

VERKENNING INFORMATIE- VOORZIENING SOCIAAL DOMEIN

Plan van eisen ten aanzien van de informatievoorziening - Klantbeeld

Opgesteld door KING
Datum 5 juni 2014
Versie 0.6

Colofon

Naam document

Handreiking Plan van eisen ten aanzien van de informatievoorziening - Klantbeeld

Versienummer

0.6 concept

Versiedatum

Mei 2014

Versiebeheer

....

Copyright

© 2014 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

KING wordt als bron vermeld;

het document en de inhoud mogen commercieel niet geëxploiteerd worden;

publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de

verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door KING;

ieder kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Rechten en vrijwaring

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke

uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor

eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden.

KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave

of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Inhoud

1 Inleiding	5
Aanleiding	5
Bereik5	
Doelgroep	5
2 Klantbeeld	6
Inleiding	6
Ondersteuning aan Archetypen	7
Gebruik van het klantbeeld binnen processen	7
Doelbinding en autorisatie	10
'Dat' en 'wat' informatie	11
Klantbeeld gegevens	11
Protocollering	13
Ontsluiten van klantbeeldgegevens	14
Het klantbeeld binnen de applicatiearchitectuur	15
Ontsluiting van gegevensbronnen	16
Redundante opslag van gegevens	20
Beveiliging	22
Functionele eisen aan het klantbeeld	23

1 Inleiding

Aanleiding

De invoering van de drie decentralisatie heeft een grote impact op de informatievoorziening van gemeenten. KING heeft om die reden een programma opgezet om gemeenten hierbij te ondersteunen. Het opstellen van een Programma van Eisen (PvE) is onderdeel hiervan. Het doel van dit PvE is gemeenten te ondersteunen bij het zo optimaal mogelijk, naar de wensen van de gemeente, inrichten van de gemeentelijke informatievoorziening. Bij de uitwerking van het PvE is uitgegaan van het standaardiseren van de eisen die door de verschillende Living Lab's zouden worden opgeleverd. In de praktijk blijkt dat de Living Lab's andere paden bewandelen met betrekking tot de inrichting van het sociaal domein. Daar waar de één kiest voor een aanbesteding voor de realisatie van een nieuw regiesysteem kiest de ander voor uitbreiding van de huidige functionaliteit. De doelstelling om de eisen vanuit de Living Labs generiek te maken voor de BV Nederland blijkt hierdoor niet mogelijk. Om de gemeenten alsnog te ondersteunen is daarom voor een andere route gekozen die gebaseerd is op vijf archetypen die thans onderkend worden als modelinrichtingen waarlangs gemeenten het sociaal domein kunnen vormgeven en een aantal belangrijke thema's die gemeenten hebben aangegeven om op 1 januari 2015 hun taken waar te maken.

Bereik

In dit document wordt een beeld geschetst van de in de eerste lijn aan de professional geboden klantbeeldfunctionaliteit ten behoeve van de decentralisaties. Van het klantbeeld wordt inzichtelijk gemaakt wat de plaats is van het klantbeeld in de afhandeling van de bedrijfsprocessen. Tevens wordt inzicht verschaft in de gegevens die via het klantbeeld inzichtelijk gemaakt kunnen worden. Op basis van dit document zijn gemeenten in staat om keuzes te maken voor de ondersteuning van de professional in de eerste lijn met betrekking tot het verkrijgen van een zo volledig mogelijk beeld van een klant, en kunnen gemeenten een dialoog voeren met leveranciers van klantbeeld oplossingen.

Doelgroep

Zowel gemeenten als leveranciers behoren tot de doelgroep van dit document. Ten aanzien van gemeenten is de doelgroep informatiemanagers, coördinatoren I&A, project- en programmaleiders decentralisaties, adviseurs en informatiearchitecten. Ten aanzien van leveranciers behoren de functioneel ontwerpers, architecten en product managers tot de doelgroep.

