

Inhoud

Aanbestedingseisen Algemeen	2
Aanbestedingseisen Data	3
Aanbestedingseisen ICT & Security eisen	6
Aanbestedingseisen informatiebeheer vakapplicatie	12
Aanbestedingseisen Integratie	15
Aanbestedingseisen Mobile Devices	16
Aanbestedingseisen Technische Infrastructuur	17
Aanbestedingseisen Overig	18

Aanbestedingseisen Algemeen

Nr	Eis/Wens	Eis	Wens
ALG. 01	Het systeem biedt een testomgeving welke ketentesten mogelijk maakt.	X	
ALG. 02	SLA Opdrachtnemer stuurt bij inschrijving een concept SLA mee welke als uitgangspunt voor de overeenkomst dient. Het SLA moet minimaal de volgende onderwerpen bevatten: - Structurele updates van de server en software die ervoor zorgen dat de veiligheid, performance en betrouwbaarheid van de oplossing gewaarborgd blijft. - Reactie- en oplostijden bij incidenten. - Procesafspraken in verband met incidenten en onderhoud. Zie bijlage voor vb Producten - Informatiebeveiligingsdienst	X	
ALG. 03	Toegankelijkheid EN 301 549 (WCAG 2.1 AA/ WCAG 2.2) De oplossing voldoet aan de toegankelijkheidseisen.		X
ALG. 04	De leverancier dient duidelijk aan te geven welke afhankelijkheden er zijn van onderaannemers. Indien de leverancier gebruik maakt van onderaannemers zijn de voorwaarden opgesomd in dit document ook van toepassing op de onderaannemers.	X	

Aanbestedingseisen Data

Stuurinformatie en rapportages (algemene info)

Er wordt onderscheid gemaakt tussen stuurinformatie en rapportages op operationeel niveau en stuurinformatie op strategische en tactisch niveau.

Binnen de applicatie ter ondersteuning van de taakstelling Leerplicht/RMC/Jongerenloket en Leerlingvervoer zijn de dagdagelijkse en operationele rapportages beschikbaar. Deze rapportages zijn eenvoudig aan te maken door de functioneel beheerder binnen de applicatie zelf.

Gebruikers kunnen deze rapportages zelf opstarten binnen de applicatie.

Strategische en tactische informatie wordt gepubliceerd in de Business Intelligence-omgeving van de gemeente Sittard-Geleen, waardoor het management, de directie en het bestuur deze informatie op een centrale locatie kunnen raadplegen. De data van de applicatie ter ondersteuning van de taakstelling Leerplicht/RMC/Jongerenloket en Leerlingvervoer moet daarom beschikbaar worden gesteld aan de interne datasnelweg van Sittard-Geleen.

Nr	Eis/Wens	Eis	Wens
DAT. 01	Eigenaarschap: De gemeente Sittard-Geleen is en blijft eigenaar van de data in de applicatie.	X	
DAT. 02	Data benaderen: De gemeente Sittard-Geleen maakt gebruik van een eigen datasnelweg, waaraan diverse Business Intelligence-tools (IBM Cognos, Microsoft Power BI, ESRI ArcGIS, etc.) zijn gekoppeld. Deze tools worden gebruikt voor het genereren van integrale rapportages, dashboards en het uitvoeren van analyses. De data van applicatie ter ondersteuning van de taakstelling Leerplicht/RMC/Jongerenloket en Leerlingvervoer is beschikbaar voor de datasnelweg van Sittard-Geleen De gemeente Sittard-Geleen heeft volledige toegang tot alle data die geregistreerd wordt in de applicatie (tot het laagste detailniveau). Bij voorkeur wordt alle data via een realtime beveiligde API-verbinding beschikbaar gesteld. • Er is duidelijke documentatie beschikbaar hoe deze API gebruikt kan worden. • De inschrijver kan – indien nodig – ondersteuning bieden bij het gebruiken van deze API. Indien een API-verbinding niet haalbaar is, wenst de gemeente Sittard-Geleen periodiek een datadump te ontvangen van alle gegevens tot het laagste detailniveau, inclusief metadata. Deze datadump wordt via een beveiligde omgeving aangeboden in een standaard dataformaat, zoals CSV, XML, enz.	X	

