen worden ondersteund.

4.1.16 Single Sign on gebeurt op basis van least privelege. De Opdrachtnemer dient aan te tonen en te onderbouwen welke premissies, attributen en/of claims nodig zijn om de koppeling op te zetten. (SSO, SCIM en SP(N)).

4.1.17 Single Sign on voor de testomgeving en productieomgeving van het Handhavingssysteem lopen niet via dezelfde koppeling en dienen dus elk een eigen koppeling te hebben.

4.1.18 Encryptie & hashing algoritmes dienen te voldoen aan de FIPS standaard N-1 (meest recente definitieve versie of 1 versie lager)

4.1.19 Te beschermen gegevens dienen veilig te opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als dit noodzakelijk is.

4.1.20 Het Handhavingssysteem voorziet in validatiecontroles in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken. De Opdrachtnemer heeft beheersmaatregelen geïmplementeerd voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

4.1.21 Het Handhavingssysteem moet voorzien zijn van strikte input- en output-validatiemechanismen. Voor de input houdt dit in dat alle ontvangen gegevens, of deze nu van gebruikers, andere systemen of bestanden afkomstig zijn, gecontroleerd en gevalideerd worden op veiligheid en correctheid voordat ze worden verwerkt. Dit is essentieel om beveiligingsrisico's zoals SQL-injectie, cross-site scripting en andere potentiële aanvallen te voorkomen. Wat betreft de output, moeten alle gegevens die naar externe bestemmingen worden verzonden, zorgvuldig worden gecontroleerd en gevalideerd om te waarborgen dat er geen gevoelige informatie wordt gelekt en dat de gegevens correct worden weergegeven. De implementatie en werking van deze validatiemechanismen dienen in lijn te zijn met de richtlijnen zoals beschreven in NORA online met betrekking tot input-/output-validatie.

4.1.22 Session time-out instellingen (Idle, Absolute, Renewal) voor het webbased gedeelte van het Handhavingssysteem zijn zo ingesteld dat de onderstaande maximale tijden niet worden overschreden.

4.1.23 Time-out voor inactiviteit (Idle): maximaal 15 minuten voor toepassingen met hoog risico of na handmatig beëindigen van de sessie (BBN 2 of hoger)

4.1.24 Absolute time-out: maximaal 4 uur of na handmatig beëindigen van de sessie

4.1.25 Verlenging Time-out (Renewal): maximaal ieder uur midden in de gebruikerssessie, en onafhankelijk van de sessieactiviteit en dus van de time-out voor inactiviteit, dient er automatisch een nieuw sessie ID te worden gegenereerd welke, met een veiligheidsinterval van max 10 minuten, automatisch overgang verzorgt van het oude naar het nieuwe sessie ID en hiermee het voorgaande sessie ID ongeldig maakt.

4.1.26 Voor het installeren van extensies in de Edge Browser dient de Opdrachtnemer het ID en de URL van de Edge-browserextensie aan te leveren. Een extensie op een andere manier installeren wordt niet ondersteund door de Opdrachtgever.

4.1.27 Het Handhavingssysteem gebruikt minimaal de onderstaande Security Headers, conform best practices van het OWASP https://owasp.org/www-project-secure-headers.

- Strict-Transport-Security (HSTS)
- Content-Security-Policy (CSP)
- X-Content-Type-Options
- Referrer-policy
- X-Frame-Options
- Permissions-Policy

4.1.28 De Opdrachtnemer is verantwoordelijk voor de beveiliging en updates van het Handhavingssysteem. Kwetsbaarheden worden conform de SLA-oplostijden opgelost. De Opdrachtnemer dient een WAF (Web Application Firewall) en antivirus te gebruiken. Het Handhavingssysteem moet worden ingericht volgens best practices, huidige technologische standaarden en het Zero Trust-principe. Daarnaast dient de leverancier te voldoen aan de volgende eisen:

- Encryptie: Alle gegevens, zowel in transit als in rust, moeten worden versleuteld met encryptiealgoritmes conform eis SECA08.
- Toegangsbeheer: Er moet een robuust toegangsbeheerbeleid zijn, inclusief multi-factor authenticatie (MFA) voor alle beheerders en personen met toegang vanuit de leverancier.
- Data Back-up en Herstel: Back-ups van alle gegevens moeten worden uitgevoerd conform RTO en RPO (zie paragraaf 4.10). Er moet een gedetailleerd disaster recovery plan zijn om snelle herstelmaatregelen te garanderen in geval van gegevensverlies. De back-up moet op een andere locatie zijn dan de locatie van het live systeem.

- Monitoring en Logging: Continue monitoring en logging van alle activiteiten binnen de applicatie conform eis 4.3.13 om verdachte activiteiten snel te detecteren en hierop te reageren.
- Datacenter: Tier 2 of hoger

4.1.29 Het Handhavingssysteem dient de mogelijkheid te bieden om op procesniveau in te richten wat er moet gebeuren bij het uitvoeren van een vernietigingsactie. Gegevens moeten bewaard, verwijderd of geanonimiseerd kunnen worden.

4.1.30 Informatieobjecten, gegevens en bijbehorende metadata (op verschillende aggregatieniveaus: melding/dossier/zaak en onderliggende documenten, bestanden, elementen in een database, koppelingen met klantprofielen of persoonsgegevens) moeten onherstelbaar kunnen worden vernietigd op basis van de als zoekcriteria opgegeven metadata. Er is geen limiet aan het aantal items dat vernietigd kan worden.

4.1.31 Wanneer voor zoeken en vinden gebruik wordt gemaakt van indexering, dient de index na vernietiging te worden geactualiseerd zodat vernietigde informatie niet meer gevonden kan worden.

4.1.32 Metadata of gegevens ten behoeve van authenticatie (Iets wat je hebt, bent of weet of mogelijk metadata tbv tijd en plaats) dienen te kunnen worden uitgewisseld met informatiesystemen. Bijvoorbeeld Identity & Access Management (IDM) of Azure ten behoeve van SSO.

4.1.33 De Opdrachtnemer moet jaarlijks zorgdragen voor een erkende en recente TPM-verklaring afgegeven door een geregistreerde EDP/ Norea auditor

4.1.34 Software libraries binnen het Handhavingssysteem mogen niet EOL (End-of-life) zijn. Update mag N-1 zijn.

4.1.35 Security incidenten en datalekken dienen gemeld te worden bij de Opdrachtgever binnen 48 uur. Security issues dienen opgelost te worden op basis van CVSS-score:

- Kritiek – Oplossen binnen 1 dag
- High – Oplossen binnen 1 week
- Medium – Oplossen binnen 2 maanden
- Low – Oplossen in overleg

4.1.36 Indien er sprake is van het gebruik van DigiD als koppeling in een applicatie dient vastgelegd te worden in de SLA dat de verbinding jaarlijks getoetst/geaudit wordt. De Opdrachtnemer is hiervoor verantwoordelijk.

4.2 Algemene eisen handhavingssysteem

4.2.1 Het Handhavingssysteem dient als SAAS-oplossing te worden geleverd, inclusief alle benodigde licenties voor de duur van de overeenkomst. Er dienen minimaal 150 gelijktijdig te gebruiken gebruikerslicenties beschikbaar te zijn voor alle rollen en medewerkers die met het Handhavingssysteem moeten werken. Het aantal gebruikers moet verder uitgebreid kunnen worden, zonder dat daarvoor ingrijpende wijzigingen aan het Handhavingssysteem noodzakelijk zijn.