2 Klantbeeld

Inleiding

Gemeenten kunnen voor het uitvoeren van de decentralisaties gebruik maken van een zogenaamd 'klantbeeld'. Het klantbeeld biedt inzicht in verschillende gegevens van een klant. De professional krijgt een zo compleet mogelijk overzicht krijgt over de leefsituatie van een klant, de problematiek, de voorgeschiedenis en de afgeronde en lopende ondersteuningstrajecten en zijn zelfredzaamheid. Het overzicht dat wordt getoond is één van de onderdelen die een professional tot zijn beschikking heeft om de hulpbehoefte van een klant te bepalen. De professional vertaalt de hulpvraag vervolgens naar een op maat gesneden arrangement van voorzieningen. Doelstelling is om de klant uitzicht te bieden op zelfredzaamheid.

Een klantbeeld is voldoende te noemen als het over de verschillende leefgebieden heen, zoals financiën, huisvesting en sociaal functioneren, gegevens over de klant ontsloten kunnen worden. Hiertoe zijn bijvoorbeeld gegevens over het inkomen van de klant, de arbeidsparticipatie van een klant en de opleidings- en huisvestingsgegevens van een klant vereist. Al deze gegevens vergroten het 'zicht' op de klant en geven de professional inzicht wat er bij een klant speelt.

Het klantbeeld biedt aan de professional *inzicht* in de gegevens van de klant gegevens. Waardoor voor de professional *overzicht* ontstaat over de huidige situatie van de klant. Dit overzicht biedt de klant *uitzicht* te bieden op een situatie van zelfredzaamheid

Met het ontsluiten van klantgegevens uit alleen verschillende bronnen ontstaat nog geen klantbeeld. Een klantbeeld samenstellen is complexer dan het bij elkaar verzamelen van gegevens over een klant. Om een goed beeld van de klant te krijgen moeten gegevens die ontsloten worden over de klant gecombineerd en geïnterpreteerd worden. Deze vertaling van gegevens naar informatie, met andere woorden het interpreteren van de gegevens en het op die manier verkrijgen van een beeld van de klant, is mensenwerk. Een informatiesysteem, zoals een bedrijfsregel management systeem, kan deze interpretatie niet overnemen maar wel ondersteunen. Of een professional het klantbeeld wil gebruiken om zich een beeld te vormen van de klant is aan de professional. Een wijkwerker die een keukentafelgesprek gaat voeren met een klant en 'blanco' het gesprek in wil gaan zal wellicht het klantbeeld niet gebruiken, of slechts om te bepalen of er veiligheidsrisico's zijn ten aanzien van een klant. De invulling van het gebruik van het klantbeeld en de koppeling van het klantbeeld aan de verschillende bronnen is daarmee gebruiker- en gemeentespecifiek.

Het gebruik van privacygevoelige gegevens is gebonden aan regels. Deze regels komen voort uit sectorale wetgeving en de Wet bescherming persoonsgegevens. Gebruik van gegevens wordt in de wet *verwerking* genoemd. Met *verwerking* wordt bedoeld het verzamelen, vastleggen, ordenen, bewaren, uitwerken, wijzigen, opvragen, verstrekken door middel van doorzending of enige andere vorm van terbeschikkingstelling, samenbrenging, uitwissing of vernietiging van gegevens. De wet bepaald dat verwerkingen van privacygevoelige gegevens herleidbaar moeten zijn. Deze

herleidbaarheid is van belang voor het kunnen verantwoorden van het gebruik van de gegevens aan burgers en bestuur. Herleidbaarheid van verwerking wordt gerealiseerd door het vastleggen van de verwerkingen in logbestanden. Via deze logbestanden kan inzage gegevens worden in wie, wanneer, welke gegevens heeft ingezien en voor welk doel. Deze gegevens kunnen gebruikt worden om te bepalen of de verwerking van gegevens volgens vastgestelde protocollen is verlopen. Het vastleggen van verwerkingen wordt in dit document *protocolleren* genoemd.