DAT. 03	Wijzigingen in onderliggende database / aangeleverde data Als er wijzigingen plaatsenvinden in de onderliggende database en/of aangeboden dataset, dan wordt de gemeente tijdig geïnformeerd. Bovendien wordt aangegeven welke wijzigingen het betreft.	X	
DAT. 04	Kosten data beschikbaar stellen Er worden geen extra kosten in rekening gebracht voor het beschikbaar stellen van de data.	X	
DAT. 05	Datamodel: Er is een datamodel beschikbaar waarin staat beschreven welke gegevens in de oplossing zijn vastgelegd, hoe deze gegevens gestructureerd zijn en wat de verbanden zijn tussen die gegevens.	X	
DAT. 06	Vernietiging data: Informatie kan definitief worden vernietigd (de gemeente is hierbij in de lead). Leverancier maakt samen met gemeente afspraken rondom verantwoorde vernietiging in overeenstemming met het bewaar- en vernietigingsbeleid van de gemeente Sittard-Geleen. De gemeente heeft zich geconformeerd aan de selectielijst 2020. Het vernietigingsbeleid is gebaseerd op de archiefwet.	X	
DAT. 07	Bewaren data: Informatie kan in zijn originele digitale vorm worden overdragen naar een zaaksysteem en/of digitaal archief.	X	
DAT. 08	Integratie netwerk gemeente met extern: Koppelingen tussen het netwerk van Sittard-Geleen en de 'buitenwereld' extern vinden standaard plaats via de integratielaag van de gemeente Sittard-Geleen. Verbindingen worden opgezet via https.	X	
DAT. 09	BRP koppeling: REST API BRP zal d.m.v Haal Centraal gekoppeld worden.	X	
DAT. 11	Operationele informatie Binnen de applicatie zijn de dagdagelijkse en operationele rapportages beschikbaar.	X	
DAT. 12	Rapportage eenvoudig aan te maken Deze operationele rapportages zijn eenvoudig aan te maken door de functioneel beheerder binnen de applicatie zelf	X	
DAT. 13	Opstarten operationele rapportages door gebruikers Gebruikers kunnen deze operationele rapportages zelf opstarten binnen de applicatie.	X	
DAT. 14	Datakwaliteit -> gegevens dienen zo correct mogelijk worden ingevoerd. • Verplichte velden zijn echt verplicht • Gebruiken van veldvalidatieregels in de applicatie zoals: ○ Bij telefoonnummer kunnen alleen cijfers worden ingevoerd. ○ Een datum-tijdveld accepteert alleen geldige datums en tijden ○ Een valutaveld accepteert alleen geldbedragen • Gebruiken van invoermaskers ○ Een invoermasker kan gebruikers bijvoorbeeld verplichten om datums in een Europese notatie in te voeren, zoals 14-02-2024. • Door – waar mogelijk – keuzelijsten te gebruiken in plaats van vrije tekst	X	

DAT. Open vraag: Op dit moment maakt de gemeente Sittard-Geleen gebruik van de generieke rapportagevoorzieningen 'IBM Cognos' en "PowerBI". 15 Geografische data wordt gepubliceerd via het ESRI ArcGIS platform. Ook gebruikt de gemeente de ETL-software 'FME van Safe software'. Het is de bedoeling om dit in de toekomst uit te breiden met diverse generieke analysetools en andere BI-producten. Beschrijf welke ervaringen u heeft met het uitwisselen met generieke BI-voorzieningen. Geef hierbij ook aan welke ervaringen u heeft met onze huidige voorzieningen.	X	