4.2.2 Het Handhavingssysteem wordt volledig gehost, onderhouden, technisch beheerd, beveiligd en periodiek geüpdatet door Opdrachtnemer. De kosten voor deze werkzaamheden zijn volledig inclusief bij het bedrag van de Inschrijving.

4.2.3 Wettelijke wijzigingen, die van invloed zijn op de werking of het gebruik van het Handhavingssysteem, dienen bij ingang van de nieuwe wetgeving zijn geïmplementeerd.

4.2.4 Voordat een update van het Handhavingssysteem of van systemen waarmee wordt gekoppeld, wordt geïmplementeerd, dient Opdrachtnemer deze update te testen met de ketenpartners en Opdrachtgever om verstoringen binnen de keten te voorkomen. Opdrachtnemer dient hiervoor een permanente test-omgeving van het Handhavingssysteem in te richten en te onderhouden., waarop Opdrachtgever en Opdrachtnemer kunnen testen en accepteren, voordat een update in de productie-omgeving van het Handhavingssysteem wordt doorgevoerd. Voor elk update levert Opdrachtnemer een concept testplan ter goedkeuring aan Opdrachtnemer.

4.2.5 Op de test-omgeving dienen ook andere (test-)omgevingen gekoppeld te kunnen worden, teneinde ketentesten mogelijk te maken.

4.2.6 Opdrachtnemer dient upgrade van de software (zoals de toevoeging van extra functionaliteiten) binnen 3 maanden na de release van de upgrade aan te bieden aan Opdrachtgever.

4.2.7 Opdrachtnemer levert over de werking van het Handhavingssysteem de volgende documentatie in digitale vorm aan in het Nederlands (tenzij het algemeen gangbare niet-Nederlandse terminologie betreft):

- Technische documentatie (waaronder architectuurplaten)
- Beschrijving van de koppelingen
- Gebruikershandleidingen

4.2.8 Binnen het Handhavingssysteem moeten aan (groepen van) gebruikers verschillende rechten en autorisaties op eenvoudige wijze toegekend en aangepast te kunnen worden.

4.2.9 Alle protocollen die worden gebruikt in de het Handhavingssysteem staan in de verplichte of aanbevolen standaarden van Forum Standaardisatie en voldoen aan de vereiste versie of hoger.

4.2.10 Het Handhavingssysteem dient blijvend te voldoen aan de meest actuele NCSC-richtlijnen voor wat betreft de ICT-beveiligingsrichtlijnen voor webapplicaties, TLS, Mobile apps en HTTPS.

4.2.11 Het Handhavingssysteem verzendt geen telemetrie naar de Opdrachtnemer welke niet is vastgelegd in de documentatie. Indien door wijzigingen in het Handhavingssysteem (updates, nieuwe functionaliteiten, etc) de inhoud van de telemetrie verandert, mag dit enkel worden verzonden naar de Opdrachtnemer na schriftelijke goedkeuring door de Opdrachtgever. De Opdrachtnemer stemt in dat deze veranderingen met de Opdrachtgever vooraf schriftelijk wordt afgestemd.

4.2.12 Het Handhavingssysteem gebruikt alleen externe componenten (bijvoorbeeld libraries) welke geen bekende kwetsbaarheden bevatten (CVSS en/of CVE) en nog steeds actief geüpdatet en ondersteund worden door hun leverancier en/of ontwikkelaar.

4.2.13 De SSL Cipher Suites volgorde is zo ingesteld dat deze als eerst gebruikt maakt van het sterkste Cipher en zo aflopend. Hierbij gebruikt de Opdrachtnemer enkel ciphers met de status goed en/of voldoende van het NCSC.

4.2.14 Het Handhavingssysteem is benaderbaar zowel IPv4 als IPv6.

4.2.15 Binnen het Handhavingssystemen dienen informatieobjecten (documenten, meldingen, zaken, dossiers, e-mails, tekstberichten en andere bestandsformaten) in relatie met elkaar worden beheerd.

4.2.16 Het Handhavingssysteem dient de geanonimiseerde versie van een document als een apart document op te slaan, in relatie tot het origineel.

4.2.17 Indien een document binnen het Handhavingssysteem aan meerdere zaken, meldingen of dossiers is gekoppeld, dient het document even lang bewaard te blijven als de langste bewaartermijn van de gekoppelde zaken, meldingen en dossiers.

4.2.18 De Opdrachtnemer volgt de richtlijnen van DigiToegankelijk voor het ontwikkelen en opleveren van websites en apps volgens de geldende EN 301 549 richtlijnen (zie https://digitoegankelijk.nl/leveranciers en https://digitoegankelijk.nl/toegankelijkheidsverklaring/onderzoek)

4.2.19 Elke 3 jaar dat de overeenkomst met de Opdrachtnemer voortduurt, voert de Opdrachtnemer opnieuw een onderzoek uit op het gebied van digitoegankelijkheid volgens de op dat moment geldende EN 301 549 richtlijnen. Wijzigingen inclusief een vernieuwde toegankelijkheidsverklaring worden opnieuw aangeleverd bij de Opdrachtgever voor verwerking in het landelijk register

4.3 Eisen aan gebruikersbeheer en functioneel beheer

4.3.1 Het Handhavingssysteem heeft een functionaliteit voor Opdrachtgever om, zonder de inzet van consultancy van Opdrachtnemer, ten minste te kunnen invoeren, wijzigen, verwijderen en toewijzen:

- Gebruikers
- Handhavers en/of groepen van handhavers
- Standaardteksten (t.b.v. (aankondigingen van) beschikkingen, meldingen, waarschuwingen)
- Straten, zones, buurten, wijken en gebieden
- Soorten overtredingen (registraties)
- Feitenboekje (inclusief een importfunctie)
- APV-informatie (inclusief een importfunctie)
- Tarieven
- Vragenlijsten
- Workflows
- Processen
- Invoerschermen

4.3.2 De functioneel beheerders van de Opdrachtgever moeten zelf een gebruiker kunnen toevoegen, wijzigen of beëindigen in het handhavingssysteem.

4.3.3 Standaard autorisatieprofielen moeten door de functioneel beheerders van de Opdrachtgever zelf te kunnen worden gedefinieerd. Deze profielen worden toegewezen aan individuele gebruikers op basis van hun rol (Role Based Acces - RBAC)

4.3.4 Autorisaties moeten worden toegekend op functionaliteit met toegang tot die modules die de gebruiker nodig heeft voor zijn of haar werkprocessen.

4.3.5 Autorisaties moeten worden toegekend op inhoud (data). Niet alle gebruikers die dezelfde functionaliteit hebben zien dezelfde data.

4.3.6 Het handhavingssysteem moet de mogelijkheid bieden om verschillende beheerders/keyusers een verschillend niveau van rechten als beheerder toe te wijzen met behulp van RBAC.

4.3.7 De standaardrapportages over de ingerichte autorisatiematrix en de manier waarop gebruikers gekoppeld werden aan de autorisatiematrix, zijn beschikbaar vanuit de Programmatuur voor Functioneel beheer van de Opdrachtgever.

4.3.8 De gebruiker moet inloggen in de applicatie volgens de door de Opdrachtgever gestelde technische en security eisen (zie 4.1.14).

4.3.9 De functioneel beheerder van de Opdrachtgever moet een secundair inlogkanaal hebben om te garanderen dat hij of zij altijd toegang heeft tot het handhavingssysteem.

