PSA Vervanging Datadistributiesysteem

Versie: 1.0 t.b.v. aanbesteding

Datum: 21-04-2026

Auteur: D&B/ICT/INFRA

1 Inhoud

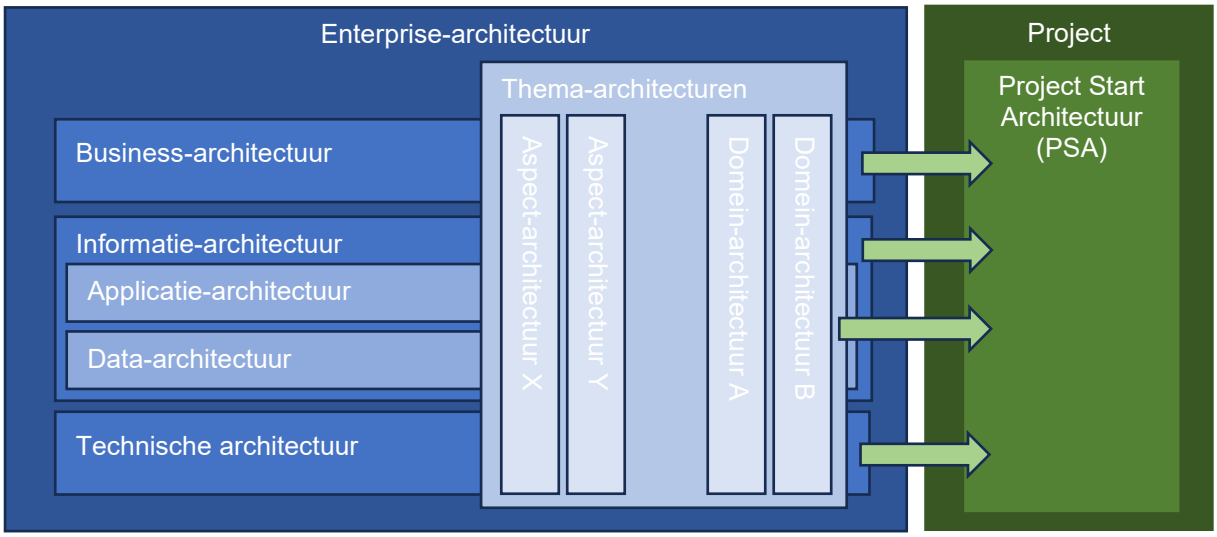
2 Inleiding

2.1 Doel, positie en opbouw PSA

Dit document beschrijft de **P**roject**S**tart**A**rchitectuur (PSA) voor de aanbesteding behorende bij het project Vervanging Datadistributiesysteem.

De PSA heeft als doel te waarborgen dat ontwikkelingen en veranderingen die in het project worden gerealiseerd passen binnen de toekomstig gewenste inrichting (op business-, applicatie-, en technisch niveau). De PSA vormt het architectuurraamwerk en toetsingskader voor het project (scope en oplossingsrichting), waarbinnen de oplossing kan worden ontworpen en gerealiseerd. De PSA is géén solution architectuur, technisch of functioneel ontwerp of een aanbestedingsbestek. Binnen het project zullen diverse detailontwerpen en architecturen worden gemaakt (bijvoorbeeld door de leverancier), binnen de kaders van deze PSA.

De PSA is een nadere uitwerking van hetgeen over de gewenste inrichting is beschreven in de Concern Informatie Architectuur (CIA) [bijlage 13], de Technische Architectuur (TA) [bijlage 12] en het beleid informatieveiligheid [bijlage 14] van de gemeente 's-Hertogenbosch. In onderstaande figuur is aangegeven hoe de verschillende architectuurproducten zich tot elkaar verhouden. De enterprise-architecturen zijn kaderstellend voor de PSA, architectuurkeuzes in de PSA kunnen leiden tot aanpassingen in de enterprise-architectuurproducten.



Figuur 1: De architectuurproducten

3 Projectcontext

Dit PSA-document heeft betrekking op het project Vervanging datadistributiesysteem en is van toepassing tijdens de volgende fases in het project: voorbereiding, aanbesteding en implementatie.

3.1 Aanleiding

Vanuit het managementteam kwam initieel de vraag om te kijken naar de toekomst van datadistributie/-notificatie/API's in relatie tot het huidige datadistributiesysteem Key2Datadistributie. Daarop zijn er in concept een tweetal architectuurplaten gemaakt met daarop de ist- en de soll-situatie en is er al een aantal sessies gepland met medewerkers van D&B/ICT/INFRA om dit onderwerp te bespreken. In dit document wordt dieper ingegaan op waar we als Gemeente 's-Hertogenbosch nu staan qua datadistributie/-notificatie/API's (hoe bevragen we op dit moment gegevens) en waar we naartoe moeten in de toekomst – en wat is daar dan voor nodig?

3.2 Doel, resultaat en drivers

Gegevensdistributie of datadistributie wil zeggen dat gegevens niet centraal worden opgeslagen, maar over meerdere plaatsen zijn verdeeld. Dit kan om verschillende redenen nuttig zijn, bijvoorbeeld om gegevens veilig te stellen, maar ook om de responstijden van lokale systemen te verkleinen. Alle systemen die van gedistribueerde gegevens gebruikmaken, hebben software die zorgt dat alle gegevens op alle locaties wordt gerepliceerd.
Persoonsgegevens, adressen, bedrijfsgegevens uit basisregistraties worden in taakapplicaties opgeslagen als onderdeel van een dossier of werkproces. Dit heeft altijd als doel gehad om met de applicaties snel en betrouwbaar te kunnen werken. Aan de andere kant wil de gemeente wel altijd met actuele gegevens werken en is dit vaak ook wettelijk verplicht. Dus moeten de gedistribueerde gegevens steeds direct worden bijgewerkt als de bronregistratie wijzigt. Tot op heden gebruikt gemeente ’s-Hertogenbosch hiervoor een specifieke applicatie die dit verzorgt op basis van de geldende landelijke StUF-standaarden. Dit is gebaseerd op SOAP en kenmerkt zich door berichtenverkeer in vraag-antwoord-vorm.
De afgelopen jaren is er door gemeenten gewerkt aan een nieuwe, modernere, standaard voor het distribueren van basisregistraties. Deze is nu landelijk overgenomen door de Rijksoverheid en wordt in stappen in gebruik genomen. Onder de naam HaalCentraal is er een reeks API’s (JSON-REST) ontwikkeld waarmee in de toekomst de basisregistraties ontsloten kunnen worden. Met HaalCentraal veranderen er in principe twee zaken fundamenteel ten opzichte van StUF:

1) Alle basisregistraties krijgen één landelijk API-endpoint waarop alle gegevens uit die registratie beschikbaar zijn. Dus geen lokale of hybride bronnen meer zoals nu het geval is.
2) Dataminimalisatie is leidend: met StUF kreeg je altijd een volledig antwoordbericht met alle beschikbare gegevens in ruwe vorm. De HaalCentraal-API’s zijn functioneel en geven alleen antwoord op de gestelde vraag. Op de vraag "Is deze persoon ouder dan 18 jaar?" komt alleen een ‘Ja’ of ‘Nee’ zonder de geboortedatum prijs te geven.

Dat vraagt ook om een verandering in de omgang van taakapplicaties met gegevens uit de basisregistraties. Zij moeten ook echt die functionele vraag gaan stellen en het antwoord direct gebruiken in plaats van de achterliggende gegevens gedistribueerd op te slaan. De werking van het stelsel van basisregistraties verandert dan van ‘datadistributie’ naar ‘bevragen bij de bron’. De Rijksoverheid noemt dit ook wel het Federatief Datastelsel (FDS).

Doelen

Nr	Omschrijving
1	Er moet snel en betrouwbaar gewerkt kunnen worden met applicaties en gegevens.
2	Er moet altijd met actuele gegevens gewerkt kunnen worden.
3	De gegevensuitwisseling moet tijdig en efficiënt uitgevoerd kunnen worden.
4	De modernste methodieken en standaarden op het gebied van datadistributie en -notificatie moeten gebruikt kunnen worden.
5	Dataminimalisatie moet zo ver als mogelijk doorgevoerd worden.
6	Open standaarden moeten ondersteund worden voor notificaties.
7	Privacy op data moet zo ver als mogelijk doorgevoerd worden.
8	De Generieke Digitale Infrastructuur en de ketenprocessen moeten ondersteund worden.
9	Alle communicatie moet gebaseerd zijn op open, door de overheid aangewezen standaarden.
10	Privacybescherming is standaard ingebouwd: dataminimalisatie, logging, scheiding van functies.
11	Beveiliging is integraal onderdeel van ontwerp en implementatie.
12	Gebruik bestaande voorzieningen (machtigingen, authenticatie, berichtenverkeer) waar mogelijk.