Aanbestedingseisen ICT & Security eisen

Nr Eis ICT & Security	Eis/Wens	Eis	Wens
	Algemeen		
SE.CLD. 01.1	De te leveren (web)applicatie/dienst voldoet aan de Baseline Informatiebeveiliging Overheid. https://bio-overheid.nl/	X	
SE.CLD. 01.2	De complete omgeving, dus alle (web)applicaties en onderliggende infrastructuur zijn ingericht conform de verplichte standaarden van het Forum Standaardisatie: zie link. https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht	X	
	Beheerorganisatie		
SE.CLD. 01.3	De medewerkers van de opdrachtnemer (beheerorganisatie) hebben een recente Verklaring Omtrent Gedrag (VOG) of beschikken over een Screening van Justitie.	X	
	Authenticatie		
SE.CLD. 01.4	De aangeboden oplossing maakt geen gebruik van lokale gebruikers, maar sluit aan op de gemeentelijke authenticatiemogelijkheden, LDAPS of Azure AD/Entra ID Connect. Het is niet toegestaan andere authenticatiemethodes te gebruiken of een eigen systeem in het netwerk van de Gemeente Sittard-Geleen te plaatsen.	X	
SE.CLD. 01.5	Ten behoeve van accountsynchronisatie wordt gebruik gemaakt van Azure AD/Entra ID Connect, SSO / SAML.	X	
SE.CLD. 01.6	Authenticatie voor burgers vindt plaats middels DigiD en eIDAS. Indien de DigiD aansluiting via Gemeente Sittard-Geleen wordt aangevraagd, dient de opdrachtnemer jaarlijks een TPM-verklaring opgesteld door een RE aan te leveren ten behoeve van de ENSIA-verantwoording aan Logius. De jaarlijkse kosten van deze TPM worden meegenomen in de totale kosten van de aangeboden webapplicatie. Ook de kosten van de TPM-verklaring ten behoeve van de aansluitaudit worden meegenomen.	X	
SE.CLD. 01.7	Wordt een gemeentelijke DigiD aansluiting gebruikt, dan dient de opdrachtnemer alle info aan te leveren inclusief het gebruikte publieke certificaat en metadata (XML), beide aangeleverd als bestand.	X	
SE.CLD. 01.9	Implementatie van MFA op de doel applicatie is verplicht.	X	
SE.CLD. 01.10	Alle accounts dienen persoonsgebonden te zijn.	X	
	Web Services		
SE.CLD. 01.11	In de response headers wordt de versie van de webserver of service niet meegestuurd.	X	
SE.CLD. 01.12	Foutmeldingen geven geen details weer die misbruik mogelijk maken.	X	

SE.CLD. 01.13	Al het webverkeer wordt middels TLS getransporteerd (https). Zie hiervoor ook de eisen voor TLS.	X	
SE.CLD. 01.14	Alleen de benodigde HTTP-request methoden worden gebruikt. (B.v. GET, POST, PUT, DELETE)	X	
SE.CLD. 01.15	Connecties via http worden automatisch doorverwezen naar https middels een http response status code 3xx.	X	
SE.CLD. 01.16	De webserver stuurt securityheaders mee in de response headers. Voor een actueel overzicht van mee te sturen securityheaders zie: https://owasp.org/www-project-secure-headers/ Voor de Content Security Policy (CSP) geldt de volgende aanscherping: Onveilige configuraties zoals het gebruik van 'unsafe-inline' en 'unsafe-eval' zijn niet toegestaan. Het whitelisten van bronnen kan uitsluitend via een secure verbinding (https). De website heeft een A+ rating op https://securityheaders.com/	X	
SE.CLD. 01.17	De webapplicatie is minimaal beschermd tegen OWASP top 10 aanvallen. https://owasp.org/www-project-top-ten/	X	
SE.CLD. 01.18	De webapplicatie is conform de ict-beveiligingsrichtlijnen voor webapplicaties van het NCSC gebouwd. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties	X	
SE.CLD. 01.19	Voor mobiele apps, dient de inschrijver aan de ICT-beveiligingsrichtlijnen voor mobiele apps te voldoen. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps . Zie ook richtlijnen document MDM van de gemeente Sittard-Geleen. Ook zijn de apps altijd beschikbaar in Apple of Android store, geen sideloaded apps toegestaan.	X	
SE.CLD. 01.20	Een webbased userinterface is zonder beperking van functionaliteit benaderbaar door de laatste twee versies van de meest gangbare en ondersteunde browsers Microsoft Edge is een vereiste (aanvullend Google Chrome, Apple Safari en Mozilla Firefox) zonder gebruik te maken van NPAPI plug-ins (zoals Flash, Silverlight, ActiveX, etc.)	X	
SE.CLD. 01.21	Gebruikte Cookies zijn voorzien van de attributen 'Secure' en 'HttpOnly'. Cookies met gevoelige informatie hebben een korte levensduur en maken gebruik van het 'SameSite' attribuut met als waarde 'Strict' of 'Lax'.	X	
E-mail			
SE.CLD. 01.22	Binnen de Gemeente Sittard-Geleen verloopt mailverkeer met een (sub)domein uitsluitend via onze exchange server. Hierdoor kunnen we het serviceaccount en het mailverkeer beter beheren en controleren. De volgende standaarden worden toegepast: SPF, DKIM, DMARC, STARTTLS, DANE.	X	