Ondersteuning aan Archetypen

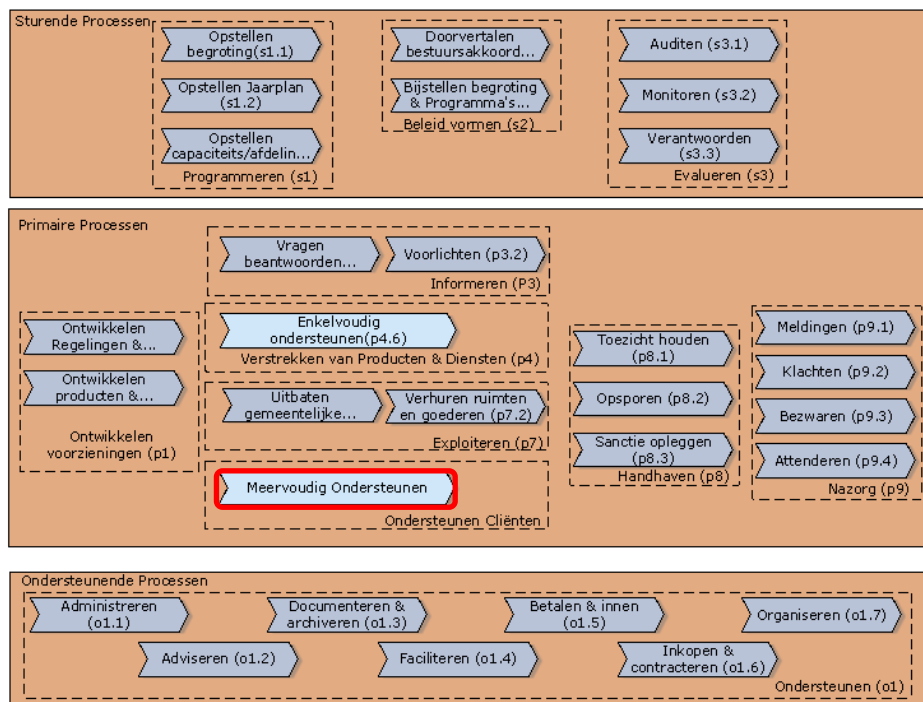
Bij de organisatie en inrichting van de decentralisaties in het sociaal domein moeten gemeenten keuzes maken ten aanzien van beleid, organisatie en proces. In de basis kunnen er even zo veel varianten ontstaan als gemeenten. Dat is niet waarschijnlijk. Het is meer waarschijnlijk, dat er zich een aantal modellen (archetypen¹) zal uitkristalliseren. Op basis van de uitvoeringspraktijk bij gemeenten zijn vijf dominante inrichtingsmodellen gedestilleerd. Het doel van deze archetypen is grip te geven op de complexe wereld van de decentralisaties en dan in het bijzonder de informatievoorziening.

Het klantbeeld is functionaliteit die vooral relevant is in situaties waar sprake is van meervoudige problematiek en regie over arrangementen. In deze trajecten is het immers van belang om er voor te zorgen dat de diverse voorzieningen uit arrangementen op de juiste momenten worden aangewend. Het integraal klantbeeld is functionaliteit die van toepassing is voor de archetypen *Totaal integraal* en *Integraal in tweede instantie*. Ook vanuit de andere archetypen kan uiteraard klantbeeldfunctionaliteit ingezet worden echter vanuit die archetypen is de functionaliteit optioneel en niet randvoorwaardelijk.

