Bijlage 2 - Programma van eisen Informatievoorziening gemeente Westerkwartier

Gemeente Westerkwartier

Programma van eisen – Informatievoorziening gemeente Westerkwartier

1.1 Automatisering

1. De ICT-oplossing bestaat bij voorkeur uit één systeem maar mag tevens bestaan uit een samenhangende combinatie van producten en diensten. De ICT-oplossing dient als SaaS-dienst aangeboden te worden vanuit de door de Inschrijver te selecteren datacentra, niet zijnde de datacentra van gemeente Westerkwartier. Hierbij dienen technisch beheer en onderhoud volledig onderdeel te zijn van de levering.
2. Er mag enkel een on-premise component geleverd worden die nodig is voor een integratie van de off-premise-ICT-oplossing met de on-premise infrastructuur en / of systemen van gemeente Westerkwartier. De levering van een dergelijk component moet expliciet benoemd worden.
3. Technisch beheer van de SaaS oplossing valt onder de verantwoordelijkheid van de leverancier. Indien on-premise componenten aangeboden worden, verzorgt de leverancier alle upgrades, updates en patches en support van de door hem geleverde/ voor de ICT-oplossing geïnstalleerde / geconfigureerde softwarecomponenten (remote en zo nodig on-site).
4. De geleverde ICT-oplossing als IAAS, PAAS of SAAS-dienst waarborgt te allen tijde een strikte scheiding van gegevens tussen verschillende tenants, omgevingen of klanten. De aan gemeente Westerkwartier geleverde ICT-oplossing is volledig afgeschermd van andere klanten en draait in een geïsoleerde omgeving.
5. De ICT-oplossing integreert native met Microsoft 365 omgeving van de gemeente Westerkwartier.
6. Alle web-based onderdelen beschikken over een volledige schaalbare web-based userinterface die zonder beperking van functionaliteit, benaderbaar is op elk willekeurig device, door de laatste twee versies van de meest gangbare en ondersteunde webbrowsers (Microsoft Edge, Mozilla Firefox, Google Chrome, Apple Safari), zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, ActiveX of soortgelijke).
7. De aangeboden licenties en / of gebruiksrechten voor productieomgevingen zijn inclusief licenties en / of gebruiksrechten van een volledige testomgeving en volledige uitwijkfunctionaliteit van de ICT-oplossing. Leverancier garandeert de levering van deze omgevingen (inclusief licenties en / of gebruiksrechten) van de totale ICT-oplossing, die volledig gelijkwaardig zijn aan de geleverde productieomgeving. Alle omgevingen zijn volledig van elkaar gescheiden en staan in geen enkele relatie met elkaar.
8. De ICT-oplossing is niet enkel toegankelijk vanuit de omgeving van gemeente Westerkwartier, bestaande uit zowel fysieke als virtuele werkplekken. Ook is toegang voor mobiele medewerkers (en eventueel inwoners, ketenpartners, etc.) tot de ICT-oplossing mogelijk via publiek internet. Ongeacht het type informatie dat verwerkt wordt in de ICT oplossing is de toegang te allen tijde voorzien van multi / two-factor authentification of identificatiediensten, zoals DigiD, e-Herkenning en eIDAS.
9. De ICT-oplossing ondersteunt authenticatie op basis van Microsoft Entra ID. Gebruikers van (de verschillende onderdelen van) de aangeboden ICT-oplossing kunnen zich aan de hand

van Single Sign On(SSO) dit gebruikersaccount authentiseren om hiertoe geautoriseerd toegang te verkrijgen.

