Programma van Eisen

Kassa-applicatie burgerzaken

20 mei 2026
Kenmerk 2025PBZ818
Versie 0.1

bronversie Format A-302 v20260115

Inhoud

1 Programma van eisen

In dit document zijn de eisen opgenomen die aan de gevraagde opdracht worden gesteld. Door het indienen van uw inschrijving voor deze opdracht verklaart u onvoorwaardelijk akkoord te gaan met ALLE eisen aan de opdracht.

1.1 Social return

Eis 1. U conformeert zich aan alle verplichtingen die voortvloeien uit het document ‘Handleiding Social Return’. Voor deze overeenkomst geldt een in te zetten percentage Social Return van 5%.

Eis 2. De gemeente bepaalt de in te zetten waarde aan Social Return op basis van de werkelijke waarde van de (nadere) opdracht. Dit is inclusief eventuele aanvullende opdrachten, zoals meerwerk, opties of wijzigingen van de opdracht.

Eis 3. U realiseert de Social return invulling tijdens de looptijd van de overeenkomst.

Eis 4. U bent zelf verantwoordelijk voor invulling van de social return opgave.

Eis 5. Na gunning van de opdracht plant u via socialreturn@utrecht.nl een gesprek met een adviseur social return. De gemeente adviseert de opdrachtnemer graag over mogelijkheden. Het toepassen van social return is maatwerk waarbij de gemeente rekening houdt met uw wensen: we zoeken naar een ‘win-win-winsituatie’.

1.2 Indexering

Eis 6. De prijzen zoals opgenomen in de overeenkomst worden jaarlijks geïndexeerd conform het bepaalde in artikel 5.7 van de GIBIT 2025 en de navolgende bepalingen.

Eis 7. Het te hanteren indexeringspercentage, afgerond op twee decimalen, komt als volgt tot stand: (Indexcijfer nieuw – Indexcijfer oud) / Indexcijfer oud × 100

Voor het vaststellen van het indexeringspercentage wordt gehanteerd:

- CBS Consumentenprijsindex (CPI) alle huishoudens, 2015=100 (reeks code: 7000001)
- Periode: Jaargemiddelde index

Voor de indexcijfers geldt:

- Indexcijfer oud: Gemiddelde jaarindex (van januari t/m december) van het jaar voorafgaand aan het contractjaar.
- Indexcijfer nieuw: Gemiddelde jaarindex (van januari t/m december) van het contractjaar.

Eis 8. De indexering vindt plaats per 1 april van elk kalenderjaar. De eerste indexering vindt plaats op 1 april 2028. De opdrachtnemer past de geïndexeerde prijzen toe zodra de definitieve jaarindex door het CBS is gepubliceerd. Indien de definitieve cijfers op het indexeringsmoment nog niet

beschikbaar zijn, wordt uitgegaan van de meest recente voorlopige cijfers. Na publicatie van de definitieve cijfers vindt zo nodig een correctie plaats met terugwerkende kracht.

Eis 9. Het indexeringspercentage bedraagt maximaal 10% per jaar. Indien de berekening een hoger percentage oplevert, wordt de indexering gemaximeerd tot 10%. Bij een negatieve indexering (deflatie) worden de prijzen naar evenredigheid verlaagd; er geldt geen bodempercentage.

1.3 Facturatie

Eis 10. Facturatie vindt plaats volgens artikel 18 van de Algemene inkoopvoorwaarden van de gemeente Utrecht 2018.

Eis 11. In afwijking op artikel 18.2 van de Algemene inkoopvoorwaarden van de gemeente Utrecht 2018 geldt dat voor deze opdracht uitsluitend e-facturering is toegestaan.

Eis 12. In januari van elk kalenderjaar ontvangt de gemeente één overzichtsfactuur die de volgende componenten bevat:

- Voorschotfacturatie voor het lopende jaar: De structurele abonnementskosten voor de periode van 1 januari tot en met 31 december van het lopende kalenderjaar worden jaarlijks vooraf gefactureerd.
- Definitieve afrekening voor het voorgaande jaar: Een gedetailleerde eindafrekening voor het gehele voorafgaande kalenderjaar, waarin: Het reeds betaalde voorschot voor dat jaar wordt verrekend. Eventuele tussentijdse wijzigingen in afgenomen diensten (zoals toegevoegde of beëindigde abonnementen) worden gespecificeerd en verrekend om tot de werkelijke kosten te komen. Het resulterende saldo (bijbetaling door de gemeente of creditering door de opdrachtnemer) wordt opgenomen.

1.4 Eisen voor overdracht bij eindiging overeenkomst

Eis 13. Als de overeenkomst afloopt doet u alles dat nodig is om te borgen dat een nieuwe opdrachtnemer, de gemeente en/of andere betrokken derden aansluitend en zonder onderbreking van de bedrijfsprocessen van de gemeente (onderdelen van) de opdracht kan overnemen en uitvoeren. Hiervoor brengt u geen additionele kosten in rekening.

Eis 14. U stelt 3 maanden voordat de overeenkomst afloopt een overdrachtsdossier op. Daarin is opgenomen welke werkzaamheden moeten worden verricht ter voorbereiding van de overdracht bij beëindiging van de overeenkomst.

Eis 15. U voert in ieder geval de onderstaande maatregelen uit:

- het overdragen van opgeslagen gegevens of opgestelde en aanvullende documenten die deel uitmaken van de opdracht;
- het overdragen van materialen/instrumenten/middelen van de gemeente die u tijdelijk in uw bezit heeft gehad bij de uitvoering van de overeenkomst;
- het vernietigen van gegevens waarvoor de gemeente verantwoordelijk is (tegen een bewijs van afgifte van de vernietiging);

- het technisch of functioneel ontvlechten of ontmantelen van de kassa applicatie.