4.3.10 Het Handhavingssysteem dient voor de schrijfwijze van straatnamen gebruik te maken van het BAG-adressenbestand. Adresgegevens dienen zowel handmatig ingevuld te kunnen worden (waarbij gegevens worden gecontroleerd met het BAG en, na bevestiging door de gebruiker, uit het BAG overgenomen kunnen worden) als via de plaatsbepaling van de smartphone automatisch te kunnen worden bepaald.

4.3.11 Het Handhavingssysteem dient de invoer van speciale tekens (waaronder diakritische tekens) te ondersteunen.

4.3.12 Het Handhavingssysteem dient te beschikken over een spellingscontrole-functionaliteit.

4.3.13 Het Handhavingssysteem dient een logging bij te houden van alle individuele handelingen van gebruikers en beheerders. De toegang tot en inzage in deze logging dient te zijn voorbehouden aan specifiek geautoriseerden, inzages dienen te worden gelogd in de logging. In de logging dient minimaal te worden vastgelegd:

- Een tot een natuurlijke persoon herleidbare gebruikersnaam of ID;
- De gebeurtenis;
- Waar mogelijk de identiteit van het werkstation;
- Host naam;
- Naam van de toepassing;
- IP-adres(sen);
- Het object waarop de handeling werd uitgevoerd;
- Het resultaat van de handeling;
- De datum en het tijdstip van de gebeurtenis.

De logging dient gefilterd te kunnen worden. De logging dient 1 jaar te worden bewaard. In geval van een incident dient de logging omtrent het incident 3 jaar te worden bewaard.

4.3.14 Het Handhavingssysteem dient alle gegenereerde data te bewaren, met inachtneming van huidige en toekomstige bepalingen in regelgeving inzake privacy en de Archiefwet. Bij het bereiken van een (instelbare) maximale bewaartermijn dienen gegevens automatisch te worden geanonimiseerd danwel verwijderd.

4.3.15 De functioneel beheerders dienen onjuiste handelingen van gebruikers herstellen, mits dit geen handelingen betreft die voorbehouden zijn aan BOA's. Voor dergelijke herstelacties dient een beheerdershandleiding te worden verstrekt.

4.3.16 De functioneel beheerders dienen binnen het handhavingssysteem te kunnen switchen naar wat een gebruiker (met een andere rol/autorisatie) kan en ziet, ten behoeve van gerichte ondersteuning.

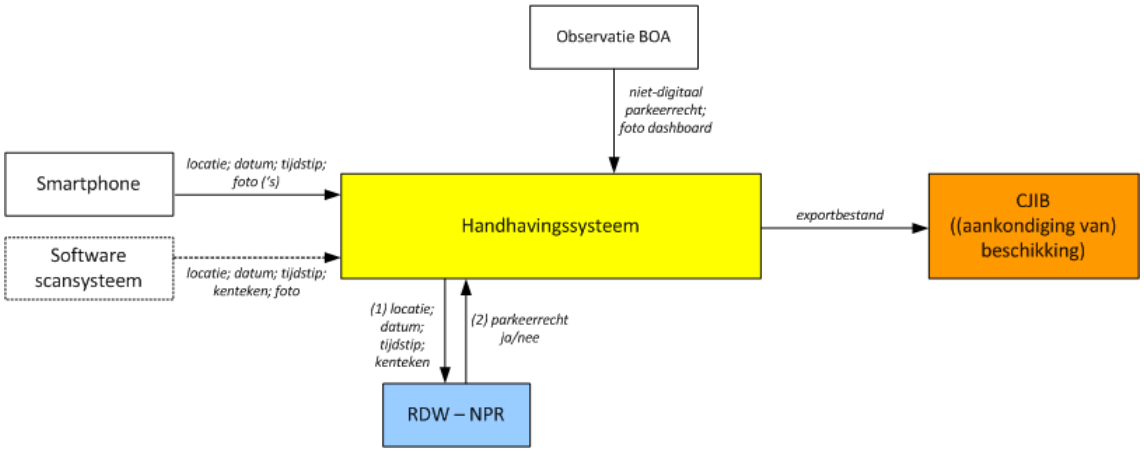
4.3.17 Het Handhavingssysteem dient te koppelen met het MIM/Azure systeem van de Opdrachtgever zodat gegevens van gebruikers/personeel op één centrale plaats beheerd worden.

4.3.18 De Opdrachtnemer dient inzicht te bieden in de samenhang tussen de verschillende entiteiten voor functioneel beheer door de Opdrachtgever (bij voorkeur door het beschikbaar stellen van het datamodel).

4.3.19 Bij nieuwe releases van het Handhavingssysteem dienen bestaande data in het systeem toegankelijk te blijven, zonder verandering van inhoud en structuur en verlies van functionaliteit. Ook de oorspronkelijke metadata dient behouden te blijven.

4.3.20 Indien voor het Handhavingssysteem gebruik gemaakt wordt van certificaten dient voor de Functioneel Beheerder van de Opdrachtgever inzichtelijk te zijn welke certificaten gebruikt worden, wat de looptijd is en wie verantwoordelijk is voor tijdige signalering en verlenging.

4.4 Administratiefrechtelijke handhaving parkeren



Figuur 2: schema Administratiefrechtelijke handhaving parkeren

4.4.1 Het Handhavingssysteem dient met behulp van de Smartphone uit op locatie gemaakte foto's of beelden het kenteken van een geparkeerd voertuig te herkennen. Deze herkenning dient een juistheid van 99,5% te hebben op een afstand van 10 meter.

4.4.2 Het Handhavingssysteem dient het herkende kenteken te bevragen op een geldig parkeerrecht voor de locatie bij het Nationaal Parkeer Register (NPR).

4.4.3 Indien sprake is van een geldig parkeerrecht voor de locatie, dienen de foto's of beelden direct en automatisch te worden verwijderd uit het Handhavingssysteem.

4.4.4 Het Handhavingssysteem dient de locatie en tijdstip van herkenning van een voertuig met een geldig (digitaal of niet-digitaal) parkeerrecht geanonimiseerd op te slaan.

4.4.5 Indien geen sprake is van een geldig parkeerrecht voor de locatie, dient het Handhavingssysteem de kentekenfoto plus het herkende kenteken te tonen. De BOA dient het kenteken handmatig te accorderen of te kunnen aanpassen, waarna opnieuw een bevraging bij het NPR plaatsvindt op een geldig parkeerrecht voor de locatie. In deze situatie dient het Handhavingssysteem te registreren dat het kenteken onjuist is herkend.

4.4.6 Indien uit de (her)bevraging blijkt dat geen sprake is van een geldig parkeerrecht, dient het Handhavingssysteem de BOA te instrueren een foto van het dashboard van het geparkeerde voertuig te maken.

4.4.7 Indien op het dashboard een geldig niet-digitaal parkeerrecht wordt geconstateerd, dient de BOA dit in het Handhavingssysteem te kunnen invoeren. In het Handhavingssysteem dient hiervoor een pull-down menu met limitatieve invoeropties (soorten niet-digitale parkeerrechten) beschikbaar te zijn. Na selectie van de juiste invoeroptie dient de BOA de invoer te bevestigen. Het Handhavingssysteem dient aansluitend de foto's of beelden waarop het kenteken zichtbaar is, direct en automatisch te verwijderen.