SE.CLD. 01.23	De opdrachtnemer maakt geen gebruik van een eigen mailservice voor het mailen naar inwoners. Indien het alleen notificaties betreft naar medewerkers, is deze eis niet van toepassing.	X	
SE.CLD. 01.24	Veilig verzenden of mailen met zorgmail moet een ondersteunende functie zijn voor de applicatie. https://enovationgroup.com/nl/aanbod/producten/enovation-zorgmail/	X	
File Transfer Services			
SE.CLD. 01.25	Bij handmatige bestandsoverdrachten dient gebruik gemaakt te worden van Doczend (via de gemeente Sittard-Geleen). Indien een file transfer service noodzakelijk is, kan alleen gebruik gemaakt worden van SFTP of Explicit FTPS (TLS enforcement). Dit gaat alleen via onze secure gateway (reverse proxy).	X	
Domain Name System (DNS)			
SE.CLD. 01.26	Wordt door opdrachtnemer een 'eigen' domein gebruikt, dan moet DNSSEC (Domain Name System Security Extensions) worden toegepast.	X	
SE.CLD. 01.27	Domeinen waarvoor certificaten zijn uitgegeven dienen CAA records (DNS Certification Authority Authorization) te publiceren.	X	
SE.CLD. 01.28	Voor controle slagen via forum standaardisatie van het 'eigen' domein n.a.v. deze technische eisen moet de gemeente een CNAME op het eigen domein aanmaken met bijhorend overheidscertificaat die in de applicatie toegevoegd dient te worden.	X	
Transport Layer Security (TLS)			
SE.CLD. 01.29	Indien een domeinnaam wordt gebruikt die niet eigendom is van Gemeente Sittard-Geleen, dient de opdrachtnemer een officieel erkend certificaat te gebruiken. Die voldoet aan de eisen van forum standaardisatie en die alleen voldoende of sterke cipher suites gebruikt. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1	X	
SE.CLD. 01.30	TLS is volgens de richtlijnen van het NCSC ingericht. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1	X	
SE.CLD. 01.31	De server is zo ingericht en onderhouden dat deze een A+ rating behaalt op SSL Labs. https://www.ssllabs.com/ssltest/index.html	X	
Governance			
SE.CLD. 01.32	De inschrijver en eventuele onderaannemers zijn ISO27001/2 (Informatiebeveiliging) gecertificeerd en/of is in het bezit van een geldige ISAE3402 SOC2 assurance rapportage en/of levert ten tijde van de inschrijving jaarlijks een TPM-verklaring over de gehele dienstverlening inclusief onderaannemers, uitgegeven door een IT Auditor (RE en/of CISA), waarmee assurance wordt afgegeven over de kwaliteitsaspecten integriteit, beschikbaarheid en betrouwbaarheid in opzet, bestaan en werking. De jaarlijkse kosten van de TPM worden meegenomen in de totale kosten van de aangeboden dienstverlening.	X	