Gebruik van het klantbeeld binnen processen

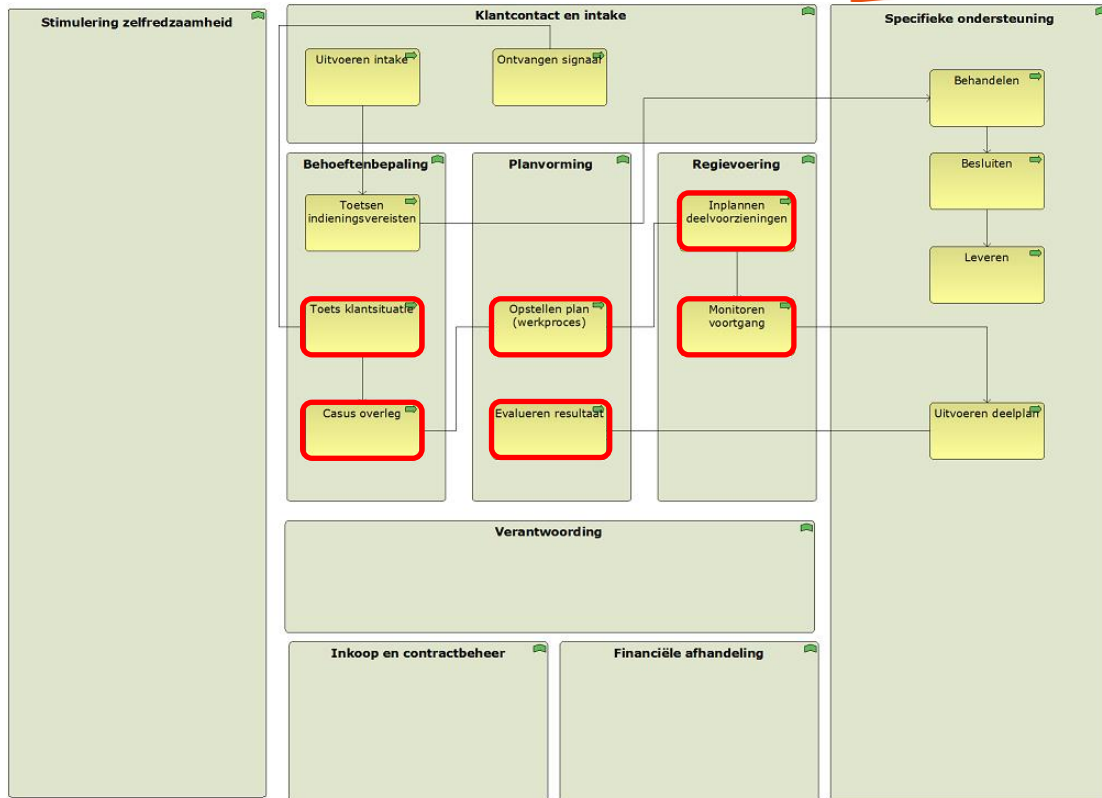
In de voorgaande paragraaf is beschreven dat het klantbeeld belangrijk is als hulpmiddel voor de professional om inzicht en overzicht te krijgen bij complexere (multiprobleem)situaties, waarbij burgers minder zelfredzaam zijn. Dit vraagt om regie op de uitvoering. Dit type problematiek wordt ondersteund door het GEMMA proces *Meervoudig ondersteunen*. Vaak begint een burger met een aanvraag voor een voorziening die via het bedrijfsproces *Enkelvoudig ondersteunen* afgehandeld kan worden. Als halverwege duidelijk wordt dat er extra ondersteuning nodig is, wordt er opgeschakeld naar het proces *Meervoudig ondersteunen*.

¹ http://www.gemmaonline.nl/wiki/Overzicht_archetypen



Figuur 1 - Processen

Onderstaand figuur illustreert deze twee processen in relatie tot het bedrijfsfunctiemodel. Het model voor meervoudig ondersteunen is hier voor de duidelijkheid sterk vereenvoudigd weergegeven. In deze figuur zijn de bedrijfsprocessen weergegeven die gebruik maken van gegevens die door het klantbeeld worden geboden. Via onder meer de gegevens uit het klantbeeld zal de professional zich binnen deze processen een beeld vormen van de cliënt en alles wat er om de cliënt heen speelt. De professional zal mede op basis van dat beeld de ondersteuning afstemmen.



Figuur 2 - Bedrijfsprocessen in relatie tot het bedrijfsfunctiemodel

Uiteraard is het klantbeeld breder in te zetten dan enkel binnen het proces meervoudig ondersteunen. Ook binnen het proces enkelvoudig ondersteunen en andere processen zal regelmatig het klantbeeld worden geraadpleegd door professionals om de meest recente gegevens van een cliënt in te zien.