Doelen: wat moet het systeem bereiken

Nr	Omschrijving	Type D: distributie N: notificatie
1	Veilige en betrouwbare uitwisseling van gegevens.	D
2	Uniforme gegevenslevering op basis van open standaarden.	D
3	Ondersteuning van “eenmalige uitvraag, meervoudig gebruik”.	D
4	Aansluiting op de Generieke Digitale Infrastructuur (GDI).	D
5	Waarborgen van rechtmatige en proportionele gegevensverwerking.	D
6	Verbeteren van interoperabiliteit.	D
7	Verlagen van administratieve lasten.	D
8	Signaalgestuurde gegevensuitwisseling mogelijk maken.	N
9	Via Haal Centraal landelijk gegevens ophalen en volgen.	N
10	Het tijdig informeren over relevante gegevenswijzigingen.	N
11	Actualiteit en kwaliteit van gegevens in ketens verbeteren.	N
12	Minimaliseren van onnodige gegevensuitwisseling (alleen notificatie, geen data).	N
13	Bevorderen van interoperabiliteit via open notificatiestandaarden.	N
14	Ondersteunen van efficiënte ketenprocessen binnen de GDI.	N

Resultaten: wat het systeem concreet oplevert

Nr	Omschrijving	Type D: distributie N: notificatie
1	Een gestandaardiseerde API- of berichtenlaag voor gegevensuitgifte.	D
2	Betrouwbare, gecontroleerde en traceerbare datastromen.	D
3	Consistente gegevenskwaliteit door centrale of gecoördineerde distributie.	D
4	Vermindering van dubbele gegevensaanvragen.	D
5	Transparante logging en auditing voor toezicht en naleving.	D
6	Integratie met machtigingsvoorzieningen en erkende identificatiemiddelen.	D

8	Een betrouwbaar notificatiemechanisme dat wijzigingen direct doorgeeft.	N
9	Vermindering van polling, periodieke uitvragen en handmatige controles.	N
10	Actuele gegevens bij alle aangesloten afnemers.	N
11	Notificaties zonder persoonsgegevens (privacy-by-design).	N
12	Heldere statusinformatie over notificaties (afgeleverd, mislukt, opnieuw verzonden).	N
13	Betere synchronisatie tussen basisregistraties en afnemers dan bij distributie van gegevens.	N
14	Snellere doorlooptijden in ketenprocessen dan bij distributie van gegevens.	N

Drijfveren: waarom dit nodig is

Nr	Omschrijving	Type D: distributie N: notificatie
1	Verplichting tot gebruik van aangewezen open standaarden.	D
2	Eisen aan informatieveiligheid en betrouwbaarheid van digitale dienstverlening.	D
3	Noodzaak tot interoperabiliteit binnen de overheid en met Europa (eIDAS) – in de toekomst.	D
4	Verplichting tot veilige toegang via erkende identificatiemiddelen.	D
5	Toezicht- en verantwoordingsplichten voor gegevensverwerking.	D
6	Druk om administratieve lasten te verlagen en dienstverlening te verbeteren.	D
7	Behoefte aan uniforme digitale infrastructuur (GDI).	D
8	Eisen aan doelmatige en proportionele gegevensverwerking (dataminimalisatie).	N
9	Verplichting tot gebruik van open standaarden voor interoperabiliteit.	N
10	Noodzaak om gegevenskwaliteit en actualiteit te verbeteren.	N
11	Ondersteuning van veilige en betrouwbare digitale dienstverlening.	N
12	Druk om ketenprocessen te versnellen en foutkansen te verkleinen.	N
13	Behoefte aan transparantie en controleerbaarheid van gegevensstromen.	N
14	Aansluiting op Europese ontwikkelingen richting event-driven overheid.	N

3.3 Gerelateerde projecten en afhankelijkheden

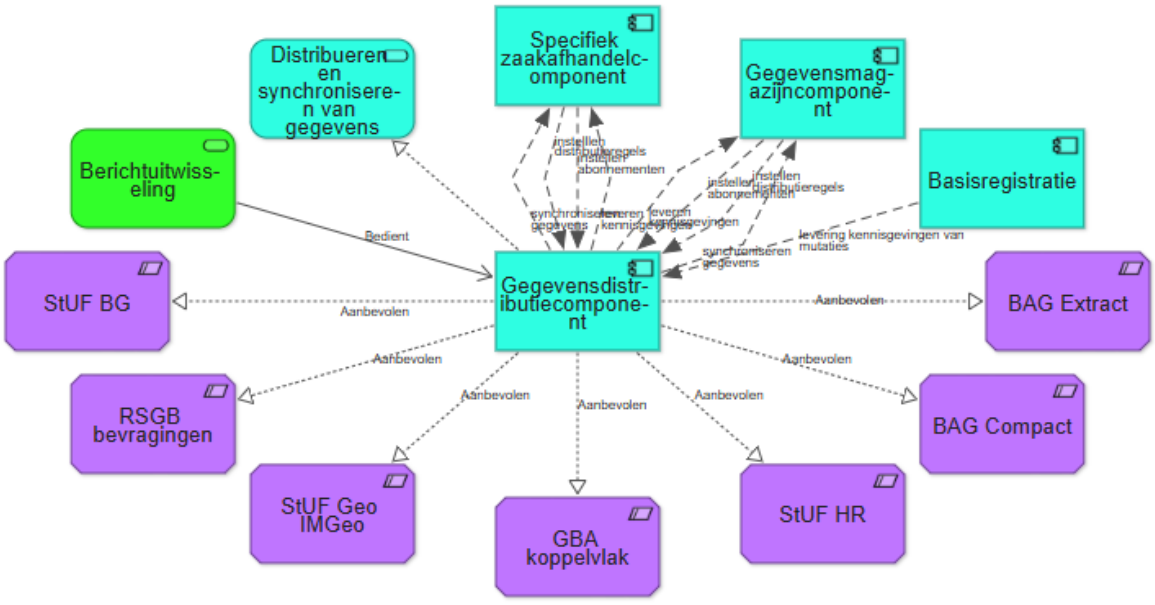
Nr	Omschrijving	Datum	Type
1	Uitfasering VOA-mailbox	31-12-2027	Functioneel, Technisch
2	Overgang van administratieve verwerking Wet APPA (Wet Algemene Pensioen- en uitkeringswet Politieke Ambtsdragers) van gemeenten (nu semi-automatische koppeling in huidige datadistributiesysteem) naar ABP	01-01-2028 (voorlopig)	Functioneel, Technisch

4 Grondslagen

In deze PSA worden er twee complementaire voorzieningen beschreven: het datadistributiesysteem (DDS) en het datanotificatiesysteem (DNS). Deze voorzieningen zijn ontworpen in overeenstemming met de Wet digitale overheid (Wdo) en sluiten aan op de Generieke Digitale Infrastructuur (GDI).
Het datadistributiesysteem verzorgt de veilige, betrouwbare en uniforme uitgifte van gegevens aan afnemers. Het systeem maakt gebruik van open standaarden (voor een overzicht zie hieronder), ondersteunt eenmalige uitvraag en meervoudig gebruik en voldoet aan de eisen van privacy- en security-by-design. Autorisatie en identificatie verlopen via erkende GDI-voorzieningen. Het datadistributiesysteem biedt volledige logging, auditing en controleerbaarheid van datastromen of is gekoppeld aan een systeem die deze functionaliteiten biedt.

Het datanotificatiesysteem verzorgt de signaalgestuurde notificatie van gegevenswijzigingen. Notificaties bevatten geen persoonsgegevens en zijn gebaseerd op open notificatiestandaarden. Het datanotificatiesysteem verhoogt de actualiteit van gegevens bij afnemers en vermindert onnodige dataverwerking door polling te vervangen door gebeurtenisgedreven communicatie. Het datanotificatiesysteem is schaalbaar, betrouwbaar en ondersteunt herlevering en foutafhandeling.
Beide systemen zijn ontworpen volgens de overheidsbrede architectuurprincipes: hergebruik boven maatwerk, interoperabiliteit binnen ketens, transparantie, controleerbaarheid en strikte scheiding tussen signalering (datanotificatiesysteem) en gegevenslevering (datadistributiesysteem). Deze architectuur borgt naleving van onderstaande wetgeving en ondersteunt een efficiënte, veilige en toekomstbestendige digitale overheid.

De paarse objecten in onderstaande figuur geven aan welke standaarden moeten worden ondersteund.



De volgende kaders zijn van belang als persoonsgegevens worden gebruikt:

1) In het algemeen voldoen aan de AVG, Uitvoeringswet AVG, Wet BRP en de Wet politiegegevens (Wpg)
    1) Algemeen Privacybeleid - https://zoek.officielebekendmakingen.nl/gmb-2019-113644.html
    Het beleid geeft aan waar gemeente 's-Hertogenbosch zich aan heeft te houden. Het geeft een duidelijke richting aan privacy en laat zien dat de gemeente de privacy van haar inwoners waarborgt, beschermt en handhaaft.

2) Algemeen Privacyreglement AVG - https://zoek.officielebekendmakingen.nl/gmb-2019-114571.html
   Het reglement geeft verdere invulling van het beleid. Hier kunt u meer specifiek vinden hoe de gemeente ’s-Hertogenbosch omgaat met uw persoonsgegevens.

Naast de bestaande architecturen en visies moet de architectuur van dit platform ook de volgende wetten/regelingen ondersteunen:

1) Wet digitale overheid
2) Stelsel van Basisregistraties
3) Wet AVG Algemene Verordening Gegevensbescherming
4) Baseline Informatiebeveiliging Overheid 2 BIO2

5 Principes

Onderstaande principes en uitspraken zijn relevant voor dit project:

Business	
Principe	**Consequenties voor het project**
We volgen de Sourcing Strategie	Ondanks dat het notificeren van gebeurtenissen – een functioneel onderdeel in dit project - nu nog de kenmerken heeft van een innovatief product, beschouwen wij het als een System of Record. Dat wil zeggen dat wij ons conformeren aan de componenten die beschikbaar zijn en de processen die worden ondersteund. Indien er voor bepaalde gewenste functionaliteit geen geschikte software beschikbaar is, laten we die alleen ontwikkelen in samenwerking met andere gemeentes.