10. Voor zover er binnen de ICT-oplossing gebruik gemaakt wordt van functionaliteit om bestanden en / of gegevens te uploaden naar de ICT-oplossing, dan zorgt Inschrijver ervoor dat dit veilig gebeurt (bijvoorbeeld door SFTP met certificaten). Het proces wordt beschreven in de Service Level Agreement.
11. Voorafgaand aan enige installatie van, dan wel enige integratie met, delen van de ICT-oplossing op locatie ontvangt de gemeente Westerkwartier een technisch ontwerp welke dan beoordeeld en geaccordeerd kan worden door gemeente Westerkwartier. Hieruit blijkt hoe de ICT-oplossing technisch functioneert en wat er nodig is om de ICT-oplossing technisch goed te laten werken binnen de infrastructuren van gemeente Westerkwartier. In dit ontwerp is tevens zichtbaar hoe de verschillende gegevensuitwisselingen in functionele en technische zin (gaan) verlopen. Het technisch ontwerp beschrijft minimaal:
    a. Diagrammen, architectuur en structuren;
    b. Infrastructuur (hardware, (mobiele)apparatuur en netwerkcomponenten);
    c. Gegevensstromen;
    d. Interfaces en integraties (koppelingen, API en gebruikte protocollen);
    e. Beveiligingsmaatregelen (authenticatie, encryptie, autorisatie);
    f. Afhankelijkheden van derde partijen (cloud- en hosting).
12. Indien licenties van derde(n) noodzakelijk zijn voor het (blijvend) functioneren van de gehele ICT-oplossing, zoals beschreven in de scope, worden deze binnen de opdracht geleverd.
13. Indien de ICT-oplossing beschikt over een e-mail functionaliteit, dan heeft het de voorkeur om via mail relay te routeren naar de omgeving van de gemeente Westerkwartier met een herkenbare domeinnaam. Indien dit niet mogelijk is moet het versturen dan wel ontvangen van e-mails voldoen aan de volgende standaarden: STARTTLS, DANE, DKIM, DMARC en SPF.
14. De ICT-oplossing vereist geen installatie van additionele programmatuur op het endpoint device van de gebruiker.
15. De leverancier garandeert dat de eigen organisatie en partners (onderaannemers) gegevens, welke uit hoofde van de Opdracht verwerkt worden, uitsluitend binnen de Europese Economische Ruimte (EER) verwerkt worden. Tenzij er voldaan aan de voorwaarden van artikel 45 of 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte. en dat doorgifte naar landen buiten de Europese Economische Ruimte uitgesloten is. Inschrijver toont op het eerste verzoek hiertoe van gemeente Westerkwartier aan waar de gegevens staan opgeslagen. De leverancier draagt er zorg voor dat alle data die wordt verwerkt, opgeslagen of beheerd in het kader van de ICT-oplossing uitsluitend plaatsvindt binnen de Europese Economische Ruimte (EER). Afwijking hiervan is uitsluitend toegestaan indien wordt voldaan aan de voorwaarden zoals opgenomen in artikel 45 of artikel 46 van de Algemene Verordening Gegevensbescherming (AVG) en dit aantoonbaar door de leverancier kan worden gemaakt. Een dergelijke afwijking is slechts toegestaan na voorafgaande schriftelijke toestemming van de opdrachtgever.
16. Het datacenter waar de oplossing is gelokaliseerd is ISO-27001 gecertificeerd.
17. De leverancier levert een actuele architectuurplaat van de geleverde oplossing.
18. De te realiseren koppelingen / webservices / API's/ berichtuitwisselingen voldoen aan de landelijke standaarden zoals Digikoppeling, StUF (Standaard UitwisselingsFormaat), ZGW

API's (Zaakgericht Werken API-standaarden), Nederlandse API-strategie (API Design Rules – ADR).

19. Toegang tot en via API's en koppelvlakken is altijd geauthentiseerd en geautoriseerd. Dit gebeurt via erkende en gestandaardiseerde methoden zoals bijvoorbeeld OAuth 2.0/ OpenID Connect, token-based of certificaat-authenticatie. Anonieme of onbeveiligde toegang is niet toegestaan.
20. Berichtenverkeer wordt te allen tijde en minimaal ondersteund op basis van webservices zoals: XML, GraphQL, REST/Json, ebMS en SOAP.
21. Het distribueren van persoonsgegevens gaat via Makelaarssuite van PinkRoccade Local Government. De gegevens uit de BRP kunnen hierbij door binnengemeentelijke afnemers worden ingezien, overgenomen en in de eigen applicaties worden onderhouden in geval van mutaties op basis van binnengemeentelijk berichtenverkeer (STUF-BG, conform de meest actuele versie) voor binnengemeentelijk (her-)gebruik van gegevens. Alle koppelingen dienen via de Gegevensmakelaar gelegd te worden.
22. Het distribueren van NNP-gegevens gaat via de KvK Api of via de Makelaarssuite van PinkRoccade Local Government

Verklaring vragen over ICT-aansluitvoorwaarden
De leverancier verklaart dat hij voldoet aan de gestelde eisen op het gebied van ICT. Als de leverancier (gedeeltelijk) niet kan voldoen aan een specifieke eis, wordt dit gemotiveerd toegelicht en wordt toegelicht op welke wijze de leverancier invulling geeft aan deze eis of aan alternatieve risicobeperkende maatregelen.