4.4.8 Indien de BOA beoordeelt dat sprake is van een "overtreding", dient de registratie door het Handhavingssysteem, middels een koppeling met het BRV ("Kentekenregister") van RDW, automatisch te worden verrijkt met de benodigde voertuiggegevens en te worden klaargezet in een voorraad 'te verzenden', welke periodiek wordt geëxporteerd ten behoeve van een upload naar het Centraal Justitieel Incasso Bureau. Deze export dient batchgewijs door de BOA te worden uitgevoerd aan het einde van een sessie in de beoordelingsmodule, voordat de BOA uit kan loggen uit het Handhavingssysteem. Alleen een teamleider van de BOA's dient de exports daadwerkelijk te kunnen uploaden naar het CJIB.

4.4.9 Voordat een export van de werkvoorraad 'te verzenden' plaatsvindt, dienen de kentekens van deze export minimaal éénmaal voor herbeoordeling op een geldig parkeerrecht aangeboden te worden aan het NPR. Kentekens waarvan dan alsnog een geldig parkeerrecht wordt gevonden, dienen uit de werkvoorraad te worden verwijderd.

4.5 Brede handhaving – algemene eisen

4.5.1 Het Handhavingssysteem dient de volledige processen die behoren tot de brede handhaving te kunnen doorlopen op zowel een mobiel device als een Windows-computer (desktop danwel laptop).

4.5.2 Het Handhavingssysteem voorziet in de mogelijkheid om bestaande processen gedurende de looptijd van de overeenkomst te wijzigen en om nieuwe processen in te richten. Het op verzoek van Opdrachtgever wijzigen of toevoegen van processen dient te worden doorgevoerd binnen een redelijke termijn passend bij de omvang van de werkzaamheden, doch in beginsel binnen een termijn van 2 maanden.

4.5.3 Het Handhavingssysteem dient processen zodanig in te richten dat de stappen binnen het proces, afhankelijk van de invoer of situatie, in een verschillende volgorde kunnen worden afgehandeld.

4.5.4 Het Handhavingssysteem dient de mogelijkheid te bieden dat bepaalde (invoer)velden verplicht ingevuld moeten worden voordat een processtap kan worden afgerond.

4.5.5 Het Handhavingssysteem dient zaken feit gecodeerd te kunnen afhandelen op basis van het vigerende zogenaamde Feitenboekje van het Openbaar Ministerie. Opdrachtnemer is gedurende de looptijd van de overeenkomst verantwoordelijk voor de tijdige verwerking in het Handhavingssysteem van gehele of gedeeltelijke aanpassingen van dit Feitenboekje. De kosten voor deze verwerking komen voor rekening van Opdrachtnemer.

4.5.6 Het Handhavingssysteem dient gegevens te kunnen verwerken zoals is vastgesteld in het model Combi-bon.

4.5.7 Het Handhavingssysteem is responsief opgebouwd. Gegevens van een zaak dienen automatisch te worden opgeslagen. Indien een zaak op een ander apparaat wordt geopend, al dan niet voor verdere afhandeling, dienen opgeslagen gegevens direct getoond te worden.

4.5.8 Het Handhavingssysteem is gebruikersvriendelijk. Stappen in de processen dienen op een logische wijze (intuïtief voor de gebruiker) doorlopen te kunnen worden, binnen een zaak mag het niet voorkomen dat gegevens vaker dan één keer moeten worden ingevoerd. Schermen dienen logisch van opbouw en onderling consistent te zijn, het noodzakelijk aantal schermwisselingen geminimaliseerd.

4.5.9 Het Handhavingssysteem dient dynamische vragenlijsten te kunnen toepassen, waarbij antwoordafhankelijk één of meerdere vragen kunnen worden overgeslagen. Binnen vragenlijsten dienen zowel open als voorgedefinieerde antwoordmogelijkheden te kunnen worden toegepast. Elke vragenlijst dient aangepast te kunnen worden, zonder dat data verloren gaat van zaken waarbij betreffende vragenlijst eerder is ingevuld.

4.5.10 Het Handhavingssysteem biedt de mogelijkheid om de daarvoor geschikte zaken en bijlagen (BUBS) te kunnen inlezen in de transactiemodule van het CJIB.

4.5.11 Het Handhavingssysteem dient het mogelijk te maken om de inhoud van periodieke briefings voor de brede handhaving te kunnen genereren en te uploaden. De briefings dienen inclusief bijlagen ingezien te kunnen worden door alle medewerkers, ongeacht welk device zij gebruiken.

4.5.12 Het Handhavingssysteem dient het mogelijk te maken om op een geografische ondergrond hotspot-gebieden te definiëren.

4.5.13 Voor hotspot-gebieden dient ingegeven te kunnen worden gedurende welke tijdsperiodes gehandhaafd dient te worden en voor welke processen van de brede handhaving deze geldt.

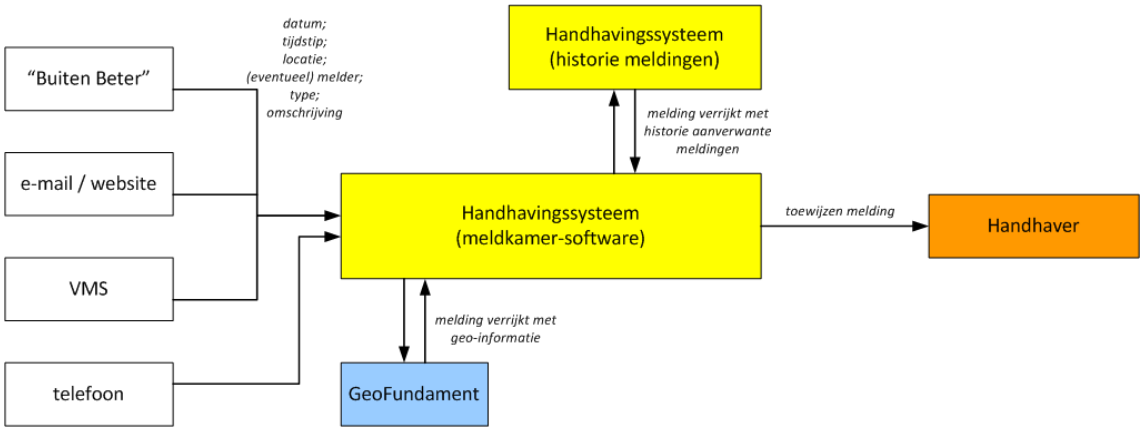
4.5.14 Aan hotspot-gebieden dienen specifieke vragenlijsten gekoppeld te kunnen worden.

4.5.15 Indien een handhaver binnen de aangegeven tijdsperiodes binnen een gedefinieerd hotspot-gebied komt, dient deze hiervan een melding te ontvangen.

4.5.16 Het Handhavingssysteem dient bij gegevensimporten in een lopende zaak of melding aan te kunnen geven wat met de geïmporteerde informatie gedaan moeten worden (overschrijven - altijd of alleen indien leeg, of toevoegen, wanneer een veld in bron of doel is gevuld met afwijkende gegevens).

4.6 Brede handhaving – eisen meldkamersoftware

Het Handhavingssysteem omvat een softwareoplossing waarmee de meldkamer de ondersteuning en coördinatie van de brede handhaving kan verzorgen. De meldkamer is het ontvangstpunt voor alle meldingen (zowel via het meldingensysteem BinnenBeter als per e-mail, de website, het VideoManagementSysteem) en telefonisch. De medewerker(s) van de meldkamer beoordelen of de meldingen worden doorgezet naar de handhavers op straat voor verdere afhandeling, dan wel anderszins worden opgepakt.