Informatie	
Principe	**Consequenties voor het project**
We gaan uit van generieke processen, functies en applicaties	De te verwerken gegevens betreffende gestandaardiseerde basisregistraties. We gaan er dus vanuit dat de applicatie ook gestandaardiseerde verwerking biedt van deze gegevens middels standaard processen en functies.
We hebben grip op onze applicaties, ook wanneer deze uitbesteed zijn	Functioneel: goede en duidelijke afspraken maken met de betrokken leverancier in de vorm van een SLA, auditing en daarop monitoren om de regierol te behouden. Technisch: de API-gateway is technisch gezien het middel om grip te houden op applicaties en koppelingen.
We gaan voor optimaal (her)gebruik van gegevens	We beschouwen het datadistributiesysteem als een technische oplossing om logisch hergebruik van basisgegevens te organiseren.
We zorgen ervoor dat onze informatie betrouwbaar, beschikbaar en veilig is	Informatie – in dit geval gegevens/data die op een bepaalde manier verzonden, ontvangen en eventueel opgeslagen wordt - moet aan de in de elders genoemde documentatie standaarden en eisen voldoen. Daarnaast hebben we een consistentie- en kwaliteitscontrolesysteem (KMGB) die de consistentie en kwaliteit van de data monitort.
We wisselen informatie uit via (overheids)standaarden	Datadistributie en -notificatie doen we alleen conform standaarden: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

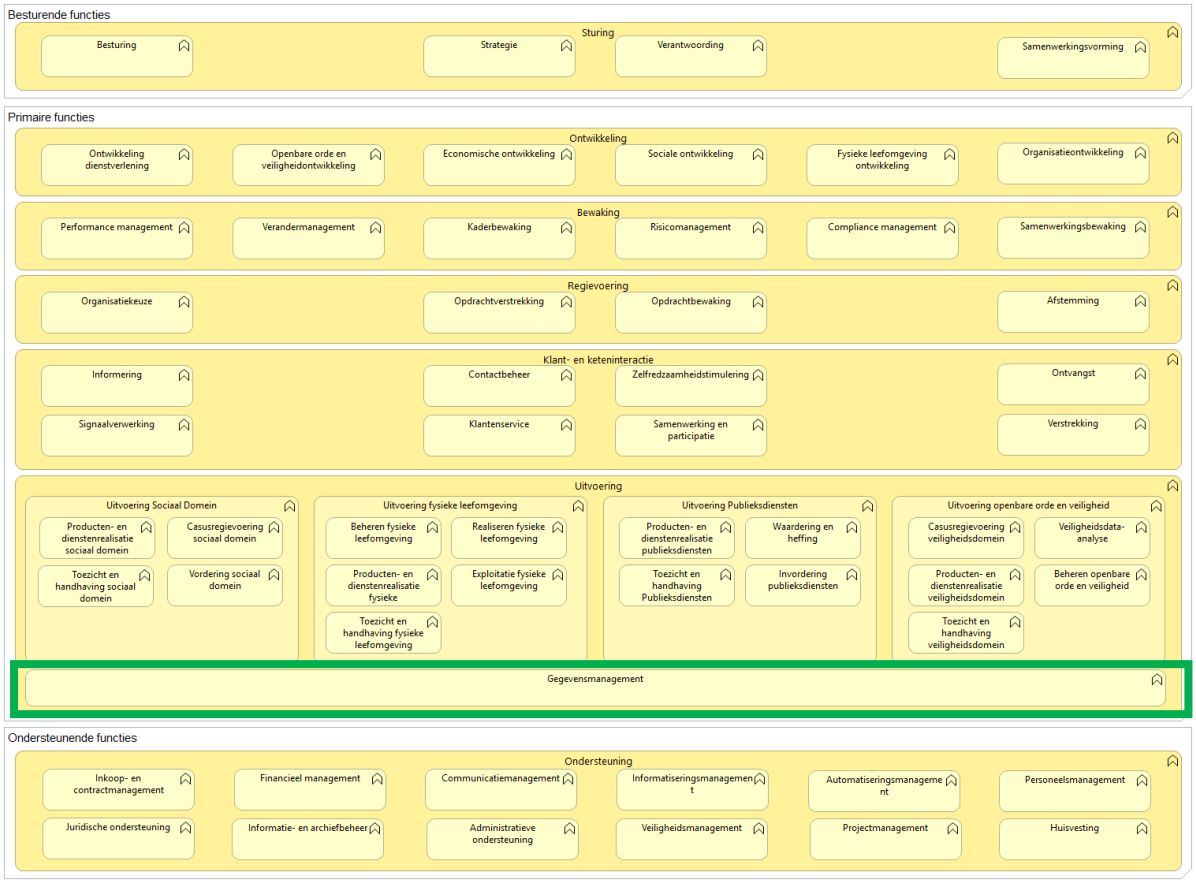
Wij gebruiken gecontroleerde gegevenssynchronisatie voor kopieën van basis- en kernregistraties	Bij gebruik van een kopie van basis- of kerngegevens voor processen waarin deze actueel moeten zijn, zijn gegevenssynchronisatie, monitoring van de gegevensstroom en periodieke consistentie- en kwaliteitscontroles verplicht. Basis- en kerngegevens worden direct bij de bron geraadpleegd. Alleen als dit niet mogelijk is wordt een kopie gemaakt. Als het voor de dienstverlening aan onze burgers en bedrijven noodzakelijk is dat deze kopieën van basis- of kernregistraties actueel blijven, dan is synchronisatie van deze kopieën met hun bronnen verplicht. Deze (synchronisatie)koppelingen worden actief gecontroleerd op een juiste en volledige werking. De kwaliteit en consistentie van de synchronisatie wordt daarnaast periodiek gecontroleerd, door middel van een volledige vergelijking van de kopie met de bron. Indien leveranciers zelf niet over afdoende controlemiddelen beschikken, vindt de controle via de gemeentelijke kwaliteitsmonitor plaats.

Technologie	
Principe	**Consequenties voor het project**
We hebben een beheersbare ICT-infrastructuur	Er wordt een oplossing geleverd die bijdraagt aan een stabiele, schaalbare en beheersbare ICT-infrastructuur. Standaarden worden gehanteerd, complexiteit beperkt en er wordt gezorgd dat beheerprocessen efficiënt kunnen worden uitgevoerd. Dit alles moet passen binnen de bestaande beheerorganisatie en lifecycle-afspraken. Het hele proces van datadistributie moet vanuit één systeem eenvoudig beheerd en gecontroleerd kunnen worden.
We hebben zicht en grip op de informatieuitwisseling tussen systemen	Alle koppelingen tussen het datadistributiesysteem en de andere applicaties lopen via de API-gateway van de gemeente.
Onze systemen zijn integer	Alle handelingen die in het datadistributie- en -notificatiesysteem worden uitgevoerd, worden gelogd.
We hebben regie over de koppelingen tussen onze applicaties	Koppelingen tussen het datadistributie- en notificatiesysteem en andere systemen worden gelegd, onderhouden en gemonitord door de gemeente.
Mensen kunnen plaats- en tijdonafhankelijk werken met onze systemen	De oplossing kan worden beheerd vanaf ieder door de gemeente beschikbaar gestelde managed device volgens de beveiligingseisen van de gemeente.

Onze systemen zijn gebruiksvriendelijk	De leverancier levert een applicatie die een begrijpbare, logisch opgebouwde gebruikersinterface heeft en waarbij de taal in het Nederlands of Engels is.

6 Businessarchitectuur

In dit hoofdstuk wordt ingegaan op de businessarchitectuur in termen van bedrijfsfuncties, producten en diensten, kanalen, actoren, bedrijfsprocessen en bedrijfsobjecten. Dit blijft beperkt tot de onderdelen die relevant zijn binnen de projectcontext. Enerzijds geeft dit zicht op de scope van het project (wat wordt ‘geraakt’?), anderzijds geeft het zicht op de gewenste verandering binnen die scope (wat gaan we wijzigen?).
Op businessniveau vinden er geen wijzigingen plaats in dit project. Onderstaande afbeelding geeft aan waar in het functielandschap het datadistributiesysteem zich bevindt (groen omkaderd).