SE.CLD. 01.33	De opdrachtnemer ondertekent bij gunning en vooraf aan de POC de vrijwaringsverklaring waardoor de Gemeente Sittard-Geleen pentesten kan (laten) uitvoeren op de aangeboden oplossing. De template van deze vrijwaringsverklaring kan bij de Gemeente Sittard-Geleen worden opgevraagd.	X	
SE.CLD. 01.34	De opdrachtnemer werkt kosteloos mee aan audits uitgevoerd door of in opdracht van de aanbesteder. Deze audits worden uitgevoerd door of onder verantwoordelijkheid van een RE of CISA.	X	
Cloud			
SE.CLD. 01.35	De ICT-infrastructuur van de geboden oplossing is in zijn geheel ondergebracht in een datacenter binnen de EER. (Niet van toepassing bij On Premise installatie).	X	
Koppelingen			
SE.CLD. 01.36	De geboden oplossing ondersteunt zowel IPv4 als IPv6. Voor Cloud oplossingen dienen beide actief te zijn.	X	
SE.CLD. 01.37	Koppelingen/verbindingen tussen systemen en/of services (ook als deze op hetzelfde systeem draaien) worden door opdrachtnemer bij inschrijving inzichtelijk gemaakt in een protocol matrix, waarin de verkeerstromen zijn opgenomen. Deze matrix bestaat minimaal uit de volgende velden: • Source IPv(4/6) • Source Port • Destination IPv(4/6) • Destination Port • Layer 4 protocol (bijv. TCP/UDP/...) Application protocol (bijv.: http/https/smtp/dns/...).	X	
SE.CLD. 01.38	Koppelingen vanuit de SaaS omgeving van de opdrachtnemer naar derden (bv andere SaaS omgevingen) lopen ten allen tijden via de integratie laag (reverse proxy) van de Gemeente Sittard-Geleen. Rechtstreekse koppelingen zijn dus niet toegestaan.	X	
SE.CLD. 01.40	Koppelingen met onze integratie laag hebben minimaal het onderstaande beveiligingsniveau: REST architectuur: TLS & API Key SOAP / StUF architectuur: TLS Mutual Authentication	X	
SE.CLD. 01.41	Het aanbieden van RDP-koppelingen (of vergelijkbaar) evenals het gebruik van Remote Desktop Gateway is niet toegestaan.	X	
Versiebeheer			
SE.CLD. 01.42	De webapplicatie en onderliggende ICT-componenten zijn altijd up-to-date. Opdrachtnemer mag maximaal 1 stabiele patch aan het einde van de train (bijv 1.0.0.1)achterlopen, mits deze versie nog volledig wordt ondersteund door de betreffende leverancier van dat component en geen kwetsbaarheden bevat.	X	
Security Incidenten			
SE.CLD. 01.43	Security incidenten worden onverwijld (binnen 4 uur), na hiervan op de hoogte te zijn, gemeld bij de Gemeente Sittard-Geleen. (Per	X	

	telefoon +31464778999 en per e-mail aan: soc@sittard-geleen.nl en sd-ict@sittard-geleen.nl)		
SE.CLD. 01.44	Bij security incidenten worden de gevolgen zo snel mogelijk ongedaan gemaakt dan wel beperkt, waardoor het incident onder controle wordt gebracht. Over de genomen maatregelen wordt de Gemeente Sittard-Geleen geïnformeerd.	X	
	Logging		
SE.CLD. 01.45	De oplossing beschikt voor alle mutaties 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 gebruiker; • het gebruikte apparaat; • het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	X	
SE.CLD. 01.46	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	X	
SE.CLD. 01.47	Ten behoeve van de loganalyse is de bewaarperiode van de logging bepaald op 6 maanden. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	X	
SE.CLD. 01.48	Indien logging bij de Gemeente Sittard-Geleen niet kan, wordt voor de Gemeente Sittard-Geleen toegang geregeld tot de logfiles op de omgeving van de opdrachtnemer.	X	
SE.CLD. 01.49	Accounting van wijzigingen door specifieke accounts dient aan te staan en mogelijk te zijn binnen de gehoste service.	X	
	OTAP		
SE.CLD. 01.50	In de aangeboden oplossing wordt tevens de OTA-inrichting meegenomen.	X	
	Back-ups		
SE.CLD. 01.51	Regelmatige, geautomatiseerde back-ups van kritieke systemen en gegevens. Minimaal dagelijkse back-up.	X	
SE.CLD. 01.52	Validatie van back-up gegevens voor integriteit. Mechanismen voor authenticatie van back-up gegevens.	X	
SE.CLD. 01.53	Fysiek gescheiden opslaglocatie. Beveiligde opslaglocaties tegen fysieke schade en ongeoorloofde toegang.	X	
SE.CLD. 01.54	Versleuteling van back-up gegevens tijdens opslag en transport.	X	
SE.CLD. 01.55	Gedocumenteerde en geteste herstelprocedure. Gedefinieerde hersteltijden volgens organisatiebehoeften.	X	
SE.CLD. 01.56	Periodieke hersteltests voor effectiviteit.	X	
SE.CLD. 01.57	Bewaartijd gebaseerd op beleidsvereisten, zie hieronder: Reguliere back-up 30 dagen bewaartijd.	X	