Figuur 3: schema Brede handhaving - meldkamersoftware

4.6.1 De meldkamersoftware dient een real-time koppeling te krijgen met het meldingensysteem van Gemeente Eindhoven (BinnenBeter). De meldkamersoftware dient zaken te kunnen ontvangen die via een e-mailadres of berichtenmodule op de gemeentelijke website, of via het Video Management Systeem worden aangeleverd. Deze meldingen en zaken komen binnen bij de Centrale Meldkamer, waarbij voor elke melding of zaak:

- de meldkamersoftware een zaak dient aan te maken,
- de meldkamersoftware voor elke zaak een brondocument dient in te vullen met van de melding/zaak tenminste: datum, tijdstip, locatie, de eventuele melder, type en een nadere beschrijving, inclusief eventueel beeldmateriaal (foto's/video's),
- voor deze zaak de historie van aanverwante meldingen/zaken kan worden bevraagd, waarbij de medewerker kan selecteren op basis van welke criteria de bevraging plaatsvindt, en deze historie (deels) kan worden toegevoegd aan deze zaak,
- de zaak, met eventuele gekoppelde zaken, inclusief eventuele deadlines kan worden toegewezen aan een (groep van) handhaver(s).

4.6.2 De medewerker van de meldkamer dient telefonische meldingen te kunnen verwerken in de meldkamersoftware. Voor elke telefonische melding:

- dient de meldkamersoftware een zaak aan te maken,
- dient de medewerker het brondocument te kunnen invullen met van de melding tenminste: datum, tijdstip, locatie, de melder, type en een nadere beschrijving.
- dient de meldkamersoftware voor de aangemaakte zaak de historie van aanverwante meldingen/zaken te kunnen bevragen, waarbij de medewerker kan selecteren op basis van welke criteria de bevraging plaatsvindt, en deze historie (deels) kan worden toegevoegd aan deze zaak,
- dient de medewerker de zaak, met eventuele gekoppelde zaken, inclusief eventuele deadlines te kunnen toewijzen aan een (groep van) handhaver(s).

4.6.3 De meldkamersoftware dient de mogelijkheid te bieden om meldingen van het meldingensysteem (BinnenBeter) te kunnen afhandelen.

4.6.4 De meldkamersoftware dient actief signaleringen van naderende deadlines én van overschreden deadlines te genereren. Vanuit deze signalering dient direct toegang tot betreffende zaken te worden verkregen, waarbij de stand van zaken van afhandeling én welke medewerkers zijn betrokken bij de afhandeling inzichtelijk is.

4.6.5 Bij ontvangst van vervolgacties uit de back-office in de meldkamersoftware, dient de medewerker deze, inclusief deadline, te kunnen toewijzen aan een (groep van) handhaver(s).

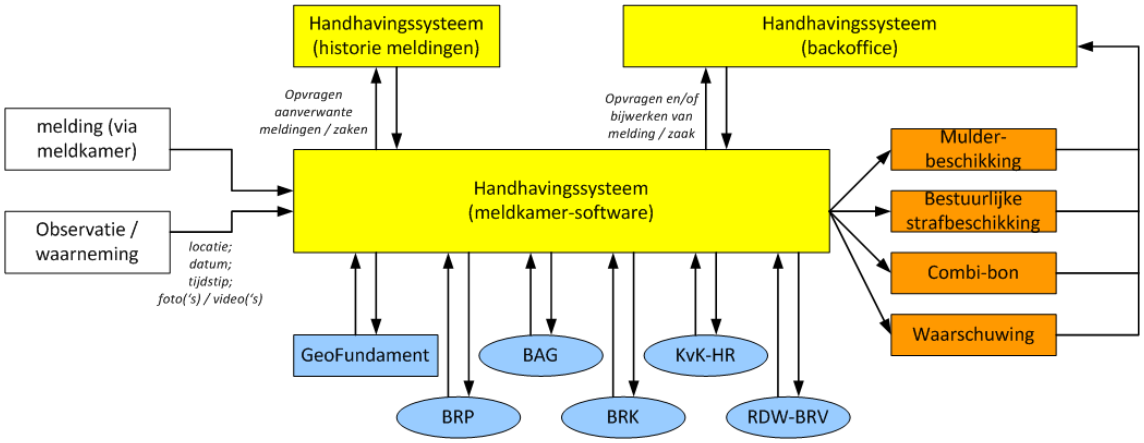
4.6.6 De meldkamersoftware dient een overzichtelijke weergave te bieden van lopende meldingen, voorzien van tijdstip van melding, uitgezette acties en afhandelingsstatus.

4.6.7 De meldkamersoftware dient een dashboard-weergave te bieden met een real-time overzicht van alle meldingen, de behandelaar(s), afhandelingsstatus, doorlooptijden en afhandeltijden.

4.6.8 De meldkamersoftware dient een real-time kaartweergave te bieden met de GPS-locaties van alle devices waarop de handhaaf-app is geactiveerd. Van de devices waarop de handhaaf-app niet actief is, dient de GPS-locatie niet te worden getoond.

4.7 Brede handhaving – eisen handhaaf-app

Het Handhavingssysteem omvat een handhaaf-app, te installeren op en te gebruiken via een smartphone of tablet, ten behoeve van de uitvoering van de brede handhaving (inclusief administratiefrechtelijke parkeer- en verkeershandhaving) op straat. Levering van de handhaaf-app in de vorm van een web-app is toegestaan.



Figuur 4: schema Brede handhaving - handhaaf-app

4.7.1 De handhaaf-app dient op de mobiele devices van Gemeente Eindhoven te kunnen worden geïnstalleerd. Indien de handhaaf-app specifiek als app (dus geen web-app) wordt aangeboden dient deze via de Playstore en/of App-store ter beschikking te worden gesteld.

4.7.2 Het instellen van pincodes en/of biometrische authenticatie voor iOS en Android apps vereist eenmalig het gebruik van Multi Factor Authenticatie, E-herkenning of DigiD tijdens de initiële configuratie. Na deze initiële opzet is het niet toegestaan dat het gebruik van E-herkenning, DigiD of Multi Factor Authenticatie nodig is voor toegang via de ingestelde pincode of biometrische gegevens.

4.7.3 De handhaaf-app dient ten minste te beschikken over de functionaliteiten:

a. Het aanmaken, opvragen, verwerken, bijwerken en afronden van een melding of zaak tot een sanctie (Mulder, BSB, combi-bon of waarschuwing) of geregistreerde waarneming.
b. Het aanmaken, verwerken en afronden van staande houdingen.
c. Het invoeren van een adres en/of het selecteren van een voorgesteld adres op basis van de GPS-locatie, inclusief adrescontrole in BAG
d. Het invoeren van documentnummers van identiteitsbewijzen.
e. Het invoeren van BurgerServiceNummers (BSN), inclusief controle in BRP.
f. Het invoeren van NAW-gegevens, inclusief adrescontrole in het BAG en/of het selecteren van voorgestelde NAW-gegevens op basis van het BSN.

g. Het raadplegen van de Basisregistraties (BRK, KvK-HR, uitgebreide bevraging RDW-BRV)
h. Het raadplegen van geo-thematische kaarten in GeoFundament op basis van de GPS-locatie en/of invoer van een adres
i. Het koppelen van ten minste 10 foto's en 5 video's aan een melding of zaak.
j. Het tonen op een geografische weergave, met een instelbaar schaalniveau, op basis van de GPS-locatie en/of invoer van een adres, en raadplegen van aanverwante meldingen of zaken, waarbij situationeel de criteria voor 'aanverwant' kunnen worden ingesteld.
k. Het vrij invoeren van toelichtingen bij keuze-opties (bijvoorbeeld het opnemen van een eigen verklaring van een betrokkene bij een melding), waarbij het minimum/maximum in te voeren karakters vrij instelbaar is.
l. De mogelijkheid om HALT-afdoening aan te bieden bij een combi-bon, inclusief vastlegging van de keuze.
m. De volledige afhandeling van de wegsleepregeling voor motorvoertuigen.
n. Het aanbieden van (vooraf gedefinieerde) standaardteksten, die door de handhaver geselecteerd kunnen worden bij het opstellen van een registratie of het afhandelen van een zaak. Deze standaardteksten moeten aangevuld kunnen worden met vrije invoer-teksten. Per type registratie/zaak dient ingesteld te kunnen worden welke standaardteksten relevant zijn en aangeboden worden.