Voor elke afwijking dient de leverancier ten minste de volgende informatie te verstrekken:

- Het nummer van de betreffende eis;
- Een omschrijving van de afwijking;
- De reden van de afwijking;
- Alternatieve invulling van gestelde de eis.

1.2 Informatiebeveiliging

Gemeente Westerkwartier hanteert de volgende eisen op het gebied van informatiebeveiliging om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te kunnen waarborgen:

1. De informatiebeveiliging vindt plaats volgens een algemeen erkend normenstelsel zoals NEN7510, NEN/ISO-27001, of de Baseline Informatiebeveiliging Overheid (BIO). De leverancier toont aan dat hij aan alle gestelde eisen voldoet in opzet, bestaan en werking, op basis van onderzoeken van onafhankelijke derden. Daartoe beschikt de leverancier over een geldig ISO 27001 en/of ISAE 3402 type II of gelijkwaardig certificaat. De leverancier is gedurende de duur van de overeenkomst gecertificeerd en toont dit aan zonder bijkomende kosten hiervoor.
2. Wanneer er sprake is van een DigiD aansluiting wordt jaarlijks door de leverancier een Third Party Mededeling (TPM) aangeleverd, die voldoet aan de Logius-richtlijnen.
3. De leverancier levert voorafgaand aan de dienstverlening een overzicht van leveranciers en toeleveranciers, waaronder subverwerkers. Veranderingen in (toe)leveringsketen worden voorafgaand aan de wijziging doorgegeven aan gemeente Westerkwartier via de aangewezen contactpersonen en contactgegevens.
4. De eisen in dit document zijn onverminderd van toepassing op (toe)leveranciers van de leverancier. De leverancier draagt er zorg voor dat deze eisen kenbaar worden gemaakt en ziet ook toe op de naleving van deze eisen door toeleveranciers.
5. Voor alle op te leveren softwarecomponenten, API's en koppelvlakken beschikt de leverancier over een actuele Software Bill of Materials (SBOM). (libraries, afhankelijkheden, versies). De leverancier houdt de SBOM gedurende de gehele levenscyclus van het product actueel.
6. De leverancier voert minimaal jaarlijks een (geautomatiseerde) penetratietest uit op het informatiesysteem. De resultaten hiervan kunnen op verzoek van Gemeente Westerkwartier worden ingezien of met medewerkers van Gemeente Westerkwartier worden besproken.
7. Gemeente Westerkwartier wordt via vertrouwde kanalen tijdig in kennis gesteld van ernstige beveiligingslekken in het geleverde informatiesysteem en tijdig in kennis gesteld van noodzakelijke mitigerende maatregelen.
8. Met betrekking tot alle web-omgevingen (zoals de te leveren self-service-webportalen), de verbinding daar naartoe en de adressering hierbij, voldoet de ICT-oplossing aan de volgende standaarden: DNSSEC en HTTPS en HSTS en IPv4 en IPv6 en TLS 1.2 of hoger, inclusief het gebruik van security-headers.
9. De geleverde ICT-oplossing beschermt alle gegevens door middel encryptie (versleuteling), zowel at rest (opslag) als in transport (gegevensuitwisseling). De versleuteling voldoet aan actuele standaarden zoals deze zijn opgenomen in het Forum standaardisatie.
10. Wanneer voor de werking van de ICT-oplossing een on-premise server benodigd is dan moet dit een virtuele machine zijn welke wordt voorzien van de hardened template van de gemeente Westerkwartier.
11. De ICT-oplossing ondersteunt robuuste en centraal beheerde authenticatie op basis van moderne standaarden. De oplossing vereist het gebruik van sterke authenticatie, bestaande uit wachtwoorden in combinatie met phishingresistente MFA, (bijv. FIDO2).
12. De ICT-oplossing ondersteunt bij voorkeur authenticatie via Microsoft Entra ID als centrale identity provider. Hierbij wordt federatieve authenticatie toegepast en wordt Single Sign-

On (SSO) gerealiseerd op basis van open standaarden en protocollen zoals SAML 2.0, OpenID Connect en OAuth 2.0.