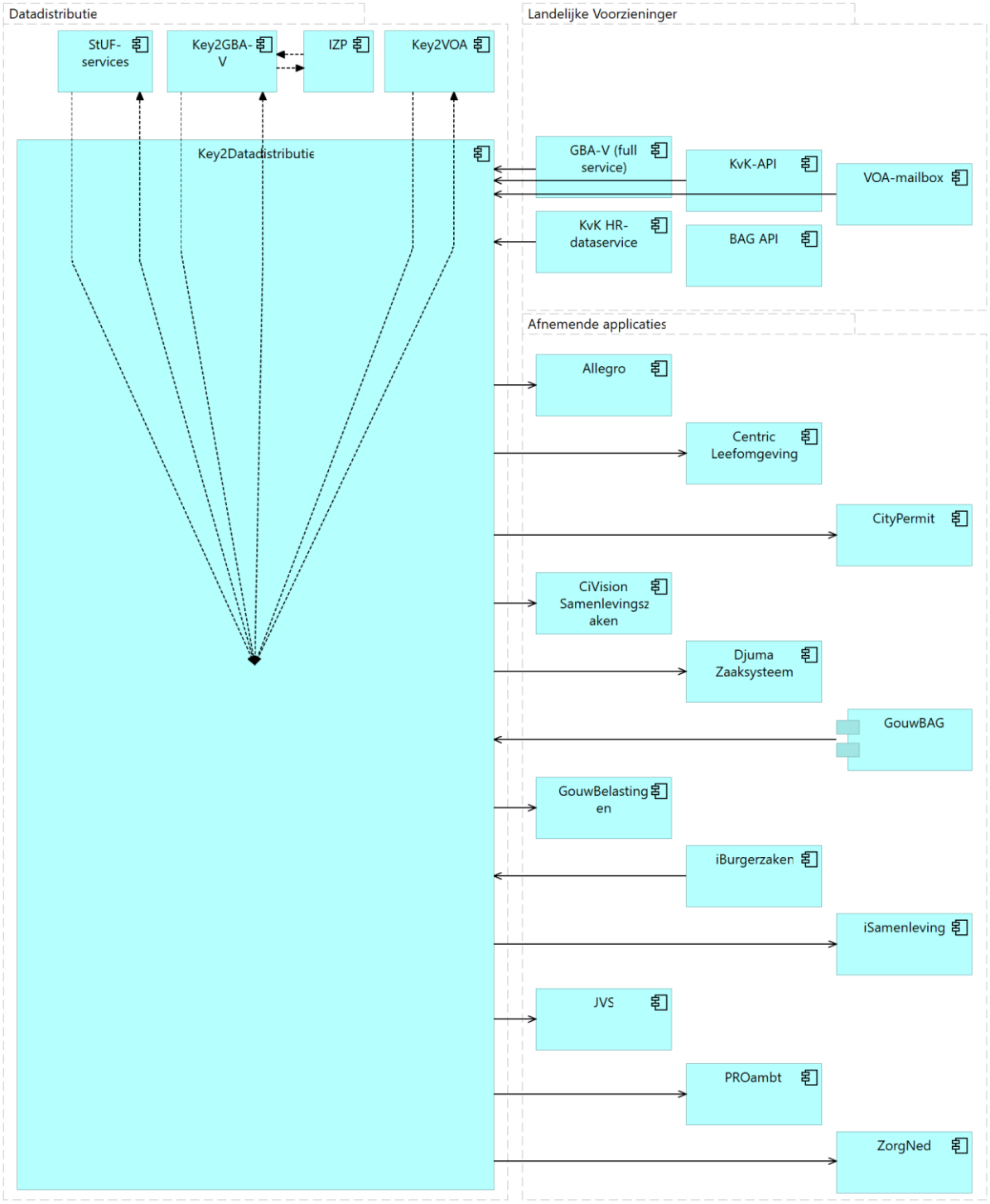


7 Informatie-architectuur

In dit hoofdstuk wordt ingegaan op de informatie-architectuur in termen van applicaties, gegevens en integratie. Dit blijft beperkt tot de onderdelen die relevant zijn binnen de projectcontext. Enerzijds geeft dit zicht op de scope van het project (wat wordt 'geraakt'?), anderzijds geeft het zicht op de gewenste verandering binnen die scope (wat gaan we wijzigen).

7.1 Applicaties

Applicaties: huidige situatie op basis van architectuur



Applicaties (gekoppeld met het datadistributiesysteem via de API-gateway)

Applicatienaam	Leverancier	Type koppeling	Gegevens	Basis-registratie-applicatie?	Verzenden/ Ontvangen gegevens
Allegro	Kred'IT	StUF3	BRP	Nee	O
Centric Leefomgeving	Centric	StUF3	BRP, NHR, *BAG (LV)**	Nee	O
CityPermit	Sigmax	StUF3	BRP	Nee	O
Civision Samenlevingszaken	PinkRoccade	StUF3	BRP	Nee	O
Djuma	Visma Circle	StUF3	BRP, BAG (lokaal)	Nee	O
Gouw BAG	GouwIT	StUF3	BAG	Ja	V
Gouw Belastingen	GouwIT	StUF3	BRP, *NHR (LV)**	Nee	O
iBurgerzaken	PinkRoccade	StUF3	BRP *BAG (LV)**	Ja	V
iSamenlevingszaken	PinkRoccade	StUF3	BRP	Nee	O
Jeugdvolgsysteem	MetaObjects	StUF3	BRP	Nee	O
Wet Algemene Pensioen- en uitkeringswet Politieke Ambtsdragers	Intern (technisch), ProAmbt (administratief)	Overzicht	BRP	Nee	O
ZorgNed	ZorgNed	StUF3	BRP	Nee	O

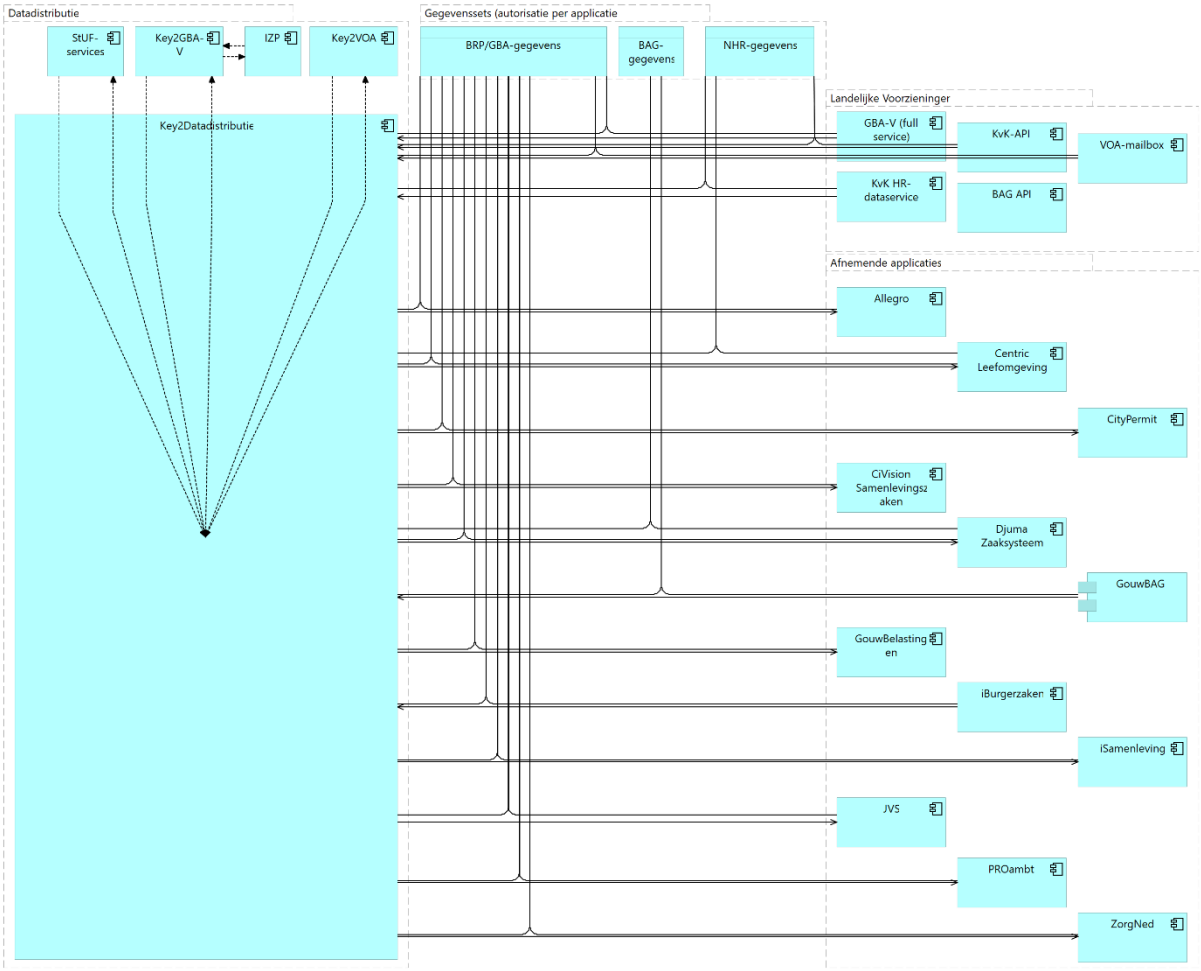
* Koppeling via applicatie zelf naar landelijke voorziening, niet via Key2Datadistributie

Koppelservices (via API-gateway) met landelijke basisregistraties

Servicenaam	Leverancier	Type koppeling	Gegevens-eigenaar	Gegevens
GBA-V (Key2GBA-V)	Centric	StUF (GBA)	RVIG	BRP
VOA (Key2VOA)	Centric	StUF (GBA)	RVIG	BRP
KvK zoeken (API)	Kamer van Koophandel	API	Kamer van Koophandel	NHR
KvK basisprofiel (API)	Kamer van Koophandel	API	Kamer van Koophandel	NHR
NHR-mutatieservice (via Key2Datadistributie)	Centric	API, StUF	Kamer van Koophandel	NHR

7.2 Gegevens

Gegevens: gekoppelde applicaties met specifieke gegevenssets uit basisregistraties

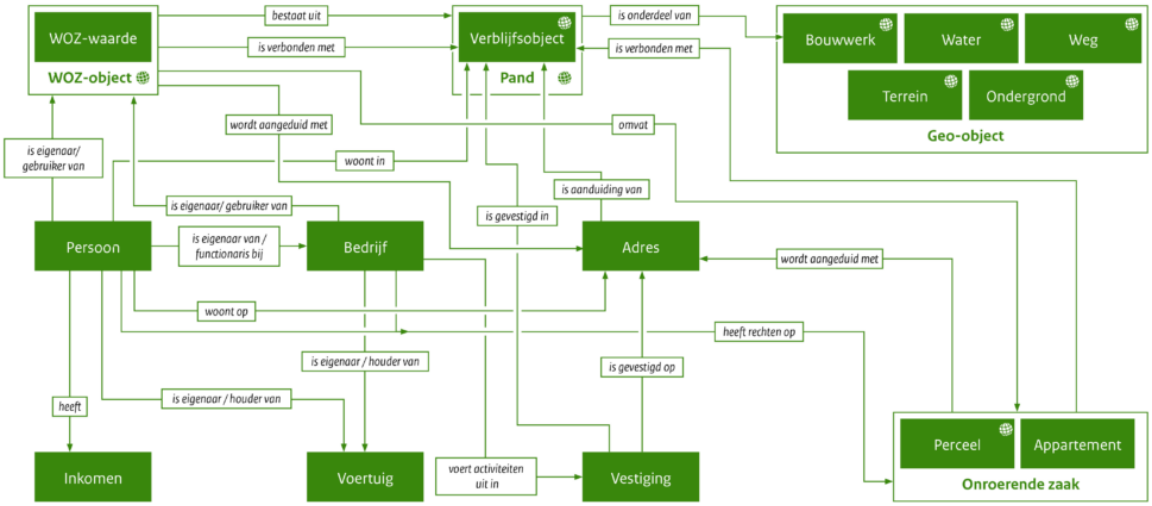


Met betrekking tot dit project zijn er qua gegevenssets de gegevens uit drie van de tien basisregistraties relevant: Basisregistratie Personen (BRP, personen), Basisregistratie Adressen en Gebouwen (BAG, adressen) en het Nieuw HandelsRegister (NHR, bedrijven); in het huidige datadistributiesysteem worden er gegevenssets uit deze basisregistraties verzonden, ontvangen en opgeslagen. De andere zeven basisregistraties zijn in de scope met betrekking tot datadistributie niet meegenomen; voor wat betreft het datanotificatiegedeelte wordt niet uitgesloten dat er voor elke basisregistratie één of meerdere koppelingen worden gerealiseerd, daarom worden ze hieronder wel (indirect) genoemd omdat er in de toekomst wel mee gekoppeld gaat worden via API's. De specificaties van deze API's hangt af van wat er vanuit de eigenaars van de betreffende basisregistraties aan gegevens verstrekt gaat worden, dat is op dit moment nog onbekend.