4.7.4 De handhaaf-app dient op basis van de GPS-locatiebepaling van het mobiele device de wijk, buurt, straatnaam en dichtstbijzijnde huisadres te kunnen tonen.

4.7.5 Een zaak wordt binnen de handhaaf-app opgeslagen totdat deze wordt verzonden naar de back-office.

4.7.6 Een zaak kan tot verzending op elk moment worden geopend, bijgewerkt en weer afgesloten.

4.7.7 Na afronding en verzending van een zaak, dient deze niet meer te kunnen worden gewijzigd, maar nog wel te kunnen worden aangevuld.

4.7.8 Na afronding en verzending van een zaak, waarbij sprake is van afhandeling op een feitcode, kan de beslissing binnen een instelbare termijn, uitsluitend onder vermelding van de reden, worden geseponeerd.

4.7.9 Indien een waarschuwing is opgemaakt, dient deze door alle handhavers direct ingezien te kunnen worden.

4.7.10 De handhaaf-app dient te beschikken over een signaleringsfunctie, wanneer de gebruiker binnen de vastgestelde tijdsperioden binnen grenzen van een aangewezen hotspot-gebied komt. Alsdan wordt getoond voor welke processen van de brede handhaving de hotspot-aanwijzing geldt.

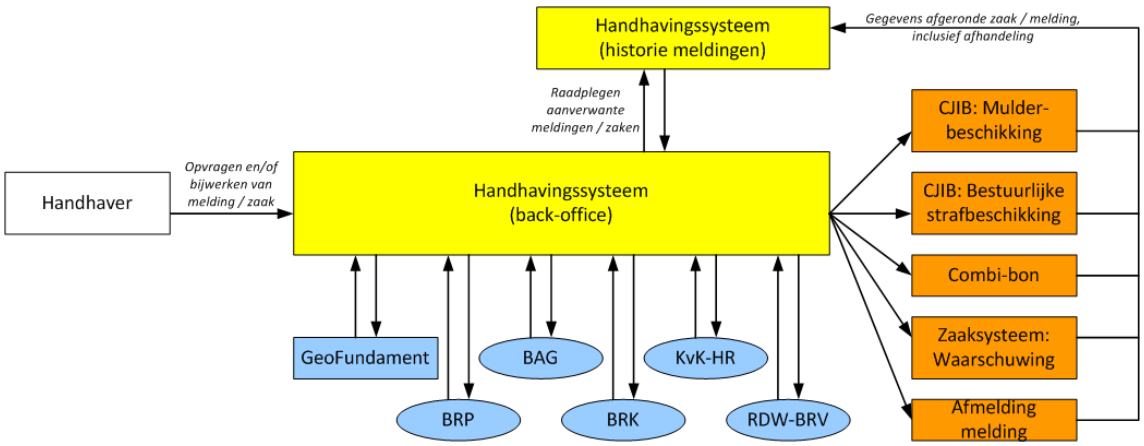
4.7.11 De handhaaf-app dient te beschikken over een leesfunctie van briefings.

4.7.12 De handhaaf-app dient automatisch te worden vergrendeld na een door Opdrachtgever te bepalen termijn van inactiviteit. Bij automatische vergrendeling blijven de ingevoerde gegevens behouden. De handhaaf-app kan eenvoudig worden ontgrendeld, bijvoorbeeld door de standaard ontgrendelfunctie van het mobiele device.

4.7.13 De user interfaces voor gebruikers zijn web-based en voldoen aan WCAG2.1. Alle user interfaces zijn geschikt voor alle gangbare mobiele apparaten (tablets, smartphones).

4.8 Brede handhaving – eisen back-office

Het Handhavingssysteem omvat een back-office omgeving waarin vanaf een Windows-computer zaken kunnen worden uitgewerkt, aangevuld, en afgerond, inclusief terugkoppeling naar het meldingensysteem BinnenBeter en het genereren van te verzenden brieven (notificaties). Vanuit de back-office omgeving vindt de batch-gewijze (BUBS) verzending van op feitcode afhandelde zaken naar de exportmodule van CJIB plaats.



Figuur 5: schema Brede handhaving - back-office

4.8.1 De back-office dient ten minste te beschikken over de functionaliteiten:

a. Het aanmaken, opvragen, verwerken, bijwerken en afronden van een melding of zaak tot een sanctie (Mulder, BSB, combi-bon of waarschuwing), een geregistreerde waarneming of een afhandeling van een melding in het meldingsysteem BinnenBeter.
b. Het aanmaken, verwerken en afronden van staande houdingen.
c. Het invoeren en/of aanpassen van een adres.
d. Het invoeren van documentnummers van identiteitsbewijzen.
e. Het invoeren van BurgerServiceNummers (BSN), inclusief controle in BRP.
f. Het invoeren van NAW-gegevens, inclusief adrescontrole in het BAG en/of het selecteren van voorgestelde NAW-gegevens op basis van het BSN.
g. Het raadplegen van de Basisregistraties (BRK, KvK-HR, RDW-BRV)
h. Het raadplegen van geo-thematische kaarten in GeoFundament op basis van de invoer van een adres
i. Het koppelen van ten minste 10 foto's en 5 video's aan een melding of zaak.
j. Het zonder informatieverlies koppelen van aangemaakte of ontvangen elektrische berichten aan een melding of zaak.
k. Het raadplegen van aanverwante meldingen of zaken in de meldingenhistorie, waarbij situationeel de criteria voor 'aanverwant' kunnen worden ingesteld.
l. Het vrij invoeren van toelichtingen bij keuze-opties (bijvoorbeeld het opnemen van een eigen verklaring van een betrokkene bij een melding), waarbij het minimum/maximum in te voeren karakters vrij instelbaar is.
m. De mogelijkheid om HALT-afdoening aan te bieden bij een combi-bon, inclusief vastlegging van de keuze.
n. Het aanbieden van (vooraf gedefinieerde) standaardteksten en standaardbrieven in de gemeentelijke huisstijl, die door de handhaver geselecteerd kunnen worden bij het opstellen van een registratie of het afhandelen van een zaak. Deze standaardteksten moeten aangevuld kunnen worden met vrije invoer-teksten. Per type registratie/zaak dient ingesteld te kunnen worden welke standaardteksten/-brieven relevant zijn en aangeboden worden.

4.8.2 Na afronding van een zaak, waarbij sprake is van afhandeling op een feitcode, kan de beslissing binnen een instelbare termijn, uitsluitend onder vermelding van de reden, worden geseponeerd. Deze seponering dient te worden gelogd.