13. De ICT-oplossing heeft de mogelijkheid op functionaliteit-, module-, registratie-, tabel-, menu, veld- proces- en documentniveau te autoriseren op basis van functiegroepen en -rollen. Eveneens ontstaat hiermee de mogelijkheid om functionaliteiten, registraties, processen en documenten ontoegankelijk te kunnen maken voor functiegroepen en rollen. Er mogen geen algemene user accounts worden aangemaakt of gebruikt, deze dienen altijd aan personen gerelateerd te zijn.
14. De ICT-oplossing heeft een mogelijkheid om vastgelegde autorisaties op alle niveaus inzichtelijk te maken per persoon, per gebruikersgroep en rol. Hiervoor is het toegepaste autorisatieschema te exporteren naar een bestand, dat leesbaar en begrijpelijk is voor derden (zoals toezichthouders zoals bijvoorbeeld de accountant, auditors, etc.).
15. Voor administratieve taken wordt een naar een persoon herleidbaar separaat account (beheer- en admin) gebruikt. Beheer- en admin accounts van de geleverde IT-oplossing worden ingericht op basis van strikte noodzaak (need-to-know/ need-to-do) en zijn uitsluitend bedoeld voor beheer.
16. Leverancierstoegang tot de geleverde ICT- oplossing wordt uitsluitend toegestaan op basis van strikte noodzaak (need-to-know/ need-to-do). De leverancier krijgt geen permanente of onbeperkte toegang; toegang wordt per incident, wijziging of voor onderhoud afzonderlijk aangevraagd en geautoriseerd door Gemeente Westerkwartier. Alle uitgevoerde handelingen moeten herleidbaar zijn.
17. De ICT-oplossing biedt zodanige functionaliteit m.b.t.auditing / logging dat van alle relevante handelingen en pogingen daartoe voor wat betreft algemene toegang tot de ICT-oplossing, processen, processtappen, mutaties, statuswijzigingen en registraties - zowel door gebruikers als de ICT-oplossing zelf - door middel van logging een historie wordt vastgelegd (van welke handelingen en pogingen daartoe, wanneer en door wie zijn uitgevoerd). De ICT-oplossing is hiermee concreet in staat informatie te geven over wie welke processen en processtappen heeft gestart, uitgevoerd, afgehandeld met vermelding van datum en tijd. Een logregel bevat minimaal: een tot een natuurlijk persoon herleidbare gebruikersnaam of ID, de gebeurtenis, waar mogelijk de identiteit van het werkstation of de locatie, het object waarop de handeling werd uitgevoerd, het resultaat van de handeling en de datum en het tijdstip van de gebeurtenis. Alle activiteiten in het systeem moeten in het kader van een audit-trail worden gelogd in een logboek. (database). De loggevens zijn beveiligd tegen ongeautoriseerde toegang en een beheerder mag niet in staat zijn de loggegevens te muteren.
18. De geleverde ICT-oplossing, inclusief de door de ICT-oplossing opgeslagen informatie is onderdeel van een betrouwbare back-upvoorziening die is beschermd tegen ongeautoriseerde toegang en tegen ransomware (offline/immutable). De leverancier controleert minimaal jaarlijks dat de back-ups succesvol en volledig kunnen worden hersteld binnen gestelde contractuele eisen.
19. De leverancier van de ICT-oplossing geeft op voorhand inzicht in het maximale mogelijke dataverlies (RPO) van Gemeente Westerkwartier in geval van een incident of calamiteit. Daarbij wordt een onderscheid gemaakt tussen redundante opslag en replicatie van gegevens en het herstel van gegevens uit een (offline/offsite) back-up.
20. De leverancier verricht zelfstandig een uitwijktest van de ICT-oplossing, zodat de borging van continuïteit en integriteit van (de gegevens in c.q. te benaderen via) de ICT-oplossing uitvoerig wordt getest.