Eis 16. U bent ervan op de hoogte dat de gemeente het overdrachtsdossier kosteloos geheel of gedeeltelijk kan overdragen aan de nieuwe contractpartner.

Eis 17. Alle transactiegegevens moeten worden overgedragen in een gangbaar, machineleesbaar formaat (minimaal CSV of XML).

Eis 18. De gemeente moet te allen tijde eigenaar blijven van alle transactiegegevens en configuraties.

1.5 Terugname bestaande pinautomaten en levering nieuwe pinautomaten

Eis 19. De opdrachtnemer neemt direct na start van de overeenkomst de 45 bestaande Verifone P400 Plus die eigendom zijn van de gemeente Utrecht, onvoorwaardelijk over. De restwaarde van deze apparatuur bedraagt € 20.000 en wordt door opdrachtnemer in mindering gebracht op de totaal geoffreerde prijs. De teruggenomen pinautomaten worden door opdrachtnemer niet opnieuw ingezet binnen de uitvoering van deze opdracht.

Eis 20. De opdrachtnemer levert en installeert uitsluitend nieuwe pinautomaten die voldoen aan alle in dit PvE gestelde eisen. Het herplaatsen, refurbishen of opnieuw in gebruik nemen van de teruggenomen gemeentelijke pinautomaten is niet toegestaan. De opdrachtnemer draagt zorg voor volledige afvoer, verwerking of herbestemming van deze apparatuur conform geldende wet- en regelgeving.

Eis 21. Naleving van deze eis is een voorwaarde voor geldige uitvoering van de opdracht.

1.6 Algemene functionaliteit

Eis 22. De kassa-applicatie moet zowel elektronische betalingen (pin) als contante betalingen kunnen verwerken.

Eis 23. De kassa-applicatie moet automatisch betaalbewijzen kunnen genereren en printen na elke transactie.

Eis 24. De kassa-applicatie moet barcodes kunnen genereren voor de afhandeling van contante betalingen.

Eis 25. De kassa-applicatie moet realtime communicatie mogelijk maken tussen de kassasoftware, pinautomaten en bonprinters.

Eis 26. De kassa-applicatie moet alle transacties volledig en onwijzigbaar loggen ten behoeve van controle en verantwoording.

Eis 27. De kassa-applicatie moet historische transactiegegevens kunnen opslaan en raadpleegbaar maken voor maximaal 7 jaar.

Eis 28. De kassa-applicatie moet een koppeling bieden met de taakapplicatie van Burgerzaken, waarbij betalingsverzoeken kunnen worden ontvangen en diverse statussen betaling kunnen worden getoond worden in de beheeromgeving inclusief foutmeldingen.

Eis 29. Het systeem moet met twee contant-betaalautomaten van de gemeente kunnen koppelen.

Eis 30. Indien er een aanbesteding komt voor een nieuwe contant-betaalautomaat werkt de leverancier mee op technisch gebied, o.a. door het opstellen van technische eisen voor het koppelvlak en het inzichtelijk maken van bijkomende kosten voorafgaand aan publicatie.

Eis 31. De koppeling met de taakapplicatie moet het volgende proces ondersteunen:

- Ontvangen van betalingsverzoeken vanuit de taakapplicatie
- Klaarzetten van de betaling op de pin- of contant-betaalautomaat
- Verwerken van de transactie
- Printen van een betaalbewijs
- Tonen van betalingsstatus in de beheeromgeving
- Indien nodig foutmelding met herleidbare foutomschrijving voor beheerders

Eis 32. De opdrachtnemer moet een werkende koppeling kunnen realiseren met de huidige contant-betaalautomaten van de gemeente. Daarnaast moet de opdrachtnemer kosteloos meewerken aan het tot stand brengen van koppelingen met toekomstige contant-betaalsystemen

1.7 Rapportage en administratie

Eis 33. Het systeem moet gedetailleerde transactieoverzichten kunnen genereren, uitgesplitst naar datum, locatie, serienummer pinautomaat, medewerker en betaalwijze.

Eis 34. Het systeem moet financiële rapportages kunnen genereren voor dagafsluitingen, weekoverzichten en maandoverzichten.

Eis 35. Het systeem moet exportfunctionaliteit bieden naar gangbare formaten (minimaal Excel, CSV en PDF).

Eis 36. Het systeem zou dashboards moeten bieden met realtime inzicht in transacties en systeemstatus en foutmeldingen.

1.8 Hardware

Algemeen

Eis 37. Alle benodigde bekabeling, adapters en aansluitingen voor het koppelen met de hardware moeten worden geleverd.

Eis 38. De hardware moet compatibel zijn met de te leveren kassasoftware.

Eis 39. De levering en vervanging van bonprinters valt buiten de scope van deze opdracht. De aangeboden kassasoftware moet volledig kunnen communiceren met en functioneren in combinatie met de bestaande bonprinters.

Eis 40. De opdrachtnemer moet de technische specificaties van alle te leveren hardware in de offerte opnemen. Deze technische specificaties moeten als afzonderlijk document worden toegevoegd bij het onderdeel Prijs.

Eis 41. De hardware moet een minimale levensduur hebben van 10 jaar bij normaal gebruik.

Pinautomaten

Eis 42. Er moeten 45 pinautomaten worden geleverd en geïnstalleerd.