Basisregistraties

Algemeen:

- Overzicht:
- https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/10-basisregistraties/
- Stelselplaten:
- https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/stelselplaat/



- Basisregistratie Personen (BRP): Logisch Ontwerp – hoofdstuk 4:
- https://www.rvig.nl/lo-brp2026
- https://www.rvig.nl/sites/default/files/20261/Logisch%20Ontwerp%20BRP%202026.Q1%20adoc.pdf

- Basisregistratie Adressen en Gebouwen (BAG): Catalogus – hoofdstuk 6 en 7:
- https://www.geobasisregistraties.nl/site/binaries/sitecontent/collections/documents/2018/03/12/catalogus-2018/Catalogus-BAG-2018.pdf
- https://imbag.github.io/catalogus/

- Nieuw HandelsRegister (NHR): gegevenscatalogus Dataservice
- https://production-site-nl.kvk.bloomreach.cloud/binaries/content/assets/kvkwebsite-nl/categorie/producten-bestellen/gegevens-catalogus-volledig.pdf
- https://production-site-nl.kvk.bloomreach.cloud/binaries/content/assets/kvkwebsite-nl/categorie/producten-bestellen/gegevenscatalogus.pdf

- Basisregistratie Personen (BRP) Persoon, Historie, Bewoning, Reisdocumenten, Tabellen, Berichten en Gebeurtenissen API
- Basisregistratie Adressen en Gebouwen (BAG) Individuele bevragingen API
- Nieuw HandelsRegister-mutatieservice (NHR)
- Kamer van Koophandel-API's (KVK)
- Basisregistratie Kadaster (BRK) Bevragen API
- Waardering Onroerende Zaken (WOZ) Bevragen API

Standaarden

StUF:

- https://www.forumstandaardisatie.nl/open-standaarden/stuf
- https://www.gemmaonline.nl/wiki/StUF-standaarden
- https://standaarden.vng.nl/StUF-standaarden

API's:

- https://www.gemmaonline.nl/wiki/API-standaarden
- https://standaarden.vng.nl/API-standaarden

7.3 Gegevensuitwisseling en integratie

Gegevensuitwisseling vindt plaats op basis van twee methodieken:

1) de StUF-standaard (Standaard UitwisselingsFormaat). Dit is een set basisafspraken over het uitwisselen van gegevens tussen applicaties in het gemeentelijke veld. StUF beschrijft de generieke toepassing van die berichten, niet de specifieke gegevens erin. Als overheidsorganisaties basisregistraties (informatie over personen, adressen of bijvoorbeeld gebouwen) uitwisselen, doen ze dat via standaarden die gebaseerd zijn op StUF. StUF zelf is weer gebaseerd op XML.
2) de API-standaard. Een Application Programming Interface (API) is een manier om twee of meer computerprogramma's met elkaar te laten communiceren. Het is een soort software-interface die een dienst aanbiedt aan andere stukjes software. De API's werken volgens de REST-architectuurstijl en volgen de REST-API Design Rules standaard.

StUF-standaard

Een overzicht van alle gegevens op basis van de StUF-standaard die naar afnemende applicaties wordt gestuurd en ontvangen wordt vanuit applicaties die basisregistraties zijn (naamgeving kan per leverancier verschillen) is in een separaat document [bijlage 11a] bijgevoegd.

API-standaard

De uitgangssituatie voor wat betreft de API-standaard qua gegevens is deels nog onbekend/in ontwikkeling, ook omdat er in de toekomst volop nieuwe API's ontwikkeld zullen gaan worden. Voor de volgende API's zijn de gegevenssets al wel bekend:

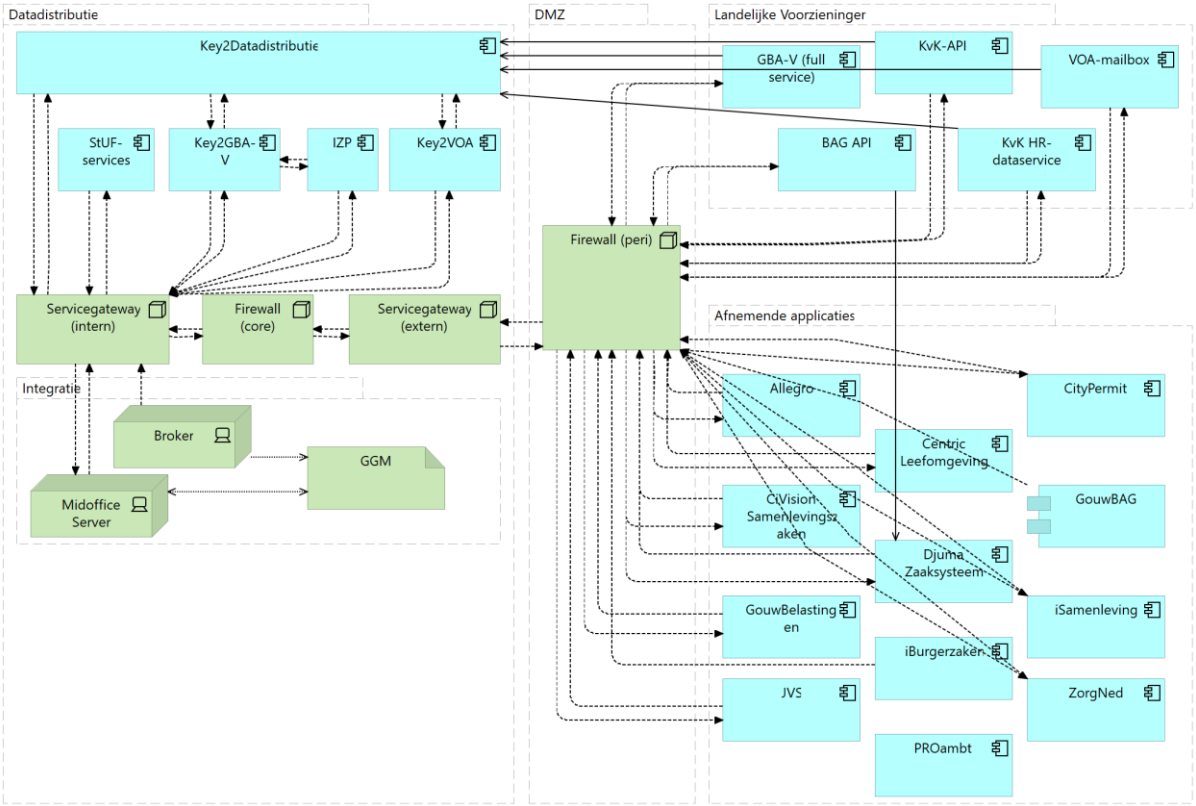
Basis-registratie	API-naam	Specificaties
BRP	Personen	https://developer.rvig.nl/brp-api/
BRP	Bewoning	https://developer.rvig.nl/brp-api/
BRP	Verblijfplaatshistorie	https://developer.rvig.nl/brp-api/
BRP	Reisdocumenten	https://brp-api.github.io/Haal-Centraal-Reisdocumenten-bevragen/
BRP	Tabellen	https://brp-api.github.io/Haal-Centraal-BRP-tabellen-bevragen/
BRP	Berichten	https://github.com/rvig-brp/BRP-Berichten-API
BRP	Gebeurtenissen	https://github.com/BRP-API/brp-api-gebeurtenissen
BAG	Individuele Bevragingen	https://lvbag.github.io/BAG-Gemeentelijke-wensen-tav-BAG-Bevragingen/
NHR	Zoeken	https://developers.kvk.nl/nl/documentation/zoeken-api
NHR	Basisprofiel	https://developers.kvk.nl/nl/documentation/basisprofiel-api
NHR	Vestigingsprofiel	https://developers.kvk.nl/nl/documentation/vestigingsprofiel-api
NHR	Naamgeving	https://developers.kvk.nl/nl/documentation/naamgeving-api

NHR	Nieuw Handelsregister-mutatieservice	https://developers.kvk.nl/nl/documentation/mutatieservice-api
BRK	Bevragen	https://kadaster.github.io/BRK-bevragen/
WOZ	Bevragen	https://kadaster.github.io/WOZ-bevragen/