21. De leverancier van de ICT-oplossing is transparant is over kwetsbaarheden en informatiebeveiligingsincidenten waaronder datalekken. Uiterlijk Deze worden zo spoedig mogelijk doch uiterlijk binnen 24 uur gemeld zodat Gemeente Westerkwartier in staat wordt gesteld om eigen maatregelen te nemen om schade te voorkomen of te beperken.

Verklaring vragen over informatiebeveiliging
De leverancier verklaart dat hij voldoet aan de gestelde eisen op het gebied van privacy. Als de leverancier (gedeeltelijk) niet kan voldoen aan een specifieke eis, wordt dit gemotiveerd toegelicht en wordt toegelicht op welke wijze de leverancier invulling geeft aan deze eis of aan alternatieve risicobeperkende maatregelen.

Voor elke afwijking dient de leverancier ten minste de volgende informatie te verstrekken:
- Het nummer van de betreffende eis;
- Een omschrijving van de afwijking;
- De reden van de afwijking;
- Alternatieve invulling van gestelde de eis.

1.3 Privacy

1. Leverancier voldoet aantoonbaar aan de relevante wet- en regelgeving op het gebied van privacy en informatiebeveiliging voor gemeenten, waaronder de (Uitvoeringswet) Algemene verordening gegevensbescherming (AVG). Ten behoeve hiervan heeft de leverancier beleid en procedures ontwikkeld en vastgesteld die periodiek worden herzien.
2. Leverancier zorgt ervoor dat iedere medewerker die met (persoon)gegevens van de gemeente Westerkwartier werkt, aantoonbaar getraind is op onderwerpen informatiebeveiliging en privacy.
3. Leverancier verleent haar volledige medewerking, waaronder het verstrekken van alle relevantie informatie, voor inventarisatie en controle de verwerking van persoonsgegevens in de ICT-oplossing door de gemeente Westerkwartier, waar nodig wordt Data Protection Impact Assessment (DPIA) uitgevoerd.
4. Wanneer toestemming van de betrokkene is een grondslag voor de verwerking van persoonsgegevens in de ICT-oplossing, faciliteert de ICT-oplossing de wettelijke vereisten van toestemming en biedt zij de mogelijkheid om deze toestemming schriftelijk vast te leggen en te bewaren om de rechtmatigheid van de verwerking te borgen.
5. De ICT-oplossing maakt het mogelijk om de persoonsgegevens te bewaren volgens de bewaartermijnen opgenomen in de meest recente versie van de Selectielijst gemeenten en intergemeentelijke organen of bewaartermijnen die door de gemeente Westerkwartier zijn vastgesteld. Bij het verstrijken van de bewaartermijn worden de persoonsgegevens automatisch vernietigd.
6. De ICT-oplossing maakt het mogelijk om eenvoudig en, waar mogelijk geautomatiseerd, uitvoering te geven aan de rechten van de betrokkene, zoals bedoeld in Hoofdstuk III van de AVG, met inachtneming van privacy rechten van derden. Dit houdt onder andere in dat de ICT-oplossing een overzicht kan verstrekken van de verwerkte persoonsgegevens van een betrokkene in het geval van een inzageverzoek.
7. De ICT-oplossing voldoet aan de vereisten met betrekking tot privacy by design en privacy by default, vastgelegd in artikel 25 AVG.
8. Leverancier heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.
9. Bij beëindiging van de overeenkomst levert de leverancier de persoonsgegevens terug of stelt deze beschikbaar voor overdracht aan een ander systeem, afhankelijk van de wens van de gemeente Westerkwartier. Daarna vernietigt de leverancier deze persoonsgegevens binnen één maand, voor zover de wet dat toestaat.
10. Afspraken tussen de leverancier en de gemeente Westerkwartier over de gegevensverwerking worden vastgelegd in een passende modelovereenkomst, conform de meest recente versie van de VNG.
11. In aanvulling op artikel 4.2 van de standaard VNG verwerkersovereenkomst is de gemeente Westerkwartier gerechtigd om de wezenlijke verplichtingen uit hoofde van de verwerkersovereenkomst en bijhorende bijlagen jaarlijks te laten controleren door een gecertificeerde auditor, alsmede bij een redelijk vermoeden van het niet voldoen aan deze verplichtingen.