4.8.3 Een geseponeerde zaak mag niet worden meegenomen in het exportproces, de seponering dient wel opvraagbaar te blijven.

4.8.4 In de back-office worden de uitgevoerde handhavingstaken opgeslagen en kunnen deze worden ingezien en aangevuld, maar niet gewijzigd. Eventuele vervolgacties van een uitgevoerde handhavingstaak worden voor planningsdoeleinden doorgezet naar de meldkamersoftware.

4.8.5 Vanuit de back-office dienen afgeronde zaken te kunnen worden geëxporteerd naar de exportmodule van het CJIB, waarbij bijlagen middels Bulk Upload Berichten Service (BUBS) dienen te kunnen worden meegestuurd.

4.9 Eisen aan koppelvlakken/interfaces

4.9.1 Het realiseren, onderhouden en instandhouden van koppelvlakken tussen onderdelen van het aangeboden handhavingssysteem behoort tot de scope van de opdracht. De opdrachtnemer garandeert de correcte werking van het geheel.

4.9.2 De opdrachtnemer is verantwoordelijk voor de goede werking van het handhavingssysteem met de relevante applicaties of gegevensregistraties (al dan niet aanwezig binnen het softwarelandschap van Gemeente Eindhoven). Het betreft in ieder geval koppelingen met:

A. Landelijke basisregistraties:

- Basisregistratie Personen (BRP)
- Basisregistratie Adressen en Gebouwen (BAG)
- Handelsregister – Kamer van Koophandel
- Basisregistratie Voertuiggegevens (BRV) – RDW, inclusief voertuighoudergegevens
- Parkeer- en verblijfsrechtendatabase (NPR) - RDW
- Basisregistratie Kadaster (BRK)

B. Overige landelijke systemen/applicaties:

- Landelijk register gehandicaptenparkeerkaarten (GPK-register) - RDW
- Digitaal Opkoop Register (DOR)
- www.verlorenofgevonden.nl
- www.stopheling.nl
- Export CJIB – Bulk Upload Berichten Service (BUBS)

C. Gemeentelijke systemen/applicaties

- Meldingen-/zaaksysteem: BinnenBeter, Signalen
- Documentsysteem: eDocs
- GIS-systeem: GeoFundament
- VideoManagementSysteem: fabricaat nog niet bekend

4.9.3 Het niet beschikbaar zijn van een interface of een via een interface te bevragen applicatie of gegevensregistratie dient geen impact te hebben op het functioneren van de handhavingsapplicatie.

4.9.4 De handhavingsapplicatie geeft een melding aan de gebruiker(s) indien een interface of gegevensregistratie niet beschikbaar is.

4.9.5 Van toepassing zijnde gegevens die zijn opgevraagd uit landelijke gegevens dienen automatisch te worden vastgelegd bij een melding, zaak of sanctie. Overige gegevens dienen door de gebruikers gekopieerd te kunnen worden binnen een melding, zaak of sanctie.

4.9.6 De opdrachtgever beschikt over een gegevensmakelaar (Key2Distributie) voor de koppelingen met de landelijke basisregistraties (5.8.2. onder A). Deze wordt tevens beschikbaar gesteld voor de overige koppelingen.

4.9.7 De opdrachtgever beschikt over de benodigde certificaten voor toegang tot de gegevensregistraties in beheer bij RDW.

4.9.8 Bij gebruik van een subdomein of domein dat door de Opdrachtgever wordt beheerd dient Leverancier alleen certificaten te gebruiken welke zijn verstrekt door de Opdrachtgever.

4.9.9 De Leverancier is verantwoordelijk voor de aanschaf van certificaten, tenzij het gaat om de door Opdrachtgever beheerde domeinnamen (zie 4.9.8).

4.9.10 On-premise to SaaS, SaaS to On-premise en SaaS to SaaS koppelingen verlopen altijd via de door Opdrachtgever aangeboden Enterprise Service Bus (ESB), API Gateway of SFTP-oplossing. Indien het gaat om openbaar raad te plegen data, mag deze data rechtstreeks bij de aanbieder van de data worden geraadpleegd en/of opgehaald. Dit geldt eveneens indien het gaat om koppelingen tussen leveranciers onderling welke vallen onder de wettelijke grondslag die is gesteld door het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties of als data van de on-premise omgeving van de Opdrachtgever via een privé-verbinding gaat naar de Azure Tenant van de Opdrachtgever.

4.9.11 Enterprise Service Bus (ESB) verbindingen verlopen via een 2-way SSL handshake met een Signed Named SSL certificaat (geen self signed en/of wildcard certificaten)

4.9.12 Enterprise Service Bus (ESB), API Gateway of SFTP-koppelingen dienen via een statisch IP adres te worden opgezet.

4.9.13 SFTP-koppeling authenticatie is op basis van certificaten, dit mogen geen wildcard certificaten zijn. De SFTP-server (indien van toepassing) aan de kant van leverancier ondersteunt IP Whitelisting.

4.9.14 Machine to machine (G1) certificaten voor de Enterprise Service Bus (ESB) of API-koppeling, die worden gebruikt voor het uitwisselen van gegevens onderling tussen machines, die door de Opdrachtgever worden aangeschaft en gebruikt, krijgen per koppeling een certificaat en dit mag geen wilcard certificaat zijn.

4.10 Eisen m.b.t. beschikbaarheid

4.10.1 Het Handhavingssysteem dient een minimale beschikbaarheid van 99,5% van de kalendertijd te hebben, gemeten per kalendermaand.

4.10.2 De RTO (Recovery Time Objective) van het Handhavingssysteem is maximaal 24 uur. Dit maximum mag niet worden overschreden.

4.10.3 De RPO (Recovery Point Objective) van het Handhavingssysteem is maximaal 1 week. De Opdrachtnemer dient afdoende maatregelen te nemen opdat deze termijn niet wordt overschreden.

4.10.4 (Preventief) Onderhoud aan het Handhavingssysteem dient plaats te vinden tijdens vaste onderhoudswindows, buiten werkdagen (standaard tussen 08:00 tot 18:00). Indien (preventief) Onderhoud leidt tot (gedeeltelijke) onbeschikbaarheid van het Handhavingssysteem, betekent dit dat het Handhavingssysteem dan niet beschikbaar is.

5 Eisen aan de implementatie

5.1 Implementatie

5.1.1 Tot de implementatie van het handhavingssysteem behoort het plaatsen en aansluiten van alle hard- en software, inclusief het (in)programmeren van processen, tot en met het operationeel in bedrijf stellen en de bijbehorende nazorg. Onderdeel van de implementatie is verder het verzorgen van de benodigde interfaces en koppelingen.

5.1.2 De Opdrachtnemer is verantwoordelijk voor de volledige implementatie van het handhavingssysteem.

5.1.3 De Opdrachtnemer dient voor elke (deel)oplevering van het handhavingssysteem een opleveringsprotocol op te stellen.

5.1.4 Het door Opdrachtnemer, in samenspraak met de Opdrachtgever, definiëren, opstellen en inregelen van processen, vragenlijsten, (verplichte) invoervelden, standaardsjablonen en -documenten, maakt onderdeel uit van de implementatie.