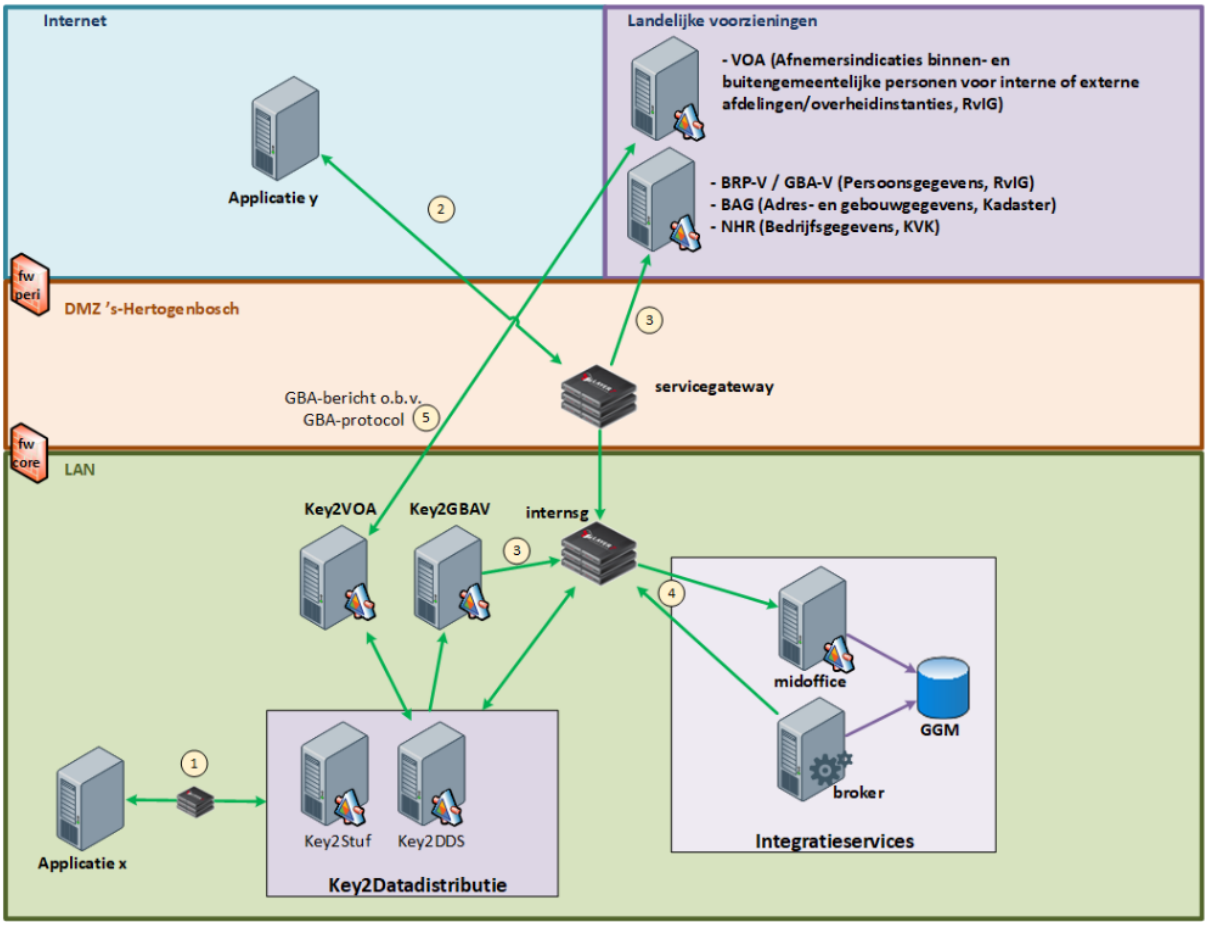
8 Technische architectuur

In dit hoofdstuk wordt ingegaan op de technische architectuur in termen van technische componenten, gegevensopslag en communicatienetwerken. Dit blijft beperkt tot de onderdelen die relevant zijn binnen de projectcontext. Enerzijds geeft dit zicht op de scope van het project (wat wordt ‘geraakt’?), anderzijds geeft het zicht op de gewenste verandering binnen die scope (wat gaan we wijzigen).

Huidige situatie architectuur



Huidige situatie techniek



1. Interne applicaties die aangesloten zijn op Key2Datadistributie
2. Externe applicaties die aangesloten zijn op Key2Datadistributie
3. Zoekvragen op personen die niet voorkomen in Key2Datadistributie worden via Key2GBAV- services opgehaald bij de Landelijke Voorziening GBA-V.
4. De integratieservices buffert afnemersindicaties en kennisgevingsberichten om deze asynchroon af te leveren. Tevens bevat het GGM een databuffer voor personen uit Key2datadistributie, die 24/7 beschikbaar is. Deze buffer voorziet SaaS-applicaties van persoonsgegevens.
5. Het Verzend- en Ontvangststation voor Afnemers (afkorting: VOA, applicatie: Key2VOA, gegevenseigenaar: RvIG) maakt het mogelijk om persoonsgerelateerde berichten uit te wisselen met de BRP-mailboxserver; dit gebeurt op landelijk niveau tussen gemeenten en andere overheidsorganisaties zoals bijvoorbeeld de Belastingdienst of DUO zodat deze organisaties personen van de gemeente 's-Hertogenbosch kunnen volgen. Daarnaast kunnen interne afnemende applicaties die in het kader van een wettelijke taak buitengemeentelijke personen moeten volgen dit op deze manier doen. Afnemersindicaties op binnengemeentelijke en buiten-gemeentelijke personen worden door de applicatie Key2VOA verzonden en ontvangen via een aparte koppeling op basis van het GBA-protocol (voorloper van StUF). Ondanks dat deze applicatie losstaat van het datadistributiesysteem, is deze applicatie en koppeling in de keten wel expliciet nodig. In 2026 wordt de techniek achter de VOA door RvIG vervangen voor een API.

Componenten

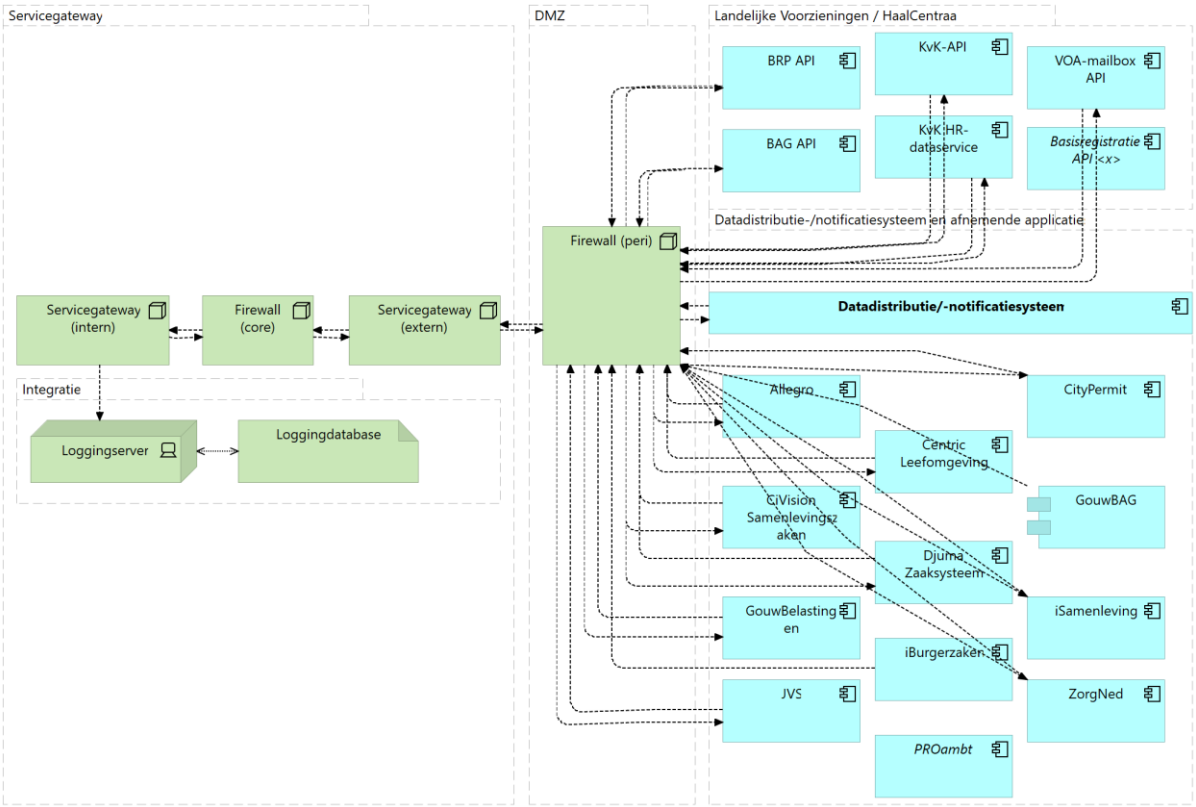
Om een goedwerkend en sluitend systeem te hebben met betrekking tot het distribueren of notificeren van gegevens(sets) zijn de volgende technische componenten benodigd:
1. bij het distribueren:
   - een datadistributiesysteem om de gegevens(sets) te verzenden, te ontvangen, te monitoren en te loggen met daarbij een autorisatiemodule en authenticatiemodule.
   - een API-gateway om de gegevens(sets) te verzenden, te ontvangen, te monitoren en te loggen
   - een broker om de gegevens(sets) te verzenden, te ontvangen, te monitoren en te loggen (in bulk)
   - één of meerdere services om het uitwisselen van gegevens(sets) via de koppeling in gang te zetten
   - een koppeling met landelijke voorzieningen om gegevens(sets) te kunnen controleren, te verzenden, op te halen of te ontvangen
   - een of meer applicaties die geautoriseerd zijn om gegevens(sets) te mogen ontvangen
   - een kwaliteitsmonitor (losstaand van het distributiesysteem) die controleert op consistentie tussen twee (of meer) systemen onderling en inhoudelijke kwaliteit.
2. bij het notificeren:
   - een datanotificatiesysteem om notificaties functioneel over gegevens(sets) te verzenden, te ontvangen en te monitoren en te loggen en – waar nodig – gegevens(sets) te verzenden en te ontvangen (deels distributie)
   - een API-gateway om notificaties over gegevens(sets) te verzenden, te ontvangen en te monitoren
   - een broker om notificaties over gegevens(sets) te verzenden, te ontvangen en te monitoren (in bulk)
   - een loggingsysteem waarin eenduidig de logging wordt opgeslagen – inclusief de benodigde metadata waaronder de bron, vertrouwelijkheid, bewaartermijn, etc.
   - één of meerdere services en/of API's om gegevens(sets) te kunnen bevragen
   - een koppeling met landelijke voorzieningen om gegevens(sets) te kunnen controleren, naar te verzenden, op te halen en/of te ontvangen
   - een of meer applicaties die geautoriseerd zijn om (notificaties over) gegevens(sets) te mogen ontvangen.

De distributie of notificatie gebeurt op een synchrone of asynchrone manier.

