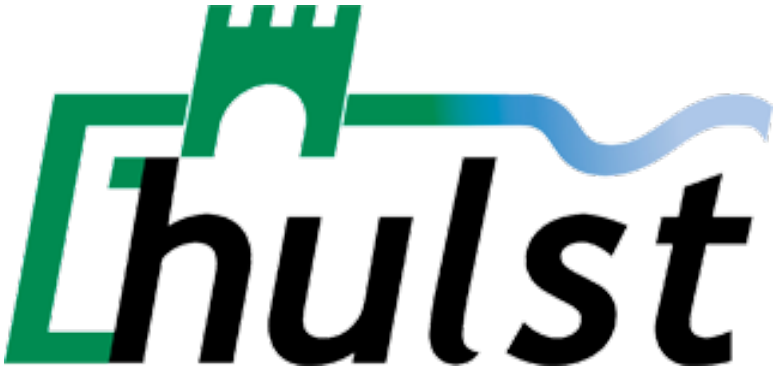
Bijlage 05 Programma van Eisen

Namens gemeente Hulst:



Begeleid door InnoviQ / Telengy:

Onderwerp	: Bijlage 05 Programma van Eisen
Kenmerk	: HUL220224
Datum	: 24 februari 2022
Status	: Definitief
Versie	: v.1.0.

Programma van Eisen

Functionele Eisen

1. De Oplossing voldoet volledig en tijdig aan de uitvoering van de volledig beschreven Opdrachtscope, met inbegrip van de detailuitwerking van de scope-bepalingen (zie bijlage 04), en de hieraan gerelateerde wet- en regelgeving gedurende de gehele looptijd. Onder deze wet- en regelgeving wordt ten minste - maar niet uitsluitend - verstaan: volledige compliancy op het AVG en BIO voor de huidige en toekomstige versies. De gemeente 'verzekert' zich hiermee binnen de Opdracht voor dergelijke wijzigingen en 'koopt' het desbetreffende onderhoud hiermee af binnen de Overeenkomst. Het onderhoud dat hiervoor benodigd is, wordt geacht onderdeel uit te maken van de Opdracht.
2. Het is mogelijk om geautomatiseerd een vernietigings- of overdrachtslijst te genereren, inclusief de grondslag hiervan waarbij deze lijst handmatig is aan te passen door een archiefverantwoordelijke alvorens tot daadwerkelijke uitvoering/verwerking van de lijst wordt overgegaan. Als alle relevante gegevens van een persoon zijn/worden vernietigd, worden eveneens alle gerelateerde gegevens binnen de Oplossing verwijderd. Het volledige vernietigingsproces kan door de gemeente worden doorlopen en uitgevoerd, zonder tussenkomst van de Inschrijver.
3. Het is mogelijk om de informatieobjecten en/of zaakdossiers met hun metadata, die elders en vaak permanent bewaard moeten blijven, te extraheren of migreren (naar een e-depot).
4. De Oplossing biedt standaard de mogelijkheid om zaken (functionaliteit, formulieren, workflows, e.d.) die in de testomgeving zijn gemaakt handmatig door de functioneel beheerder beschikbaar te stellen in de productieomgeving, zonder dat hiervoor de zaken opnieuw moeten worden gedefinieerd (bijvoorbeeld met behulp van export-import functionaliteit).