Doelbinding en autorisatie

In het sociaal domein gaat het vaak om mensen in kwetsbare posities. Zij zijn met ingang van 1 januari 2015 veelal afhankelijk van de zorg, die de gemeente hun biedt. De gemeente verwerkt een groot aantal gegevens van deze kwetsbare groep mensen en ontsluit deze via het klantbeeld. Voorbeelden hiervan zijn het inkomen, de schulden, gevallen van huiselijk geweld, medische zaken etc. Allemaal persoonsgegevens die behoren tot de privésfeer van burgers. Gebruikers van het klantbeeld dienen zeer zorgvuldig met deze gegevens om te gaan en toegang moet beperkt worden tot die gebruikers die ze nodig hebben voor hun taakuitoefening. De burger moet daarop kunnen vertrouwen.

Doelbinding

De verwerking van gegevens die door het klantbeeld gebruikt worden is gebonden aan nationale en sectorale wet- en regelgeving. Voorbeelden hiervan zijn de Wet bescherming persoonsgegevens (Wbp) en de Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi). Conform wet- en regelgeving zijn gegevensuitwisseling, en daarmee verstrekking aan professionals, alleen mogelijk als:

- de eindgebruiker die gegevens nodig heeft voor het uitoefenen van een wettelijke taak. Dit wordt ook wel *doelbinding* genoemd, en
- de betrokkene zelf expliciet toestemming heeft gegeven om die gegevens voor dat doel te gebruiken, of
- de wet (Jeugdwet, Wmo, Participatiewet e.d.) het toestaat, of
- een noodsituatie waarbij de veiligheid van de inwoner of zijn of haar omgeving in het geding is.

Autorisatie

In het gemeentelijk privacyreglement wordt vastgelegd wie, welke privacygevoelige gegevens mag verwerken en wat de grondslag is voor de verwerking van gegevens is. Afgeleid van dit privacyreglement is een autorisatieplan. Een goed opgezet autorisatieplan maakt transparant wie, wanneer, welke gegevens mag verwerken. Autorisaties zijn daardoor afleidbaar en herleidbaar. Het klantbeeld biedt een mechanisme waarmee naleving van het autorisatieplan geborgd kan worden. Hiertoe is er behoefte aan autorisatie op zowel functioneel- (wie mag welke functie van het klantbeeld gebruiken) als gegevensniveau (wie mag welke gegevens zien).

Functieautorisatie

Het klantbeeld biedt zowel eindgebruiker- als beheerfuncties. De toegang tot deze functies is autoriseerbaar per gebruiker of groep van gebruikers. Een mechanisme wat hiervoor gebruikt kan worden is Role Based Access Control (RBAC). RBAC heeft als eigenschap dat gebruikers uitsluitend rechten krijgen door een vorm van groepslidmaatschap, op basis van de rol die ze hebben binnen een organisatie of bedrijfsproces.

Gegevensautorisatie

Naast de functieautorisatie is het noodzakelijk dat autorisatie op gegevensniveau mogelijk is. Gebruik van gegevens alleen toegestaan indien deze gegevens voor het uitoefenen van een wettelijke taak benodigd zijn, de zogenaamde doelbinding van de

gebruiker. Het klantbeeld houdt bij het tonen van gegevens rekening met deze doelbinding. De doelbinding is niet af te leiden van de rol(len) van een gebruiker. Gebruikers kunnen vanuit hun takenpakket meerdere doelbindingen hebben van waaruit ze gegevens via het klantbeeld opvragen. Bij een bevraging van het klantbeeld zal de gebruiker moeten aangeven vanuit welk doel de vraag wordt gesteld. Doelbindingen dienen aan gebruikers, of groepen gebruikers gekoppeld te kunnen worden. Het is mogelijk om de doelbindingen via dezelfde Role Based Access Control (RBAC) als de functieautorisatie te laten lopen.