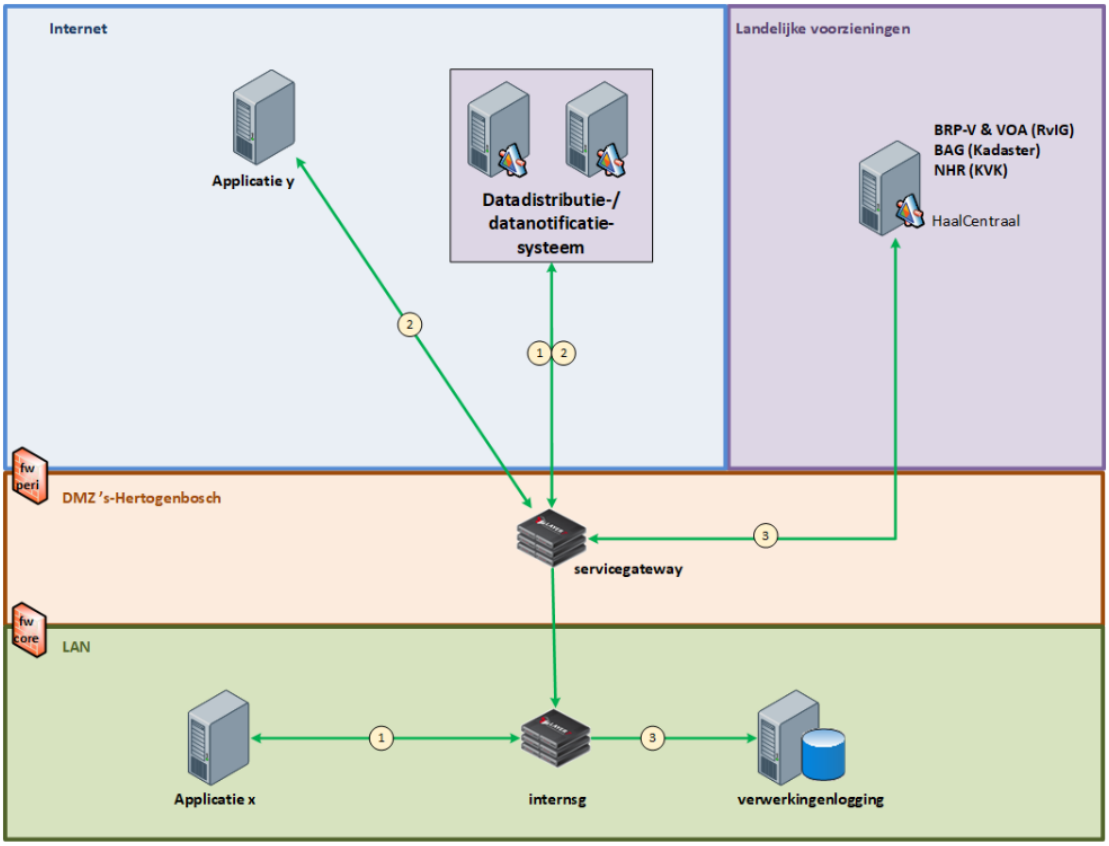
Componenten gerelateerd aan het datadistributiesysteem

Decomponenten BI-tooling en prefilling zijn niet rechtstreeks zoals een applicatie aan het datadistributiesysteem gekoppeld – en daarom niet specifiek in de scope van dit project meegenomen - maar het is er wel degelijk aan gerelateerd op basis van data: er worden periodiek (dagelijks, wekelijks, maandelijks, jaarlijks) voor BI-tooling en prefilling-doeleinden dumps klaargezet. Om de twee uur wordt er een (vereenvoudigde) kopie van de datadistributie-database geëxporteerd naar de database van het gemeentelijk gegevensmagazijn (GGM), wat weer als bron dient voor BI-tooling en prefillingdoeleinden zoals BRP- (persoons-) en BAG- (adres-) gegevens voor webformulieren, Klantbeelden via Cognos (ook in relatie tot het gegevenszakenmagazijn (GZM)) en de afdeling SO/SB gebruikt de gegevens uit het gemeentelijk gegevensmagazijn (GGM) die op kaarten weergegeven kunnen worden. De tijd en kosten om dit allemaal om te zetten moet wel ingecalculeerd worden binnen het project.

Gewenste situatie architectuur



Gewenste situatie techniek



In de SOLL-situatie zijn de afnemerindicaties en kennisgevingen ook centraal geregeld in HaalCentraal. Het datadistributiesysteem is alleen nog nodig voor de autorisatie van applicaties en het eventueel nog vertalen van de oude StUF-standaard naar HaalCentraal APIs.

1) Interne applicaties communiceren via de API-gateways met het datadistributiesysteem
2) Externe applicaties communiceren via de externe API-gateway met het datadistributiesysteem
3) HaalCentraal is met API-verkeer te benaderen en heeft volledige afnemerindicatie en kennisgeving functionaliteit. Het vereiste loggingcomponent volgens Common Ground is in deze situatie intern gerealiseerd.

Hetgeen waarmee gekoppeld is zijn basisregistraties en landelijke voorzieningen – een basisregistratie is een landelijke voorziening, maar een landelijke voorziening hoeft geen basisregistratie te zijn, bijvoorbeeld de koppeling met de VOA.

Continuïteit (betrouwbaarheid en updates), schaalbaarheid, stabiliteit, veiligheid, performance, beheer(s)baarheid

Het systeem moet voldoen aan de Technische Architectuur (TA), Concern Informatie Architectuur (CIA) en het beveiligingsbeleid met daarbij de randvoorwaarde dat het systeem 24x7 operationeel moet zijn (in lijn met het beleid rondom de API-gateway).

Datakwaliteit

Om de datakwaliteit te garanderen, moet er een kwaliteitsmonitor worden ingericht (los van de datadistributie/-notificatieomgeving). Deze monitor controleert op consistentie tussen twee (of meer) systemen onderling en inhoudelijke kwaliteit, bijvoorbeeld: dubbele waarden, extreme waarden, incomplete waarden, unieke waarden in relatie tot sleutels, recente/actuele waarden (al dan niet in combinatie met processen), registratie (in zijn algemeenheid) van waarden. Daarbij moet de data afstammen van een betrouwbare gegevensbron – een basisregistratie, een kernregistratie of een gegevensbron waarbij geverifieerd is dat dit een betrouwbare gegevensbron is. Deze kwaliteitsmonitor moet aan alle technische eisen voldoen die beschreven staan in de technische architectuur. Om deze kwaliteitscontrole uit te kunnen voeren moet er altijd toegang tot de data zijn – on premises of via een beveiligde verbinding bij SaaS of aanverwante as a service-vormen. Eigenschappen van datakwaliteit:

Eigenschap	Beschrijving
Volledigheid	De data moet volledig zijn. Dit houdt in dat alle verplichte velden in de tabellen van de database gevuld zijn.
Juistheid	Het is mogelijk dat tijdens verwerking van de gegevens bepaalde gegevens niet op de juiste manier zijn ingevuld in de velden in de tabellen van de database of dat de data verminkt wordt door het verkeerd lopen van ETL-processen. Het is van belang dat de data goed te controleren is op de juistheid.
Betrouwbaar	Data moet afstammen van een betrouwbare bron.
Consistent	Consistentiecontroles uitvoeren om de data vergelijken met de brondata.
Datastroom	Goed in beeld hebben hoe de datastroom verloopt.
Controle	Monitoren van de kwaliteit en de consistentie van de data m.b.v. een dashboard, bijvoorbeeld de KMGB van Synaxion.

9 Beveiliging en privacy

De Oplossing moet voldoen aan kaders voor informatiebeveiliging en privacy. In deze paragraaf zijn de kaders zoals van toepassing samengevat.

Informatieveiligheid
De strategische uitgangspunten vormen de basis, die wordt gebruikt voor de vertaling van de Baseline Informatiebeveiliging Nederlandse Overheid (BIO) naar de kernpunten van het Beleid Informatieveiligheid van de gemeente 's-Hertogenbosch [3], paragraaf 1.3]. De BIO wordt opgevolgd door BIO2 welke inmiddels vastgesteld is. De gemeente 's-Hertogenbosch heeft geen architectuurprincipes gedefinieerd specifiek voor informatiebeveiliging. In deze paragraaf zijn informatiebeveiligingseisen in scope van het project samengevat. Deze zijn geordend vanuit beschikbaarheid, integriteit en vertrouwelijkheid (BIV, zie ook BIO2, maatregel 5.19.01).Maatregelen m.b.t. inkoop zoals contractuele vastlegging zijn niet meegenomen in dit hoofdstuk.

Beschikbaarheid

	Klasse	Toelichting
	1-Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en dit heeft nauwelijks of geen gevolgen voor burgers/gebruikers.
X	2-Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en dit heeft voelbare gevolgen voor burgers/gebruikers.
	3-Hoog	Het informatiesysteem mag slechts in uitzonderlijke situaties uitvallen en dient zo snel mogelijk weer hersteld te worden. Uitval heeft (zeer) grote gevolgen voor inwoners/gebruikers.

Kenmerken:
- Tijdigheid: kan de informatie worden geleverd op het moment dat deze nodig is?
- Continuïteit: kan de informatie ook in de toekomst worden geleverd?

Relevante kaders die betrekking hebben op beschikbaarheid zijn:

Onderdeel	Vastlegging vereisten	BIO2 maategel(en)
Afspraken over serviceniveaus zoals beschikbaarheidspercentages, tijdsvensters en maximale downtime.	Projectspecifieke SLA	5.19.01 5.23.01
Toegang tot audit logs voor geautoriseerde medewerkers	Technische Architectuur, SaaS voorwaarden	8.15 8.16

Uitgangspunten:
- Dienstverlening aan inwoner 24/7; inwoner moet niet afhankelijk zijn van openstellingstijden van de gemeente voor het aanvragen van producten of het inzien van statussen en andere gegevens. Beschikbaarheidspercentage van 99,8%
- Medewerkers moeten met de systemen kunnen werken in de intern afgesproken werktijd: tussen 8:00 uur en 20:00 uur op woensdagen en donderdagen (eindtijd voor Frontoffice-, Balie- en klantcontactcentrumfuncties van Publieke Dienstverlening) en tussen 8:00 uur en 18:00 uur op werkdagen voor andere werkzaamheden. Buiten deze tijden is de beschikbaarheid van de systemen wenselijk om tijd- en plaatsonafhankelijk werken te kunnen ondersteunen. Beschikbaarheidspercentage van 99,8% tijdens bovengenoemde werktijden; Beschikbaarheidspercentage van 99,0% buiten deze werktijden.