Technische Eisen

5. De SaaS-oplossing dient minimaal te voldoen aan:
    a. De opslag van (persoons)gegevens vindt fysiek plaats binnen de EER in een datacenter van minimaal van het niveau Tier 3 of gelijkwaardig;
    b. Toegang tot de SaaS-omgeving is alleen mogelijk via de werkplek omgeving van gemeente Hulst;
    c. Authenticatie van gebruikers vindt plaats op basis van SSO (connectie met Azure AD);
    d. De SaaS-omgeving bestaat minimaal uit een gescheiden test- en productieomgeving;
    e. De data in de testomgeving dient in het kader van de AVG met fictieve informatie gevuld te worden;
    f. Het technisch beheer van deze SaaS-omgeving wordt uitgevoerd door de leverancier;
    g. Het onderhoud van deze SaaS-omgeving wordt uitgevoerd door de leverancier, waarbij sprake is van continuous delivery van releases en patches, bij voorkeur op een multi-tenant omgeving voor alle klanten. Het functioneel beheer van de Oplossing geschiedt door de gemeente zelf;
    h. De SaaS-omgeving voldoet aan de BIO en aan de AVG, getoetst met behulp van een DPIA;
    i. Data-opslag is volledig gescheiden (ten minste logisch) van andere klanten van de Inschrijver en is encrypted;
    j. Indien data op basis van wettelijke eisen door Nederlands bevoegd gezag wordt gevorderd de Leverancier terstond de gemeente hierover informeert en niet zonder toestemming van de gemeente levert;
    k. Indien data op basis van wettelijke eisen door niet-Nederlands bevoegd gezag wordt gevorderd de leverancier terstond de gemeente hierover informeert en niet zonder toestemming van de gemeente levert;
    l. Alle gebruikte verbindingen dienen beveiligd te zijn en te voldoen aan de op dat moment geldende beveiligingsnormen, al dan niet met certificaten geregeld.
6. Leverancier mag enkel on-premise componenten leveren die enkel nodig zijn voor een correcte integratie van de off-premise-oplossing met de infrastructuur en / of systemen van de gemeente, mits

dit expliciet aangegeven wordt door leverancier in de Inschrijving en die niet reeds in de bestaande infrastructuur voorhanden is. Alle componenten van de Oplossing dienen off-premise geleverd te worden. Leverancier dient dergelijke situaties in haar Inschrijving aan te geven in het onderdeel Programma van Wensen: implementatieplan.

7. De Oplossing dient zich in een webbased omgeving te presenteren, ten minste web- responsive en bij voorkeur cloud-native, die volledig functioneel en remote wordt ondersteund op standaardbrowsers, waarbij de webbrowsers Chrome en Edge voor wat betreft de versies van het afgelopen jaar worden ondersteund. De Oplossing maakt geen gebruik van extra configuratie, plug-ins en software, anders dan de standaardconfiguratie van genoemde webbrowsers. Instellingen worden in de gebruikersprofielen opgeslagen en zijn dus niet machine gebonden.
8. De Oplossing dient benaderbaar te zijn via een “fully qualified domain name”. Voor onderdelen van de Oplossing die in dienstverleningsprocessen aan burgers en bedrijven worden gebruikt, wordt een subdomein van .gemeentehulst.nl toegepast.
9. De aangeboden Oplossing is inclusief voldoende opslagruimte en voldoende dataverbinding voor het benodigd dataverkeer (initieel en gedurende de contractduur) voor adequaat gebruik door de gemeente.

Service Eisen

10. De leverancier verplicht zich tot het voorzien in een SLA / DAP op basis van de volgende minimale criteria:
    a. De gehele Oplossing is 24 uur per dag / 7 dagen per week toegankelijk rekening houdend met de volgende percentages en tijdsblokken, onafhankelijk van tijd, plaats en type device:
        i. Beschikbaarheid van de gehele Oplossing incl. de webportalen, uitgaande van een beschikbaarheid van de gemeentelijke infrastructuur van 100%, op werkdag van 07:00 tot 23:00 uur voor ten minste 99,5% op jaarbasis;
        ii. Daarbuiten geldt een beschikbaarheidsgarantie van 95% op jaarbasis;
    b. Downtime vanwege installatie- en herstelverzoeken en gepland onderhoud en beheer van de gemeente wordt niet meegerekend in het meten van de beschikbaarheid;
    c. Gepland onderhoud en beheer met risico op downtime worden in beginsel buiten deze tijden uitgevoerd;
    d. De leverancier is verantwoordelijk voor backup, restore, recovery en uitwijk met betrekking tot de gehele Oplossing. Hiervoor geldt een RPO van maximaal 24 uur en een RTO van maximaal 4 uur;
    e. De SLA / DAP dient ‘operationeel’ te zijn bij oplevering van de Oplossing;
    f. Zodra er in de keten van informatieoverdracht een storing optreedt, waardoor informatie niet direct verwerkt kan worden, dient deze informatieoverdracht automatisch hersteld te worden nadat de keten hersteld is. Er mag geen informatie verloren gaan;
    g. Inschrijver verschaft over de uitvoering van de SLA en de resultaten periodiek een rapportage aan de gemeente, minimaal 1 maal per jaar;
11. De leverancier verzorgt een Nederlandse helpdesk, welke als ‘single point of contact’ dienstdoet voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen, alsook voor informatie over de afhandeling daarvan. De helpdesk is telefonisch bereikbaar van 8.00 uur tot 18.00 uur op werkdagen (maandag tot en met vrijdag met uitzondering van officiële feestdagen). Buiten deze tijden wordt een calamiteitenregeling door leverancier beschikbaar gesteld. In de SLA geeft leverancier de omgang, respons- en oplostijden aan voor aangemelde incidenten. Daarbij wordt tevens de calamiteitenregeling beschreven.
12. De helpdesk is ook beschikbaar via internet (webportaal of e-mail). Vragen, meldingen van incidenten en wijzigingsvoorstellen kunnen op alle dagen 24 uur per dag online worden ingediend (formulier). Dergelijke online vragen, meldingen van incidenten en wijzigingsvoorstellen worden automatisch per mail bevestigd en daarmee geregistreerd. Tevens kan de voortgang van deze incidenten en wijzigingsmeldingen digitaal worden geraadpleegd en gevolgd.