SE.CLD. 01.58	Veilige en permanente verwijdering van verouderde back-ups. Gedetailleerde logboeken van bewaar- en verwijderacties. Zie ook logging eisen.	X	
SE.CLD. 01.59	Gedocumenteerde rechtvaardiging voor uitzonderingen	X	

Aanbestedingseisen informatiebeheer vakapplicatie

Nr	Eis/Wens	Toelichting	Eis	Wens
DIV. 01	Metadata die van belang is voor dossiervorming moet in ongewijzigde en ongecomprimeerde vorm worden aangeboden aan Open Zaak		X	
DIV. 02	De applicatie biedt de mogelijkheid tot definitief vernietigen van alle gegevens en bestanden, waarbij ook back-ups na een afgestemde retentietijd vernietigd worden.		X	
DIV. 03	Informatie (bestanden en metadata) moet toegankelijk en duurzaam blijven tijdens de geldende bewaartermijn.	Toegankelijk betekent vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar voor degenen die er recht op hebben, vanaf het moment van ontstaan en voor zolang als noodzakelijk (gerelateerd aan geldende bewaartermijn). Duurzaam betekent dat de toegankelijkheid van de informatie bestand is tegen veranderingen van elke aard. Deze geldende bewaartermijn kan variëren van 6 weken tot 20 jaar (na in werking treding nieuwe Archiefwet is de termijn uiterlijk 10 jaar).	X	
DIV. 04	De informatie (bestanden en metadata) moeten in de originele vorm overgebracht kunnen worden naar een digitaal duurzaam archief na de bewaartermijn van 20 jaar	Na het in werking treden van de nieuwe Archiefwet is de termijn uiterlijk 10 jaar	X	
DIV. 05	Het moet mogelijk zijn vernietigingslijsten/ overzichten te genereren op basis van een vooraf ingestelde vernietigingstermijn	Deze vernietigingstermijn wordt bij voorkeur opgesteld op zaakniveau	X	

DIV. 06	Het moet mogelijk zijn deze vernietigingslijsten als bestandsvorm op te slaan		X	
DIV. 07	Het mogelijk zijn deze vernietigingslijsten te kunnen distribueren		X	
DIV. 08	Het moet mogelijk zijn op basis van deze vernietigingslijsten de informatieobjecten (zaak, metadata, documenten) te kunnen vernietigen		X	
DIV. 09	Het moet mogelijk zijn een bewijs van vernietiging te kunnen opslaan in een bestandsvorm	De vernietigingslijst en het bewijs van vernietiging moeten blijvend bewaard worden	X	
DIV. 10	Het moet mogelijk zijn de vernietigingslijst te voorzien van een specifieke set aan metadata: zaaknummer (of uniek identificatienummer), omschrijving zaak, startdatum zaak, resultaat van de zaak, einddatum van afhandeling, bewaartermijn)		X	

Aanvullende vragen (geen eisen):

1. Welke bestandsformaten kunnen worden opgeslagen in de applicatie?
2. Is het mogelijk bewaar- en vernietigingstermijnen in te stellen (bij voorkeur op zaakniveau)?
3. Is het mogelijk deze termijnen per zaak handmatig aan te passen (in geval van uitzondering van vernietiging)?
4. Wat is de retentietermijn van back-ups?