Eis 43. De pinautomaten moeten minimaal de volgende betaalmethoden ondersteunen: Maestro, V-PAY, Mastercard, Visa en contactloos betalen (via mobiele apparaat of pinpas).

Eis 44. De pinautomaten moeten geschikt zijn voor zowel contact- als contactloze betalingen.

Eis 45. De pinautomaten moeten een gebruiksvriendelijk kleurendisplay hebben.

Eis 46. De pinautomaten kunnen worden voorzien van het gemeentelogo op het display.

Eis 47. De pinautomaten moeten betrouwbaar functioneren in een kantooromgeving met normale temperatuur en luchtvochtigheid.

1.9 Software

Architectuur

Eis 48. De kassasoftware moet worden geleverd als Software-as-a-Service (SaaS).

Eis 49. De SaaS-oplossing moet worden gehost binnen de Europese Economische Ruimte (EER).

Eis 50. De software moet een webgebaseerde interface bieden die toegankelijk is via moderne webbrowsers (minimaal Chrome, Edge, Firefox in hun huidige en voorgaande versie).

Eis 51. De software moet responsief en bruikbaar zijn op verschillende schermformaten.

Eis 52. De software moet multi-tenant architectuur ondersteunen met volledige scheiding van gegevens tussen verschillende gebruikers/afdelingen.

Prestaties

Eis 53. Het systeem moet een beschikbaarheid van minimaal 99,5% gedurende de contractperiode garanderen (gemeten per kwartaal, exclusief gepland onderhoud).

Eis 54. Gepland onderhoud mag maximaal 1x per maand plaatsvinden en moet minimaal 5 werkdagen van tevoren worden aangekondigd.

Eis 55. Gepland onderhoud mag uitsluitend buiten kantooruren plaatsvinden: Op werkdagen na 18:00 (dinsdag en donderdag na 20:00) en voor 07:00 uur.

Eis 56. De responstijd van de kassasoftware moet gemiddeld minder dan 2 seconden bedragen voor standaardtransacties.

Eis 57. Het systeem moet schaalbaar zijn en minimaal 100 gelijktijdige transacties kunnen verwerken zonder prestatievermindering.

1.10 Beveiliging

Eis 58. Alle communicatie tussen componenten moet versleuteld zijn (minimaal TLS 1.2 of hoger).

Eis 59. Het systeem moet tweefactorauthenticatie ondersteunen voor beheerders.

Eis 60. Het systeem moet voldoen aan de eisen van de Algemene Verordening Gegevensbescherming (AVG/GDPR).

Eis 61. De opdrachtnemer moet kunnen aantonen dat regelmatig beveiligingsaudits worden uitgevoerd en moet de resultaten daarvan op verzoek kunnen overleggen.

Eis 62. Het systeem moet automatische back-ups maken met een frequentie van minimaal dagelijks.

Eis 63. Back-ups moeten worden opgeslagen op een geografisch gescheiden locatie binnen de EER.

Eis 64. De Recovery Time Objective (RTO) mag maximaal 4 uur bedragen.

Eis 65. De Recovery Point Objective (RPO) mag maximaal 24 uur bedragen.

1.11 Certificeringen en compliance

Eis 66. De opdrachtnemer moet gedurende de looptijd van de overeenkomst beschikken over een ISO 27001 certificering voor informatiebeveiliging en het certificaat op verzoek van opdrachtgever binnen 2 weken na het verzoek kunnen indienen bij opdrachtgever.

Eis 67. De opdrachtnemer moet gedurende de looptijd van de overeenkomst beschikken over een ISO 9001 certificering voor kwaliteitsmanagement en het certificaat op verzoek van opdrachtgever binnen 2 weken na het verzoek kunnen indienen bij opdrachtgever.

Eis 68. De opdrachtnemer moet op verzoek kunnen aantonen dat de dienstverlening volledig AVG-compliant is en moet een verwerkersovereenkomst afsluiten met de gemeente Utrecht.

1.12 Implementatie

Algemene eisen implementatie

Eis 69. De opdrachtnemer moet een ervaren projectleider aanstellen die als vast aanspreekpunt fungeert voor de gemeente.

Eis 70. De opdrachtnemer werkt het bij inschrijving ingediende implementatieplan binnen 2 weken na gunning uit tot een gedetailleerd en definitief implementatieplan. Dit plan vormt een uitwerking en concretisering van het bij inschrijving ingediende plan en mag daarvan inhoudelijk niet wezenlijk afwijken. Het definitieve implementatieplan wordt in overleg met de gemeente vastgesteld..

Eis 71. Het Het definitieve implementatieplan bevat minimaal de volgende onderwerpen, overeenkomstig de structuur van het bij inschrijving ingediende implementatieplan:

- Een gefaseerde projectaanpak met concrete mijlpalen, gericht op het realiseren van de volledige implementatie binnen de fatale termijn van 3 maanden na start van de overeenkomst;
- De wijze waarop de continuïteit van de dienstverlening aan burgers wordt gewaarborgd gedurende de gehele implementatieperiode;
- De aanpak voor de installatie van hardware, inrichting van de SaaS-applicatie, realisatie van koppelingen en datamigratie, inclusief de test- en acceptatiestrategie;
- Het opleidingsprogramma voor alle gebruikersgroepen, afgestemd op de verschillende rollen (baliemedewerkers, functioneel beheerders en technisch beheerders);
- Een overzicht van de belangrijkste implementatierisico's met bijbehorende beheersmaatregelen;
- Een beschrijving van het noodscenario voor het geval de implementatie niet binnen de gestelde termijn kan worden afgerond of de continuïteit van de dienstverlening in gevaar komt.