Verklaring vragen over privacy
De leverancier verklaart dat hij voldoet aan de gestelde eisen op het gebied van privacy. Als de leverancier (gedeeltelijk) niet kan voldoen aan een specifieke eis, wordt dit gemotiveerd toegelicht en wordt toegelicht op welke wijze de leverancier invulling geeft aan deze eis of aan alternatieve risicobeperkende maatregelen.

Voor elke afwijking dient de leverancier ten minste de volgende informatie te verstrekken:

- Het nummer van de betreffende eis;
- Een omschrijving van de afwijking;
- De reden van de afwijking;
- Alternatieve invulling van gestelde de eis.

1.4 Communicatie

1. De onderdelen van de aangeboden ICT-oplossing die web-based zijn dan wel web-based worden, voldoen aan de vigerende toegankelijkheidseisen conform EN 301 549 van Standaardisatie Forum en Web Content Accessibility Guidelines 2.1 Level AA (WCAG 2.1 AA). Dit geldt zonder uitzondering voor alle interne en externe componenten van de aangeboden ICT-oplossing, inclusief componenten achter een login. De leverancier toont haar compliancy aan door middel van een onderzoeksrapport opgesteld volgens de WCAG-EM methodiek, dat op eerste verzoek van gemeente Westerkwartier wordt verstrekt. De ICT-oplossing dient mee te ontwikkelen met aanpassingen in de (wettelijke) toegankelijkheidseisen.
2. Voor applicaties waarbij communicatie met inwoners of ondernemers plaatsvindt, dienen ZGW-API's (Zaak Gericht Werken) te worden geïmplementeerd conform de actuele standaarden van VNG Realisatie. Deze ZGW-API's moeten aansluiting mogelijk maken op de bestaande Formulieren en Mijn Westerkwartier omgeving en voldoen aan de Common Ground principes. De API's faciliteren de uitwisseling van gegevens, statussen en documenten zonder dat aanvullende maatwerkoplossingen noodzakelijk zijn.
3. Voor alle portaalfunctionaliteit geldt: deze worden aan de hand van een 'fully qualiyfied domainname' van gemeente Westerkwartier beschikbaar gesteld, te weten <subdomein>.Westerkwartier.nl.
4. Huisstijl
    a. De ICT-oplossing dient volledig aanpasbaar te zijn aan de huisstijl van gemeente Westerkwartier. Dit omvat zonder uitzondering alle interne en externe componenten, zowel voor als achter de login. De leverancier garandeert volledige flexibiliteit voor het doorvoeren van huisstijlelementen zoals logo, kleurstellingen, typografie, fotografie en vormgevingsprincipes. De ICT-oplossing moet zodanig zijn ingericht dat toekomstige wijzigingen in de huisstijl eenvoudig kunnen worden doorgevoerd zonder ingrijpende technische aanpassingen.
    b. Wanneer de applicatie een (niet-optionele) document-creatie component bevat moeten brieven volgens de lay-out, zoals vastgelegd in de huisstijl, kunnen worden gegenereerd.

Verklaring vragen over communicatie en toegankelijkheid
De leverancier verklaart dat hij voldoet aan de gestelde eisen op het gebied van communicatie en toegankelijkheid. Als de leverancier (gedeeltelijk) niet kan voldoen aan een specifieke eis, wordt dit gemotiveerd toegelicht en wordt toegelicht op welke wijze de leverancier invulling geeft aan deze eis of aan alternatieve risicobeperkende maatregelen.

Voor elke afwijking dient de leverancier ten minste de volgende informatie te verstrekken:

- Het nummer van de betreffende eis;
- Een omschrijving van de afwijking;
- De reden van de afwijking;
- Alternatieve invulling van gestelde de eis.

1.5 Digitale Informatie

Archivering:

1. De ICT-oplossing waar informatie in opgeslagen wordt die onder de selectielijst van de VNG (https://vng.nl/artikelen/selectielijst) vallen moeten archiefwaardig de informatie op kunnen slaan;
2. Hiervoor moet het minimaal mogelijk zijn documenttypes aan documenten te kunnen koppelen. Het afhandelen van processen wordt zaakgericht vastgelegd waarbij ook een resultaat gekozen kan worden. De vernietigingstermijnen worden vastgelegd op basis van het zaaktype (eventueel documenttype) en het resultaat;
3. Specifieke (voornamelijk AVG) vernietigingstermijnen worden op basis van wijzigingen van onderliggende brondata getriggerd;
4. Het moet mogelijk zijn om een publicatielijst te kunnen exporteren om vervolgens data automatisch te kunnen vernietigen vanuit het systeem zelf;
5. Het Normenkader is volgens de NEN 2082.