Algemeen digitaal informatiebeheer

Nr	Eis/Wens	Toelichting	Eis	Wens
DIV. 11	Indien binnen de applicatie gebruik wordt gemaakt van algoritmes dan moeten de algoritmes in een leesbaar formaat kunnen worden opgeslagen en tevens buiten de applicatie worden bewaard	Indien gebruik gemaakt wordt van algoritmes dan dient de gemeente deze openbaar te maken. (Selectielijst 2020)	X	

DIV. 12	Indien de oplossing gebruik maakt van een algoritme, dient vooraf de ontwerpdocumentatie incl. input en output overlegd te worden ter archivering	Indien gebruik gemaakt wordt van algoritmes dan dient de gemeente deze openbaar te maken. (Selectielijst 2020). De gemeente dient zich te kunnen verantwoorden over de uitvoering van zijn taken. Indien in een proces een algoritme de beslissingen neemt i.p.v. de ambtenaar moet de gemeente zich kunnen verantwoorden over deze beslissingen.	X	
DIV. 13	Bij een migratie van data naar een ander systeem moet een verklaring kunnen worden opgeleverd waarin is opgenomen dat de migratie zonder onacceptabel gegevensverlies heeft plaatsgevonden (informatie is volledig interpreteerbaar)		X	
DIV. 14	Indien bij migratie/ conversie gegevensverlies optreedt, dan wordt in de verklaring gespecificeerd welke data verloren is gegaan. Dat kan bijvoorbeeld van toepassing zijn bij tekstvelden die het maximum aantal karakters overschrijden in de doelapplicatie		X	
DIV. 15	Bij het uitvoeren van migratie of conversie dient altijd een migratieplan en testplan te worden overhandigd.	(nadere invulling van details in het plan kunnen worden besproken na gunning)	X	
DIV. 16	In de oplossing is het mogelijk metadatavelden toe te voegen zonder extra (ontwikkelings)kosten.		X	

Aanbestedingseisen Integratie

Nr	Eis/Wens	Eis	Wens
INT. 01	De oplossing moet voor koppelingen met andere applicaties of functionaliteiten gebruik maken van actuele standaarden conform de GEMMA architectuur. Hierbij hebben eindproduct standaarden de voorkeur boven halffabrikaat- en grondstof standaarden.	X	
INT. 02	Sittard-Geleen hanteert het principe “Hergebruik van betrouwbare gegevens vindt plaats als hiervoor een landelijke verplichting geldt, de gegevens op meerdere plekken voor het uitvoeren van gemeentelijke taken nodig zijn of de gemeente de gegevens openbaar wil maken.”		X
INT. 03	Open vraag: Omschrijf van de standaarden waarvoor u geen officieel testrapport kunt aanleveren, per standaard: • Op welke wijze u het gebruik van de standaarden kunt realiseren; • Binnen welke termijn u garandeert te voldoen aan de standaard en dit kunt aantonen middels een officieel testrapport.	X	

Aanbestedingseisen Mobile Devices

Nr	Eis/Wens	Eis	Wens
MD. 01	Uw oplossing is dusdanig geprogrammeerd dat ze herkennen op welke apparaat de applicatie wordt geopend en hier hun schermopbouw op aanpassen (responsive design).	X	
MD. 02	Een mobiele applicatie (app) maakt geen gebruik van dataopslag op het apparaat of in een andere cloud dan het bronsysteem.	X	
MD. 03	Belanghebbenden werken altijd met de meest actuele versie van een App. Adviezen van de Informatie Beveiligings Dienst (IBD) worden hierin opgevolgd.	X	
MD. 04	Bij een zakelijke app voor belanghebbenden die de gemeente in gebruik neemt heeft de leverancier reeds bij het ontwerp en realisatie van de app goed over de beveiliging nagedacht (security by design).	X	
MD. 05	Een app die in gebruik wordt genomen dient te voldoen aan de Baseline informatiebeveiliging. Op basis van dataclassificatie moet de App mogelijk aan extra maatregelen voldoen.	X	
MD. 06	Afhankelijk van de dataclassificatie moet een (web)app checken of de toegestane besturingssystemen en browsers worden gebruikt.	X	
MD. 07	Bij vertrouwelijke/geheime informatie dient de (web)app na het geven van een melding te blokkeren, totdat het apparaat over de juiste versies beschikt.	X	
MD. 08	Bij bedrijfsvertrouwelijke informatie geeft de (web)app alleen een melding ten aanzien van de ongeschikte versie van het besturingssysteem en/of browser.	X	