Eis 72. Er moeten minimaal tweewekelijks voortgangsgesprekken plaatsvinden tussen de projectleider en de gemeente.

Implementatie en configuratie

Eis 73. De volledige implementatie moet binnen 3 maanden na start van de overeenkomst zijn afgerond. Dit geldt als een fatale termijn.

Eis 74. De implementatie moet plaatsvinden buiten kantooruren of in overleg met de gemeente om verstoring van de dienstverlening te minimaliseren.

Eis 75. Alle hardware moet op locatie worden geïnstalleerd, geconfigureerd en getest.

Eis 76. Relevante gegevens van de afgelopen zeven jaar uit het huidige systeem moeten worden gemigreerd naar het nieuwe systeem.

Testen

Eis 77. De opdrachtnemer moet functionele en technische tests uitvoeren op alle componenten van het systeem bij elke nieuwe release en/of update.

Eis 78. Er moeten integratietests worden uitgevoerd met de taakapplicatie van Burgerzaken bij elke nieuwe release en/of update.

Eis 79. De opdrachtnemer moet de gemeente begeleiden bij het uitvoeren van acceptatietests.

Eis 80. Er moet door opdrachtnemer een testrapport worden opgeleverd met de resultaten van alle uitgevoerde tests.

Eis 81. Geconstateerde gebreken tijdens testen moeten worden hersteld voordat formele oplevering plaatsvindt.

Oplevering

Eis 82. Formele oplevering vindt plaats na door de gemeente vastgestelde succesvolle afronding van de acceptatietests.

Eis 83. Bij oplevering moeten alle daartoe aangewezen medewerkers van de gemeente de heironder beschreven opleidingen hebben ontvangen.

1.13 Opleiding

Algemene eisen opleiding

Eis 84. Bij significante updates of wijzigingen aan het systeem moeten aanvullende opleidingen worden verzorgd voor alle betreffende en daartoe aangewezen medewerkers van de gemeente.

Eis 85. Er moeten online trainingsmaterialen (video's, e-learning) beschikbaar worden gesteld uiterlijk 5 werkdagen na updates of wijzigingen.

Eis 86. Alle opleidingsmaterialen en documentatie moeten worden opgeleverd in digitale vorm.

Opleiding (balie)medewerkers

Eis 87. Er moet een praktijkgerichte opleiding worden verzorgd voor baliemedewerkers over het dagelijks gebruik van de kassasoftware en hardware.

Eis 88. De opleiding moet minimaal de volgende onderwerpen behandelen: starten en afsluiten van een werkdag, verwerken van pintransacties, verwerken van contante betalingen, printen van betaalbewijzen, omgaan met veelvoorkomende foutmeldingen.

Eis 89. De opleiding moet in het Nederlands worden gegeven.

Eis 90. Er moeten voldoende trainingsmomenten worden ingepland zodat alle baliemedewerkers (ca. 60 personen) kunnen deelnemen.

Eis 91. Er moet een gebruikershandleiding worden geleverd in het Nederlands.

Opleiding functioneel beheerders

Eis 92. Er moet een opleiding worden verzorgd voor functioneel beheerders (ca. 5 personen) over het beheren van de software.

Eis 93. De opleiding moet minimaal de volgende onderwerpen behandelen: gebruikersbeheer, genereren van rapportages, configuratie-instellingen, oplossen van eenvoudige storingen, eerste lijn support.

Eis 94. Er moet een beheerdershandleiding worden geleverd in het Nederlands.

Opleiding technisch beheerders

Eis 95. Er moet technische documentatie en instructie worden verzorgd voor technisch beheerders (ca. 3 personen).

Eis 96. De technische documentatie moet minimaal bevatten: systeemarchitectuur, technische configuratie, API-documentatie, troubleshooting procedures, contactgegevens voor support.

1.14 Onderhoud en support

Onderhoud software

Eis 97. De opdrachtnemer is verantwoordelijk voor het volledige onderhoud van de SaaS-oplossing gedurende de contractperiode.

Eis 98. Correctief onderhoud (oplossen van storingen en bugs) moet worden uitgevoerd conform de overeengekomen service levels.

Eis 99. Preventief onderhoud (monitoring, proactieve maatregelen) moet regelmatig worden uitgevoerd.

Eis 100. Adaptief onderhoud (updates, patches, aanpassingen aan wet- en regelgeving) moet tijdig worden doorgevoerd.

Eis 101. Beveiligingsupdates moeten binnen 48 uur na beschikbaarheid worden geïnstalleerd bij kritieke kwetsbaarheden.

Eis 102. Functionele updates moeten minimaal 2 weken van tevoren worden aangekondigd.

Onderhoud hardware

Eis 103. De opdrachtnemer is verantwoordelijk voor het volledige onderhoud van alle geleverde hardware gedurende de contractperiode.

Eis 104. Defecte hardware moet worden gerepareerd of vervangen conform de overeengekomen service levels.

Eis 105. Vervangende hardware moet van gelijkwaardige of betere kwaliteit zijn.

Servicedesk en support

Eis 106. De opdrachtnemer moet een servicedesk inrichten die telefonisch en per e-mail bereikbaar is.

Eis 107. De servicedesk moet minimaal bereikbaar zijn tijdens kantooruren (maandag t/m vrijdag, 08:00-17:00 uur, op dinsdag en donderdag tot 20:00 exclusief erkende feestdagen).

Eis 108. Voor kritieke storingen (Priority 1) moet bereikbaarheid via een storingsnummer worden gegarandeerd tijdens openingstijden van de balies (09:00-17:00 en tot 20:00 op dinsdag/donderdag).