13. Er is een help-functie/kennisbank beschikbaar waarin o.a. handleidingen en gebruikersinstructies zijn opgenomen.
14. Door leverancier wordt voor de in gebruik name van de Oplossing een exitovereenkomst opgesteld, zoals benoemd in de GIBIT, 2020: artikel 22. Leverancier beschrijft hierbij de wijze waarop de gegevens terug beschikbaar worden gesteld aan de gemeente vanuit de gehele Oplossing, ontmanteling van de totale Oplossing (inclusief acceptatie hiervan) plaatsvindt, welke termijnen gelden gedurende deze exitprocedure en welke capaciteit en kosten hiermee gemoeid gaan. De kosten voor het opstellen van deze (concept)exitovereenkomst (inclusief exitplan) dienen in de Inschrijving opgenomen te zijn. De kosten voor uitvoering van de exitovereenkomst vallen buiten de Inschrijving. Leverancier garandeert dat er geen data achterblijft na acceptatie van de exitfase.

Beveiligings Eisen

15. De Oplossing functioneert, en blijft gedurende de gehele looptijd functioneren, op het gebied van beveiliging en privacy volledig conform alle betreffende wet- en regelgeving, ten minste AVG, BIO en andere van toepassing zijnde vereiste wetgeving. De Inschrijver garandeert bovendien de toekomstige (door)ontwikkeling (en onderhoudskosten) van de Oplossing gedurende de looptijd van de Overeenkomst binnen de jaarlijkse prijzen, zodanig dat de Oplossing 'meegroeit' met alle security-ontwikkelingen.
16. De leverancier werkt mee aan audits en pentesten op verzoek van Opdrachtgever (‘Right to audit’). Een dergelijke audit zal slechts plaatsvinden nadat door Inschrijver een auditplan is goedgekeurd. Compliancy kan tevens proactief door de Inschrijver met beveiligings- en auditrapportages van externe en onafhankelijke toetsende instanties worden aangetoond, bij voorkeur met een ISAE 3402 - type 2, ISO 27001 of een vergelijkbare variant hiervan.
17. Eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. dergelijke beveiligingstest/- audits dienen te worden weggenomen bij de volgende versie van de Oplossingen (als onderdeel van het onderhoud) en zo nodig op de kortst mogelijke termijn te worden gepatcht.
18. Na afhandeling van een zaak worden personen automatisch ontvolgt;
19. Een audittrail is per zaak aanwezig, met daarin alle doorlopen stappen in chronologische volgorde;
20. De Inschrijver dient jaarlijks een geldige TPM-verklaring ten aanzien van DigiD-beveiligingsaudit te overleggen. Alle activiteiten rondom het kunnen overleggen van een TPM-verklaring dienen in de Inschrijving opgenomen te zijn.
21. Voor de Oplossingen die ingezet worden om de vereiste en gewenste self-service aan burgers, organisaties en instellingen aan te bieden geldt dat de juiste beveiligingen en certificaten worden toegepast conform geldende wet- en regelgeving en algemeen geldende standaarden. De gemeente hanteert de volgende procedure: de gemeente is eigenaar van het (sub)domein. Inschrijver doet certificaat request aan de gemeente. De gemeente vraagt het certificaat aan waarna de Inschrijver het certificaat plaatst.
22. De Standaard Verwerkersovereenkomst Gemeenten van de Informatie Beveiligings Dienst (VNG Realisatie) is volledig van toepassing op de gehele Opdracht.