Data:

1. Data uit de applicatie moet in het datawarehouse van de gemeente geladen kunnen worden;
2. Data moet via een beveiligde verbinding opgehaald worden;
3. De voorkeur is een verbinding die op basis van firewall regels een beveiligde verbinding legt tussen de beide systemen waar de data in zit en een readonly toegang voor het ophalen van de data. Hierdoor is er een technische beveiliging voor de verbinding en een toegangsbeveiliging voor het benaderen van de data (zie verder ook de eisen onder automatisering en informatiebeveiliging);
4. De koppeling met het DWH is beveiligd volgens BIO en AVG.
5. De toegangsbeveiliging voor het ophalen van data moet via een systeem account gebeuren en niet via een gebruikersaccount;
6. Het wachtwoorden van een systeemaccount mag niet vanzelf verlopen;
7. Datatoegang wordt gelogd en minimaal 12 maanden bewaard;
8. Gegevens zijn ontsluitbaar via een REST API (bij voorkeur OData) en/of via database-toegang (read-only);
9. De leverancier levert actuele documentatie over: API's / extracties en beveiligingsmechanismen;
10. Bij levering- of verbindingsfouten wordt er een foutmelding terug geleverd;
11. Om data te kunnen duiden levert de leverancier een ERD schema (Entiteit Relationship Diagram) aan met eventueel aanvullende documentatie;
12. Aangeleverde data moet bij voorkeur niet ouder dan één dag zijn;
13. Wijzigingen in datamodel of API worden minimaal 2 weken vooraf aangekondigd;
14. Breaking changes worden expliciet aangekondigd;
15. Backward compatibility wordt zo veel mogelijk behouden;
16. Als de leverancier datamarts beschikbaar heeft zouden wij deze graag ontvangen.

Verklaring vragen over archivering en data
De leverancier verklaart dat hij voldoet aan de gestelde eisen op het gebied van archivering en data. Als de leverancier (gedeeltelijk) niet kan voldoen aan een specifieke eis, wordt dit gemotiveerd toegelicht en wordt toegelicht op welke wijze de leverancier invulling geeft aan deze eis of aan alternatieve risicobeperkende maatregelen.

Voor elke afwijking dient de leverancier ten minste de volgende informatie te verstrekken:

- Het nummer van de betreffende eis;
- Een omschrijving van de afwijking;
- De reden van de afwijking;
- Alternatieve invulling van gestelde de eis.