Aanbestedingseisen Technische Infrastructuur

Nr	Eis/Wens	Eis	Wens
TI.01	Gegevens uit productieomgeving worden niet gebruikt in (O)T(A)-omgevingen (tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven).	X	
TI.02	De licentie van het product staat toe dat naast de installatie in de productieomgeving het product ook 2x in de Test-omgeving kan worden geïnstalleerd zonder extra kosten.		X

Aanbestedingseisen Overig

Nr	Eis/Wens	Eis	Wens
OV .01	De leverancier heeft het groeipact Common Ground ondertekend of treedt toe binnen 2 maanden (na afsluiten overeenkomst).		X
OV .02	De gemeente integreert en ontsluit haar gemeentelijke gegevensbronnen via gestandaardiseerde gegevensdiensten waar mogelijk aangeboden door gemeentelijke collectieve voorzieningen binnen Common Ground. Hierbij wordt gebruik gemaakt van Application Programming. Uw oplossing moet dit in de toekomst niet in de weg staan.		X
OV .03	Het realtime opvragen van detailgegevens bij de bronregistratie - nadat de afnemer op basis van een gebeurtenisbericht constateert dat de mutatie relevant is - heeft de voorkeur. Uw oplossing moet dit in de toekomst niet in de weg staan.	X	
OV .04	Betalen naar gebruik: Eis/open vraag: Bij een 'service georiënteerde architectuur' hoort ook een passend kostenmodel van de leveranciers. Namelijk betalen naar gebruik (pay for what you use). Dit betekent dat alleen de kosten in rekening worden gebracht voor de daadwerkelijk gebruikte functionaliteiten gedurende de betreffende periode. De gemeente zal bij livegang van het systeem mogelijk niet alle functionaliteiten van het systeem direct gebruiken. Daarnaast kan het ook voorkomen dat de gemeente ervoor kiest om bepaalde functionaliteiten niet meer in te zetten. U brengt daarom alleen de kosten in rekening van de daadwerkelijk gebruikte functionaliteiten (pay for what you use). Geef aan op welke wijze u invulling geeft aan betalen naar gebruik.	X	
OV .05	Exitstrategie: Open vraag: Een exit strategie dient aanwezig te zijn. Hieronder wordt tenminste verstaan dat de leverancier duidelijk dient aan te geven hoe er wordt omgegaan met de opgeslagen gegevens na afloop van het contract. Uitgangspunt is dat gegevens migreren naar een door de gemeente opgegeven locatie en daarna bij de leverancier worden verwijderd op een voor informatiebeveiliging verantwoorde wijze. Dit laatste geldt ook voor back-up media. De leverancier zorgt dat de data in een format wordt opgeslagen zodat migratie van gegevens naar een andere provider na afloop van het contract mogelijk is. Geef aan hoe geborgd is dat de data toegankelijk blijft voor de gemeente.	X	

OV .06	Workflow-/procesinrichting, modellering voor de behandeling en routing van zaken vindt plaats op basis van configuratie en niet op basis van programmeren. Kennis van programmeertalen en scripting is niet vereist.	X	
OV .07	De schaalbaarheid van de applicaties is zo geregeld/ingericht dat groei of afname van het gebruik niet hoeft te leiden tot ingrijpende wijzigingen.	X	
OV .08	Het recht op de nieuwste versies van het geleverde platform is inbegrepen bij het aanbod en de prijs.	X	