Eis 109. De servicedesk moet in het Nederlands communiceren.

Eis 110. Meldingen moeten worden geregistreerd in een ticketsysteem met unieke referentienummers.

Eis 111. De gemeente moet via een webportaal de status van meldingen kunnen inzien

Service levels

Eis 112. De opdrachtnemer moet in de offerte duidelijke service levels specificeren voor responstijd en oplostijd, uitgesplitst naar de volgende prioriteiten:

- Priority 1 (Kritiek): Systeem volledig buiten gebruik, betalingen kunnen niet worden verwerkt
- Priority 2 (Hoog): Ernstige functionaliteitsbeperking, betalingen kunnen beperkt worden verwerkt
- Priority 3 (Gemiddeld): Functionaliteitsbeperking, workaround beschikbaar
- Priority 4 (Laag): Kleine storing of vraag, geen directe impact op dienstverlening

Eis 113. Voor Priority 1 storingen moet de responstijd maximaal 1 uur bedragen.

Eis 114. Voor Priority 1 storingen moet een tijdelijke oplossing (workaround) binnen 4 uur beschikbaar zijn.

Eis 115. Voor Priority 1 storingen moet een definitieve oplossing binnen 8 uur worden gerealiseerd.

Eis 116. De opdrachtnemer moet maandelijks rapporteren over de naleving van de servicelevels.

1.15 Flexibiliteit en schaalbaarheid

Eis 117. Het moet mogelijk zijn om gedurende de looptijd koppelingen met hardware (zoals extra pinautomaten/contant betaalautomaten) toe te voegen of te verwijderen.

Eis 118. Het moet mogelijk zijn om gedurende de looptijd koppelingen met software (zoals andere gemeentelijke systemen) toe te voegen of te verwijderen zoals omschreven in de leidraad.

Eis 119. Toevoegen of verwijderen van koppelingen mag geen negatieve impact hebben op de stabiliteit en prestaties van het bestaande systeem.

Eis 120. Het systeem moet schaalbaar zijn om een toename van het aantal balies tot 75 te kunnen ondersteunen zonder ingrijpende aanpassingen.

Eis 121. Het systeem moet een toename van het transactievolume met minimaal 200% kunnen verwerken zonder prestatievermindering.

Eis 122. Het systeem zou geschikt moeten zijn voor uitbreiding naar andere afdelingen of locaties binnen de IT-netwerkstructuur van de gemeente Utrecht.

1.16 Wijziging financiële afhandeling

Eis 123. Abonnementskosten voor koppelingen zijn uitsluitend verschuldigd voor de periode dat deze daadwerkelijk aangesloten en in gebruik zijn.

Eis 124. Alle structurele kosten worden jaarlijks gefactureerd in 1 overzichtsfactuur, waarbij afwijkende abonnenmentsperiodes (dus niet per 01-01) worden gecorrigeerd op de eerstvolgende

jaarrekening en dan vervolgens van 01-01 tot 31-12 het daaropvolgende jaar worden gefactureerd.

Eis 125. Eventuele incidentele kosten kunnen apart worden gefactureerd.

1.17 Non functionele eisen

Algemene voorwaarden

Eis 126. De oplossing ondersteunt de van toepassing zijnde standaarden uit de lijsten "pas toe of leg uit" en "aanbevolen standaarden" zoals gepubliceerd door het Forum standaardisatie

Eis 127. De gemeente conformeert zich aan de richtlijnen Baseline Informatiebeveiliging Overheid (BIO). De oplossing fungeert binnen de kaders van deze richtlijnen

Eis 128. Bij het raadplegen, verwerken van persoonsgegevens conformeert de oplossing zich aan de geldende AVG-regels

Eis 129. Alle opslag van data binnen de oplossing vindt plaats op locaties welke binnen de Europese economische ruimte bevinden (EER)

Eis 130. De oplossing conformeert zich aan het domeinnamenbeleid van de Gemeente Utrecht. Zie Bijlage 10.

Eis 131. De oplossing ondersteunt de uitwisseling van gegevens tussen applicaties middels API (web) services of een andere gestandaardiseerde methodiek

Authenticatie en autorisatie

Eis 132. De oplossing voorziet in goede scheiding van toegang en rollen d.m.v. Role Based Access Control (RBAC) voor beheerders en gebruikers.

Eis 133. De beheerinterface moet de mogelijkheid bieden om Active Directory (Entra ID) gebruikersgroepen rechten te geven om de volgende elementen wel of niet te zien:

a. (Group) layers;

b. Attributen;

c. Data uit gerelateerde tabellen;

d. Zoekfuncties;

e. Rapporten (indien aangeboden in de oplossing);

f. Workflows (indien aangeboden in de oplossing).

Eis 134. Toegang tot de oplossing is dwingend geregeld voor gebruikers van de gemeente Utrecht op basis van Single-Sign-On, (SSO) zie Bijlage 09: Authenticatie

Eis 135. De oplossing ondersteunt de SSO standaarden vermeldt in Bijlage 09: Authenticatie

Eis 136. De oplossing ondersteunt indien nodig MFA.

Eis 137. Gegevens die via het internet worden uitgewisseld dienen op een bij de data passende manier te worden beveiligd. Privacygevoelige gegevens moeten versleuteld worden.

Eis 138. Bij berichtuitwisseling met externe voorzieningen wordt authenticatie d.m.v. 2-zijdig TLS1.2 of hoger toegepast.

Releasemanagement

Eis 139. De opdrachtnemer levert op aanvraag inzicht in de te verwachten ontwikkelingen in de oplossing.