- De audit logs zijn 24/7 te raadplegen en exporteren in een gangbaar bestandsformat voor geautoriseerde medewerkers van gemeente 's-Hertogenbosch.
- Bij uitval mag het platform maximaal 1 uur niet beschikbaar zijn, inclusief het herstellen van data, indien nodig.

Integriteit

	Klasse	Toelichting
	1-Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen (VIR definitie). Het verlies van integriteit kan leiden tot beperkte schade.
X	2-Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie (VIR-definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade.
	3-Hoog	Passende maatregelen om de juistheid, tijdigheid en volledigheid van informatie te waarborgen zijn van cruciaal belang. Het verlies van integriteit kan leiden tot zeer grote schade.

Relevante kaders die betrekking hebben op integriteit zijn inclusief wijze van vastlegging:

Onderdeel	Vastlegging vereisten	BIO2 maategel(en)
Mailverzending	Technische Architectuur, SaaS-voorwaarden	5.14.01
Securitygerelateerde inhoud auditlogs	Technische Architectuur, SaaS-voorwaarden	8.15.01
Integriteit/bescherming auditlogs	Technische Architectuur, SaaS-voorwaarden	8.15.05

Uitgangspunten:

- E-mails worden verstuurd via de gemeentelijke mailservers met al door de gemeente in gebruik zijnde domeinen. De gemeente biedt toegang tot een service/api gateway door een service, of services, te publiceren waar de technische oplossing gebruik van kan maken. Deze services zijn beveiligd met mutual TLS (MTLS) en IP-restricties. De service om de mail te versturen ondersteunt een aantal Microsoft Graph operaties. Daarbinnen zijn er de volgende mogelijkheden:
    - In de afhandeling van het bericht zal de service/api gateway een token ophalen bij Microsoft 365. Dit token wordt aan het bericht van de aanroepende partij toegevoegd en verstuurt naar Microsoft Graph. Hierbij wordt dus gebruik gemaakt van één service, één endpoint
    - Of er zijn twee endpoints beschikbaar
        - een service/endpoint voor de tokenaanvraag bij microsoftonline
        - een service/endpoint voor de Microsoft Graph operaties

    In dit geval zal de service/api gateway geen token toevoegen maar verwacht het dat de aanroepende partij dit gedaan heeft.
- Het is dus niet toegestaan om rechtstreeks met de Microsoft Graph Api te verbinden namens de gemeente.
- Uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging worden vastgelegd in zogenaamde "audit logs", die tenminste het volgende bevatten:
    - gebruikers-ID's;
    - data en tijdstippen van aanloggen en afmelden;

- overzichten van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem;
- overzichten van geslaagde en geweigerde en andere pogingen om toegang te krijgen tot individuele onderdelen van het systeem en bestanden;
- overzichten van raadplegingen en mutaties inclusief gebruikers-ID's, data en tijdstippen in geval
- van verwerking van persoonsgegevens en of vertrouwelijke gegevens.

- De audit logs zijn beschermd zodat ze niet aangepast of gemanipuleerd kunnen worden.

Vertrouwelijkheid

	Klasse	Toelichting
	1-Laag (Publiek)	Organisatievertrouwelijk - Kennisname van informatie door niet-geautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang.
X	2-Midden (Intern)	Afdelingsvertrouwelijk - Bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat.
	3-Hoog (Vertrouwelijk)	Behandelaarvertrouwelijk - Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het hoogste beveiligingsniveau.

Relevante kaders die betrekking hebben op vertrouwelijkheid zijn:

Onderdeel	Vastlegging vereisten	BIO2 maategel(en)
Verplichtstelling ISO27001-certificering voor SaaS- leverancier en hostingpartij	Technische Architectuur, SaaS-voorwaarden	5.20.03
SOC II Type II verklaring en/of een TPM (bij verwerking van bijzondere en/of gevoelige persoonsgegevens)	Technische Architectuur, SaaS-voorwaarden	5.20.03
Beveiligingsrichtlijnen voor webapplicaties	ICT-beveiligingsrichtlijnen voor webapplicaties (NCSC), Technische Architectuur, SaaS-voorwaarden.	8.27 8.29
Voldoen aan verplichte technische standaarden	Technische Architectuur, SaaS-voorwaarden	5.14.01
Gebruik van certificaten		5.14.02
Mogelijkheid tot controleren van contractueel vastgelegde verantwoordelijkheden; externe audits	Technische Architectuur, SaaS-voorwaarden	5.20.04
Verantwoordelijkheid leverancier voor beveiligingseisen bij toeleveranciers in de keten		5.21
Het gebruik van TLS en HTTP- headers	Technische Architectuur, SaaS-voorwaarden, “Gebruik van TLS en HTTP response headers” [bijlage 12a]	5.14.01
Medewerkersauthenticatie vanuit webapplicaties	Technische Architectuur, SaaS-voorwaarden	

Leveranciersverklaring bij verwerking van bijzondere en/of gevoelige persoonsgegevens	Technische Architectuur, SaaS-voorwaarden	5.20.01
Locatie van data-opslag en vestigingsplaats hostingpartij	Technische Architectuur, SaaS-voorwaarden	5.23.01
Autorisatieproces voor toegang en rechten van gebruikers en beheerders van de applicatie	Projectspecifieke SLA	5.16, 5.17
Bijhouden van autorisaties en privileges, inzage door opdrachtgever	Projectspecifieke SLA	5.16, 5.17
Het recht om contractueel vastgelegde verantwoordelijkheden te controleren of deze controle door een derde te laten uitvoeren	Projectspecifieke SLA	5.20.04
Beperkingen ten aanzien van het kopiëren en openbaar maken van informatie;	Projectspecifieke SLA	8.07.01
Inrichting escalatieproces	Projectspecifieke SLA	5.25.01

Uitgangspunten:

- Exclusiviteit: kan de informatie worden afgeschermd voor onbevoegden?
- Privacy: wordt er op een correcte manier omgegaan met persoonlijke gegevens?
- De applicatie voldoet aan de beveiligingsrichtlijnen voor webapplicaties van het NCSC, is versleuteld met protocollen en algoritmen volgens de laatste stand van de techniek en moet voldoen aan de pas-toe-of-leg-uit lijst (PTOLU) van het Forum Standaardisatie (o.a. https://, DNSSEC, IPv6, etc.)
- Het gebruik van TLS en HTTP-headers voldoet aan de laatste stand van de techniek, zoals beschreven in het document Gebruik van TLS en HTTP response headers.
    2) Componenten die gebruikt worden door medewerkers maken gebruik van een koppeling met Single Sign On (SSO) met Azure AD/Entra ID als de Identity Provider. Hierbij kan het component gebruik maken van SAML 2.0 of Open-id connect (OAuth 2.0). We gaan uit van minimale set aan gegevens en attributen: voor- en achternaam en email. De SSO-koppeling is bedoeld voor authenticatie, autorisatie dient plaats te vinden binnen de gekoppelde applicatie. Voor de toegang tot applicaties wordt gebruik gemaakt van Conditional Access.Bij verwerking van bijzondere en/of gevoelige persoonsgegevens levert de partij die het technisch beheer van de componenten doet jaarlijks een SOC II Type II-verklaring en/of een TPM op basis van een andere erkende norm op het gebied van informatieveiligheid.
- De partij die de hosting van het platform verzorgt beschikt over een ISO27001-certificering. Waarbij de verklaring van toepasbaarheid dient te worden aangeleverd.
- De data moet zijn opgeslagen binnen de Europese Economische Ruimte. Daarnaast is de vestigingsplaats van de hostende partij binnen de Europese Economische Ruimte.
- De volgende aandachtspunten moeten in ieder geval worden opgenomen in de SLA met de partij die het technisch beheer doet:
    - een autorisatieproces voor toegang en rechten van gebruikers en beheerders van de applicatie;
    - de verplichting tot het bijhouden van een lijst van geautoriseerde personen tot het gebruik van een dienst en hun rechten en privileges ten aanzien van een dergelijk gebruik;
    - beperkingen ten aanzien van het kopiëren en openbaar maken van informatie;
    - verantwoordelijkheden ten aanzien van installatie en onderhoud van software;
    - het beoogde niveau van de service (responsetijden, beschikbaarheid), evenals onaanvaardbare serviceniveaus;

    - het recht om contractueel vastgelegde verantwoordelijkheden te controleren of deze controle door een derde te laten uitvoeren;
    - het vaststellen van een escalatieproces voor het oplossen van problemen;
- De volgende aandachtspunten moeten in ieder geval worden opgenomen in de SLA met de partij die de hosting doet:
    - verantwoordelijkheden ten aanzien van installatie en onderhoud van hardware en software;
    - het beoogde niveau van de service (responsetijden, beschikbaarheid), evenals onaanvaardbare serviceniveaus;
    - het recht om contractueel vastgelegde verantwoordelijkheden te controleren of deze controle door een derde te laten uitvoeren;
    - het vaststellen van een escalatieproces voor het oplossen van problemen;
- Gegevens worden versleuteld (gehasht) opgeslagen.
- De gemeente heeft te allen tijde inzage in uitgedeelde autorisaties.

Privacy

De Oplossingen moeten voldoen aan de het Algemeen Privacybeleid van de gemeente ’s-Hertogenbosch, inclusief het Algemeen Privacyreglement AVG en het Algemeen Privacyreglement Wpg.