1.6 Functionele eisen

1. Indien hiervan sprake is wordt functioneel beheer uitgevoerd door een aangewezen beheerder van gemeente Westerkwartier zelf.
2. Uitvoering van tenminste de ondergenoemde taken dient mogelijk te zijn, zonder tussenkomst van een leverancier. Hiertoe worden alle benodigdheden (opleiding, documentatie, toegang, etc.) door de leverancier geleverd, zodat het functioneel beheer zelfstandig, en incidenteel onder begeleiding van de leverancier, uitgevoerd kan worden.
    a. Alle beheertaken op functioneel vlak kunnen worden uitgevoerd terwijl gebruikers zijn ingelogd, uitgezonderd het eventueel direct toepassen van gewijzigde autorisaties.
    b. Functionele wijzigingen dienen direct te kunnen worden geactiveerd voor gebruikers, zodat deze gelijk actief zijn dan wel na uit- en inloggen van de gebruiker
    c. Binnen de ICT oplossing moeten minimaal 2 users als functioneel beheerder kunnen worden geautoriseerd.
3. Autorisatiebeheer
    a. Een door gemeente Westerkwartier aangewezen beheerder kan in de ICT-oplossing zelfstandig gebruikers (de)activeren en toegang verlenen. Let op: in beginsel wordt hierbij uitgegaan van authenticatie op basis van een Microsoft Entra ID.
    b. Een door gemeente Westerkwartier aangewezen beheerder kan de ICT-oplossing afstemmen op de eigen organisatie-inrichting, voor wat betreft medewerkers, teams en rollen.
    c. Een door gemeente Westerkwartier aangewezen beheerder kan de ICT-oplossing afstemmen op de eigen organisatie-werkwijze, voor wat betreft processen en de gerelateerde termijnbewaking.
4. Een door gemeente Westerkwartier aangewezen beheerder kan de ICT-oplossing volledig afstemmen op de eigen huisstijl-documenten, voor wat betreft de opbouw en lay-out van documenten die met de ICT-oplossing kunnen worden gecreëerd.
    a. Bij voorkeur kan worden gekoppeld aan de huidige document creatie applicatie van de gemeente Westerkwartier.
5. Een door gemeente Westerkwartier aangewezen beheerder kan de berichtenuitwisselingen met systemen en afnemers monitoren op volledigheid en correctheid en zo nodig functioneel herstel hierop uitvoeren.
6. Auditing / logging genoemd bij 2.16 dient zonder tussenkomst van de Inschrijver, bij voorkeur vanuit de interface van de ICT-oplossing, bekeken te kunnen worden.
7. De functioneel beheerder moet proactief geïnformeerd worden over verstoringen in het gebruik van de ICT-oplossing.
8. Er moet een gedegen omgeving zijn van waar de functioneel beheerder beheer documentatie en release informatie kan vinden.
9. Er moet een gedegen omgeving zijn waar de functioneel beheerder verstoringen, issues en wensen kan melden en van waaruit de functioneel beheerder de status ervan kan volgen.

Verklaring vragen over functionele eisen en beheer
De leverancier verklaart dat hij voldoet aan de gestelde eisen op het gebied van functionele eisen en beheer. Als de leverancier (gedeeltelijk) niet kan voldoen aan een specifieke eis, wordt dit gemotiveerd toegelicht en wordt toegelicht op welke wijze de leverancier invulling geeft aan deze eis of aan alternatieve risicobeperkende maatregelen.

Voor elke afwijking dient de leverancier ten minste de volgende informatie te verstrekken:

- Het nummer van de betreffende eis;
- Een omschrijving van de afwijking;
- De reden van de afwijking;
- Alternatieve invulling van gestelde de eis.

1.7 SLA

1. De ICT-dienst is 99,9% beschikbaar per maand, exclusief gepland onderhoud.
2. Gepland onderhoud vindt plaats buiten kantoortijden (ma–vr 18:00–07:00). En wordt minimaal 5 werkdagen vooraf aangekondigd.
3. De leverancier beschikt over een Business Continuity Plan (BCP) en Disaster Recovery Plan (DRP). Dit plan wordt minimaal jaarlijks getest.
4. Maximale hersteltijd (RTO) bij een calamiteit: 4 uur
5. Support is beschikbaar 24x7 of ma–vr 08:00–18:00 (afhankelijk van afspraak).
6. De leverancier monitort prestaties en capaciteit(opslag) proactief.
7. Bij beëindiging ondersteunt de leverancier een exit-strategie zonder vendor lock-in.
8. Data wordt geleverd in open standaarden (conform "Pas toe of leg uit").
9. Overdracht naar een nieuwe leverancier wordt actief ondersteund.
10. Data wordt na beëindiging aantoonbaar veilig verwijderd.

Verklaring vragen over SLA
De leverancier verklaart dat hij voldoet aan de gestelde eisen op het gebied van functionele eisen en beheer. Als de leverancier (gedeeltelijk) niet kan voldoen aan een specifieke eis, wordt dit gemotiveerd toegelicht en wordt toegelicht op welke wijze de leverancier invulling geeft aan deze eis of aan alternatieve risicobeperkende maatregelen.

Voor elke afwijking dient de leverancier ten minste de volgende informatie te verstrekken:

- Het nummer van de betreffende eis;
- Een omschrijving van de afwijking;
- De reden van de afwijking;
- Alternatieve invulling van gestelde de eis.

Team:	Automatisering, Digitale Informatie, Communicatie, Concerncontrol
Datum:	18-02-2026
Versie:	1.1

Gemeente Westerkwartier