Eis 140. De opdrachtnemer biedt de mogelijkheid om periodiek (minimaal 1 keer per jaar) ontwikkelverzoeken van opdrachtgever te bespreken voor de roadmap van de applicatie(s) van de opdrachtnemer. Er is bijvoorbeeld een mogelijkheid voor de gemeente Utrecht aanvullende functionele wensen aan te leveren.

Eis 141. De opdrachtnemer levert een test/acceptatie en een productieomgeving.

Eis 142. De opdrachtnemer heeft de ontwikkel-, test en acceptatie omgevingen (separaat of geïntegreerd tot één omgeving) gescheiden van productieomgevingen en maakt geen gebruik van persoonlijke gegevens uit de productieomgeving.

Eis 143. Nieuwe functionaliteit kan worden getest in een OTAP proces.

Gegevensbeschermingseisen

Eis 144. Opdrachtnemer moet de keten van opdrachtnemers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeopdrachtnemers op aanvraag van Opdrachtnemer.

Eis 145. De applicatie volgt de tijdsperiodes voor herstel van de dienstverlening (RTO) behorende bij BBN Niveau 2 (BBN2). De afgesproken dienstverlening moet binnen 48 uur worden gecontinueerd.

Eis 146. De applicatie volgt de geborgde maximale dataverlies (RPO) behorende bij BBN Niveau 2. Het verlies van gegevens mag maximaal 24 uur bedragen.

Eis 147. Er wordt een periodieke versleutelde back-up gemaakt van de data binnen de applicatie en de herstelprocedure wordt minimaal 1 keer per jaar getest. De Opdrachtnemer garandeert een adequate backup- en restorevoorziening van de Oplossing voor de acceptatieomgeving waarbij ten minste 7 dagen teruggegaan kan worden.

Eis 148. Er is een proces voor het zo snel mogelijk doorvoeren van beveiligingsupdates binnen de applicatie en de omgeving die hiervoor benodigd is. De Opdrachtgever wil in staat gesteld worden om bij releases- en updates op voorhand afdoende te kunnen testen. Het is voor de Opdrachtgever daarom van meerwaarde dat voldoende voorbereidingsmogelijkheid bestaat en een (onverwachts grote) belasting voor de beheersorganisatie wordt voorkomen.

Eis 149. Er wordt gebruik gemaakt van monitoring voor het signaleren van uitval en andere incidenten.

Eis 150. De opdrachtnemer logt gelukte aanmeldpogingen, mislukte aanmeldpogingen en het gebruik van systeemhulpmiddelen (auditing), waarbij de logbestanden beschermd en periodiek (met

elkaar af te stemmen) beoordeeld worden. De Oplossing beschikt over een niet-muteerbare audit-trail met daarin minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis. Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.

Eis 151. Logging wordt minimaal een half jaar bewaard. In geval van een (vermoed) informatiebeveiligingsincident wordt de logging minimaal 3 jaar bewaard voor onderzoek en op verzoek ter beschikking gesteld aan gemeente Utrecht.

Eis 152. Log-bestanden van gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen worden geregistreerd bij het gebruik van nietopenbare/ gevoelige informatie. Er wordt gelogd voor op persoons- en systeemniveau. Het moet inzichtelijk gemaakt kunnen worden hoevaak er sprake is van incidenten. Bij (grote) incidenten dient de opdrachtgever direct te worden geinformeerd <24 uur. Op verzoek kan de opdrachtgever, opdrachtnemer verzoeken om logging/rapportages te overleggen.

Eis 153. De oplossing kan het door de organisatie vastgestelde opschoningsproces mogelijk maken, faciliteren en ervoor zorgen dat informatieobjecten, bijbehorende metagegevens en logbestanden administratief verwijderd of ontoegankelijk gemaakt worden.

Eis 154. Beheerders hebben enkel toegang tot de functionaliteiten waarvoor zij specifiek bevoegd zijn.

Eis 155. Data wordt veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld.

Eis 156. De opdrachtnemer houdt te allen tijde systemen en databases (logisch) gescheiden van andere klanten van de inschrijver.

Eis 157. Er wordt gebruik gemaakt van versleuteling bij de uitwisseling van gegevens over interne als externe netwerken.

Eis 158. Gebruikers hebben enkel toegang tot de data waarvoor zij specifiek bevoegd zijn (conform autorisatiematrix).

Eis 159. Data wordt niet langer bewaard dan toegestaan volgens geldende bewaartermijnen.

Eis 160. Persoonsgegevens worden waar mogelijk geanonimiseerd, dan wel gepseudonimiseerd opgeslagen en verwerkt, zodat informatie niet tot een persoon herleidbaar is.

Eis 161. Persoonsgegevens moeten worden worden verwijderd zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld (bijvoordeeld door beheerders).

Eis 162. Informatiebeveiligingsincidenten en datalekken behoren zo snel mogelijk te worden gerapporteerd aan gemeente, uiterlijk binnen 24 uur.

Eis 163. Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.

Eis 164. Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen. Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.

1.18 Informatiebeheer

Algemeen

Eis 165. De gemeente Utrecht is en blijft in alle gevallen eigenaar van de gegevens die verwerkt worden in de applicatie conform artikel 20 van de GIBIT 2025.

Eis 166. "De opdrachtnemer geeft de opdrachtgever gedurende de looptijd van de overeenkomst, tijdens normale kantoortijden en/of anders overeengekomen beschikbaarheidstijden, toegang tot de verwerkte gegevens, logbestanden, autorisaties en specifieke instellingen van de applicatie conform artikel 21 van de GIBIT 2025.