5.1.5 Voorafgaand aan de eindoplevering van het complete handhavingssysteem, dient een Site Acceptance Test (SAT) te worden uitgevoerd. Tijdens deze SAT dient Opdrachtnemer aan te tonen dat het systeem voldoet aan de gestelde eisen ten aanzien van volledigheid (aangeboden functionaliteiten, processen), betrouwbaarheid (kwaliteit foto's, inrichting processen), nauwkeurigheid (locatiebepaling GPS, inrichting vragenlijsten), privacy en (data)safety. Bij deze SAT dient tevens de werking van de koppelingen te worden getest.

5.1.6 Het implementeren van de ontwikkeling, test en acceptatie (OTA) omgeving naar productie dient zonder overtypen te worden uitgevoerd.

5.2 Conversie

5.2.1 De migratie van bestaande gegevens uit HeApp en/of BlueBrick naar de aangeboden oplossing van de Opdrachtnemer maakt onderdeel uit van de implementatie.

5.2.2 De gemigreerde gegevens dienen opvraagbaar te zijn op basis van (onder andere: bonnummer, zaaknummer, verbalisantnummer, adres)

5.2.3 Opdrachtgever overweegt om binnen de looptijd van de te sluiten overeenkomst een DataWareHouse in te richten. Alle met het handhavingssysteem gegenereerde meldingen dienen te zijner tijd door Opdrachtnemer kosteloos voor opname in dat DataWareHouse te worden aangeboden. Tot dat moment dienen alle met het handhavingssysteem gegenereerde meldingen beschikbaar te zijn voor gebruik in de BI-omgeving van Opdrachtgever.

5.2.4 Een eenmalige dataoverdracht (bijv het aanleveren of ontvangen van een database) dient plaats te vinden op basis van SFTP. Indien de leverancier de SFTP-server is en opdrachtnemer de client dient de leverancier hiervoor IP-whitelisting te gebruiken en een tijdelijk SFTP-account ter beschikking te stellen met enkel het doel van de eenmalige dataoverdracht heeft.

5.3 Informatie en training

5.3.1 Onderdeel van de eindoplevering van het handhavingssysteem is het verstrekken (in de Nederlandse taal) door de Opdrachtnemer van de documentatie zoals verplicht gesteld in artikel 6 en 14 GIBIT en informatie:

- Handleidingen, gebruiks- en onderhoudsinstructie van (de onderdelen van) het handhavingssysteem, alsmede handleidingen voor het vervangen van certificaten/secret keys gebruikt door het Handhavingssysteem bij Azure application tbv SSO/SCIM
- Ontwerp en ontwerpbeschrijving van het handhavingssysteem
- Installatie- en SAT-documentatie
- Beschrijvingen van de koppelvlakken/koppelingen met te koppelen systemen in het kader van deze opdracht
- Beschrijving van de ingerichte processen en vragenlijsten ten behoeve van de brede handhaving.
- Overzicht van de parametrisering van de ICT Prestatie

- Overzicht van gebruikte http-requestmethoden (GET, POST)
- Informatie in de http-headers die voor het functioneren van belang zijn
- Vastlegging van de poorten en protocollen van en naar Handhavingssysteem, dit mag in de vorm van een overzicht of netwerktekening

De Opdrachtnemer houdt deze documentatie actueel en stelt actualiseringen per ommegaande beschikbaar aan Opdrachtgever.

5.3.2 De opdrachtnemer beschikt over en verstrekt (geanonimiseerd) aan opdrachtgever de Incident Response procedure welke minimaal voldoet aan de ISO 27001 template.

5.3.3 De Opdrachtnemer beschikt over en verstrekt aan opdrachtgever de Coordinated Vulnerability Disclosure procedure, dit mag via een publiek beschikbare security.txt file. Deze moet voldoen aan de richtlijnen van NCSC.

5.3.4 Opdrachtnemer verzorgt voorafgaand aan de oplevering van het handhavingssysteem initiële trainingen voor de verschillende gebruikers (autorisatiegroepen) én beheerders van de Opdrachtgever inzake de werking en het gebruik van het geleverde systeem. Opdrachtnemer doet bij zijn inschrijving een voorstel voor de invulling van deze trainingen inclusief een specificatie van eventueel benodigde specifieke basisvaardigheden en/of opleidingen die de betrokken medewerkers gevolgd dienen te hebben.

5.3.5 Opdrachtnemer biedt gedurende de looptijd van de te sluiten overeenkomst tenminste elk kwartaal de mogelijkheid voor nieuwe medewerkers van Opdrachtgever om een training/cursus voor (onderdelen van) het geleverde systeem te volgen.

5.4 Helpdesk – ondersteuning

5.4.1 De Opdrachtnemer dient gedurende de gehele looptijd van de overeenkomst een telefonische Helpdesk-functie te bieden waar Opdrachtgever terecht kunnen met vragen en problemen m.b.t. het handhavingssysteem.

5.4.2 Bij de telefonische helpdesk en overige ondersteuning (inclusief schriftelijke communicatie) dient Nederlands de voertaal te zijn.

5.4.3 De telefonische helpdesk dient ten minste gedurende de volgende uren beschikbaar te zijn:

- Maandag tot en met zaterdag, minimaal van 07.00 tot 22.00 uur
- Zon- en feestdagen, minimaal van 08.00 tot 22.00 uur

5.4.4 De reactietijd voor het opnemen van telefoontjes bedraagt maximaal 20 seconden

5.4.5 Het minimale service-window van de Opdrachtnemer voor het oplossen van aangemelde problemen is:

- Maandag tot en met zaterdag, van 07.00 tot 22.00 uur
- Zon- en feestdagen, van 08.00 tot 22.00 uur

5.4.6 Voor het indienen, monitoren en bewerken van calls en het reageren op ingediende calls dient de Opdrachtnemer 24/7 een digitale omgeving beschikbaar te stellen.

5.5 Einde overeenkomst

5.5.1 Na de einddatum van de overeenkomst blijft alle data die binnen het handhavingssysteem zijn gegenereerd in het bezit van en beschikbaar voor de Opdrachtgever. De Opdrachtnemer dient alle data aan Opdrachtgever te overhandigen in nader overeen te komen bewerkbare bestandsformaten (.xml of .csv, danwel een vergelijkbaar alternatief).

5.5.2 Na de einddatum van de overeenkomst behoudt de Opdrachtgever gedurende minimaal 3 maanden het gebruiksrecht op de back-office en de rapportagemodules van het handhavingssysteem.

5.5.3 De Opdrachtnemer dient een pro-actieve houding aan te nemen om te borgen dat de handhavingsprocessen na het beeindigen van de overeenkomst soepel zullen blijven verlopen. Hierbij valt (niet uitputtend) te denken aan: overdracht van de procesinrichting voor brede handhaving, gegeven van voertuigen waarvoor een Mulder-beschikking is aangemaakt, etc.

5.5.4 Na overdracht van alle data en bestanden na het einde van de overeenkomst dient Opdrachtnemer een ondertekende verklaring van vernietiging van alle gegevens te overhandigen aan Opdrachtgever. Opdrachtnemer mag geen data van Opdrachtgever in eigen opslag hebben c.q. verrijken en/of verkopen aan derden.

Ondertekening

Door ondertekening van dit document verklaart de inschrijver kennis te hebben genomen van alle eisen en informatie die zijn opgenomen in de aanbestedingsstukken, en hiermee akkoord te gaan. De inschrijver bevestigt dat de aangeboden oplossing aan alle door de aanbestedende dienst gestelde eisen voldoet. Let op: u dient een ondertekend exemplaar in te dienen bij uw inschrijving.

Naam inschrijver	
Naam rechtsgeldige ondertekenaar	
Datum	
Handtekening	