Dit kan gebeuren door:

- Regulier gebruik van de applicatie
- Aanleveren van opgeslagen gegevens in een geschikt duurzaam formaat, zoals CSV formaat.
- Ter beschikking stellen van koppelingen en documentatie.
- Verstrekken van gedetailleerde datamodel-beschrijvingen.

Eis 167. Opdrachtnemer informeert en waarschuwt Opdrachtgever als beveiligingsmaatregelen worden omzeild. Opdrachtgever is zelf verantwoordelijk voor het gebruik van de verkregen gegevens en vrijwaart Opdrachtnemer tegen claims van derden uit dit gebruik.

Eis 168. Bij beëindiging van de overeenkomst, stelt de opdrachtnemer de gegevens, die in de applicatie werden gebruikt en/of beheerd, weer beschikbaar aan de gemeente Utrecht en werkt opdrachtnemer mee aan de migratie en, indien van toepassing, conversie van die gegevens. De opdrachtnemer draagt vervolgens verder zorg voor de vernietiging van deze gegevens (in test-, acceptatie en productieomgeving en op de back-ups) zodra de gegevens zijn gemigreerd en opdrachtgever daar akkoord op geeft.

Eis 169. Voor al deze stappen wordt een exit-plan opgesteld, op het moment dat opdrachtgever hier om vraagt.

Eis 170. De opdrachtnemer verklaart om op het moment van beëindigen van de overeenkomst of bij buiten bedrijfstellen van de applicatie, om welke reden dan ook, op verzoek van de opdrachtgever het volgende te doen:

- Een nieuwe oplossing leveren of de bestaande beperkt voortzetten, zodat de opdrachtgever de opgeslagen gegevens kan blijven raadplegen.
- Beperkt onderhoud blijven bieden voor de bestaande applicatie bij tijdelijke verlenging die ten minste mogelijk maakt om, met soortgelijke prestatie als gedurende contractlooptijd, opgeslagen gegevens te blijven raadplegen.

Eis 171. Voor de duur, kosten en voorwaarden van deze ICT-dienst geldt het volgende:

- De duur is minimaal voldoende zodat de opdrachtgever aan wettelijke administratieverplichtingen kan voldoen.
- De kosten staan in redelijke verhouding tot de oorspronkelijke kosten van de gehele oplossing, rekening houdende met verminderde functionaliteit. Noodzakelijke verlengingen van derdenprogrammatuur kunnen volledig worden doorberekend.
- De voorwaarden zijn over het algemeen gelijk aan die van de oorspronkelijke overeenkomst, met uitzondering van het eerder genoemde.

Eis 172. Bij nieuwe releases van de applicatie wordt opdrachtgever daar tijdig van geïnformeerd en moeten bestaande gegevens onder beheer van de applicatie toegankelijk blijven zonder verandering van inhoud en structuur van gegevens en verlies van functionaliteit van de applicatie.

Toegangsbeheer en beveiliging

Eis 173. De applicatie kan beveiligings- en toegangsbeperkingsmaatregelen toepassen om de inhoud van informatieobjecten en bijbehorende metagegevens en logbestanden te beschermen tegen toegang, wijziging, export, vernietiging of andere mogelijke bewerkingen door onbevoegden.

Eis 174. De applicatie kan beveiligde) overzichten creëren en onderhouden die alle handelingen met betrekking tot informatieobjecten en bijbehorende metagegevens, zoals toegang, wijziging, export, vernietiging of andere mogelijke bewerkingen door (on)bevoegden vastleggen.

Eis 175. De applicatie kan op verschillende aggregatieniveaus van informatieobjecten toegangsrechten toekennen.

Eis 176. De applicatie kan routinematig elke gebruiker authenticeren en autoriseren alvorens toegang te verlenen, in het geval toegang tot informatieobjecten en bijbehorende metagegevens een specifiek rol/permissies vereist.

Eis 177. De applicatie kan op alle informatieobjecten [naar behoefte organisatie/proces] toegangsrechten toekennen.

Inwinning

Eis 178. De applicatie kan brongegevens ophalen uit de van toepassing zijnde bronregistraties.

Opname

Eis 179. De applicatie kan, voor de te ondersteunen processen relevante, informatieobjecten met bijbehorende metagegevens opnemen vanuit externe bronnen.

Eis 180. De applicatie kan informatieobjecten met bijbehorende metagegevens zowel in bulk als individueel opnemen, waarbij de integriteit van de inhoud en structuur van informatieobjecten kan worden gegarandeerd.

Eis 181. De applicatie kan op het moment van opname of inwinning de integriteit van informatieobjecten verifiëren aan de hand van aanvullende criteria (zoals elektronische handtekeningen of checksums).

Eis 182. De applicatie kan informatieobjecten vastleggen in open standaarden en/of in hun oorspronkelijke formats.

Creatie

Eis 183. De applicatie kan, voor de te ondersteunen processen relevante, informatieobjecten creëren en opslaan binnen de applicatie.

Metagegevens beheer

Eis 184. De applicatie kan het opnemen, aanmaken, opslaan en bewerken van metagegevens voor informatieobjecten te allen tijde mogelijk maken, voor daartoe geautoriseerde gebruikers, gedurende de levenscyclus van die informatieobjecten

Eis 185. De applicatie kan open formaten (of combinaties daarvan) voor elementen/eigenschappen van metagegevens (zoals bijvoorbeeld .XML) ondersteunen.

Eis 186. De applicatie kan een bewaartermijn en passende archiefacties (b.v. vernietigen en/of overbrengen), proces- en archiefactietermijnen toewijzen aan informatieobject(en) gedurende de levenscyclus, in overeenstemming met het Utrechts metadatamodel, het relevante ordeningsplan van het organisatieonderdeel en de vigerende selectielijsten.

Eis 187. De applicatie kan een bewaartermijn en passende archiefacties (bijvoorbeeld vernietigen of overbrengen) en archiefactietermijnen toewijzen op meerdere aggregatieniveaus, waarbij:

Eis 188. 1. Metagegevens kunnen worden overgeërfd van een hoger naar een lager aggregatieniveau (waar dit wenselijk is).

Eis 189. 2. Metagegevens op een lager aggregatieniveau kunnen afwijken van bewaartermijnen op een hoger aggregatieniveau (waar dit wenselijk is)."

Eis 190. De applicatie kan bewaartermijnen en archiefacties (b.v. vernietigen of overbrengen), proces- en archiefactietermijnen in bulk toewijzen en/of aanpassen.

Eis 191. De applicatie kan de bijbehorende metagegevens in de ICT-oplossing wijzigen wanneer bewaartermijnen, archiefacties, proces- en archiefactietermijnen in de selectielijst worden aangepast. Dit kan zowel met terugwerkende kracht als vanaf een bepaalde datum worden ingesteld. Bovendien kan ook de reden voor de aanpassing worden vastgelegd.

Eis 192. Wanneer wordt afgeweken van vastgestelde bewaartermijnen, kan de applicatie een toelichting opnemen om de reden van deze afwijking te verduidelijken.

Opslag

Eis 193. De applicatie kan informatieobjecten, en bijbehorende metagegevens, zodanig opslaan en beheren, dat ze door de tijd, gedurende hun levenscyclus, toegankelijk en opvraagbaar blijven voor bevoegde gebruikers.

Validatie

Eis 194. De applicatie kan, op het niveau van individuele informatieobjecten, hashes (b.v. checksum) genereren of andere mechanismen implementeren om integriteitscontrole op informatieobjecten mogelijk te maken

Eis 195. De applicatie kan Informatieobjecten controleren op virussen, wormen en andere vormen van schadelijke

Eis 196. De applicatie kan, bij het beschikbaar stellen van informatieobjecten en/of metagegevens, een mogelijkheid bieden waarmee gebruikers terugmeldingen kunnen doen over de weergave en de kwaliteit daarvan.

Bevriezen

Eis 197. De applicatie kan de inhoud van informatieobjecten en bijbehorende metagegevens onveranderlijk maken en beschermen tegen onbevoegde wijziging.

Zoeken

Eis 198. De applicatie kan gebruikers van functionaliteiten voorzien voor het zoeken en opvragen van informatieobjecten, en/of (meta)gegevens, waarbij er gezocht kan worden op basis van alle mogelijke combinaties van relevante (meta)gegevens en er binnen zoekresultaten gefilterd kan worden op basis van specifieke (meta)gegevens of combinaties daarvan.

Vernietiging

Eis 199. De applicatie kan het door de organisatie vastgestelde vernietigingsproces mogelijk maken (wanneer bewaartermijnen zijn verstreken), faciliteren en ervoor zorgen dat het vernietigen van (verwijzingen naar) informatieobjecten, bijbehorende metagegevens en logbestanden leidt tot het volledig wissen of ontoegankelijk maken daarvan (met inbegrip van alle componenten van elk informatieobject en eventuele reservekopieën), en dat ze niet kunnen worden hersteld met behulp van functionaliteiten van de applicatie, gekoppelde applicaties/componenten en en/of specialistische technieken voor gegevensherstel.

Eis 200. De applicatie kan overzichten creëren van (aggregaties) van informatieobjecten die voor vernietiging in aanmerking komen.

Eis 201. De applicatie kan overzichten, van informatieobjecten die voor vernietiging in aanmerking komen, in een gewenst bestandsformaat beschikbaar maken.

Eis 202. De applicatie kan overzichten, van informatieobjecten die voor vernietiging in aanmerking komen, configureren op basis van beschikbare metagegevensvelden.

Eis 203. De applicatie kan het mogelijk maken om een rapport te genereren waaruit blijkt dat informatieobjecten en hun bijbehorende metagegevens zijn vernietigd.

Eis 204. De applicatie kan (verwijzingen naar) informatieobjecten en bijbehorende metagegevens in bulk vernietigen.

Eis 205. De applicatie kan (verwijzingen naar) informatieobjecten, en bijbehorende metagegevens, in alle op de voorziening aangesloten bronnen in één keer vernietigen (indien dit wenselijk is en daar bevoegdheid toe is).

Eis 206. De applicatie kan het vernietigingsproces geautomatiseerd uitvoeren (waar wenselijk en juridisch toegestaan).

Eis 207. De applicatie kan het mogelijk maken om, na een succesvol migratietraject naar een volgende applicatie, de achtergebleven informatieobjecten en bijbehorende metagegevens te vernietigen. Denk hierbij ook aan het overbrengen van informatieobjecten en bijbehorende metagegevens naar een archiefbewaarplaats.

Verantwoording

Eis 208. De applicatie kan rapporten genereren over alle mogelijke systeem- en gebruikersactie die samenhangen met informatieobjecten en bijbehorende metagegevens zoals, bijvoorbeeld, uitwisseling, opname, opslag, gebruik, beheer, export en verwijdering.

Eis 209. De applicatie kan, automatisch of op aanvraag, de gegevens van alle authenticatie- en veiligheidsgerelateerde activiteiten opnemen en laten zien wanneer dat gewenst is.