Gemeenten zijn verplicht vast te leggen welke gegevens bij de doelbinding horen. Het klantbeeld toont vervolgens op verzoek enkel die gegevens te tonen die vastgelegd zijn in de doelbinding.

'Dat' en 'wat' informatie

Het klantbeeld ontsluit twee soorten gegevens: zogenaamde 'dat' en 'wat' gegevens. Op basis van 'dat-gegevens' is inzichtelijk dát iemand een relatie heeft met een bepaalde afdeling of organisatie zonder de inhoudelijke gegevens in te zien of te ontvangen (de 'wat-gegevens'). Een gebruiker van het klantbeeld kan dus bijvoorbeeld via de 'dat-gegevens' zien dát iemand een relatie heeft met de gemeentelijke kredietbank. Via de 'wat-gegevens' kan vervolgens, indien de gebruiker er voor geautoriseerd is, de inhoudelijke gegevens inzien. Vanuit de 'dat-gegevens' is bijvoorbeeld af te leiden dat de klant via de gemeentelijke kredietbank hulp krijgt bij schulden, preventie van schulden, inkomensbeheer en sociale kredietverlening. Via de 'wat-gegevens', bijvoorbeeld hoogte en duur van een uitkering, kunnen de inhoudelijke gegevens van de gemeentelijke kredietbank worden ingezien.

Het klantbeeld stelt vanuit de verschillende bronnen de 'dat-gegevens' samen.

Hoewel 'dat-gegevens' geen concrete informatie geven over de aard van een relatie van een klant met een instelling geeft het wel informatie over de persoon. Ook de 'dat-gegevens' vallen daarmee onder de werking van de Wet bescherming persoonsgegevens. Dit houdt in dat toegang tot deze gegevens gebonden is aan doelbinding, geautoriseerd moet worden en de verwerking gelogd dient te worden.

Klantbeeld gegevens

<<Uitkomsten discussie over gegevensset nog verwerken>>

Door het klantbeeld worden diverse gegevens ontsloten uit relevante gekoppelde externe en interne bronnen. Voorbeelden van dergelijke gegevens zijn:

- meldingen en signalen,
- onderliggende documentatie en stukken;
- lopende informele zorg (familie, overige mantelzorg, algemene voorzieningen);
- lopende collectieve en individuele voorzieningen;
- de kosten, leveringssoort, indicatie- en contractgegevens;
- de tevredenheid en wensen van de cliënt t.a.v. de geboden ondersteuning;
- de zelfredzaamheidsontwikkeling van de klant;
- et cetera.

In het rapport 'Eindadvies Verkenning Informatievoorziening Sociaal domein (VISD)' ² is een voorzet gegeven ten aanzien van de gegevens die benodigd zijn bij de uitvoering van de werkprocessen. Deze set van gegevens is in het vervolgtraject nader beschouwd. De volgende bronnen en gegevens dienen door het integraal klantbeeld minimaal ontsloten te worden:

- Actuele persoonsidentificerende gegevens zoals de familienaam, (ex)partner, (leeftijd) kinderen, ouders, onder curatele stelling, gezag minderjarige afkomstig uit de GBA;
- Persoonsidentificerende gegevens van inwonenden afkomstig uit de GBA;
- Soort inkomens- en uitkeringsverhouding afkomstig uit de Polisadministratie;
- Leerplicht / RMC afkomstig uit leerlingenadministratie gemeenten en RMC;
- Geleverde of lopende dienstverlening afkomstig uit administraties van gemeenten;
- Actuele en historische Re-integratiegegevens, zoals soort traject, aanvang en einde traject;
- Reden einde trajectplan afkomstig uit re-integratiesystemen gemeenten;
- Contactgegevens hulpverlener en hulpverlenende organisatie, de melding en duur van de melding afkomstig uit VIR;
- Signalen en meldingen en de eventuele afhandeling hiervan (o.a. overlast, huiselijk geweld) afkomstig uit het signalenregister. Onderdeel van dit signalenregister zijn signalen uit de samenloopvoorziening van het Inlichtingenbureau;
- Woningbezit;
- Medische zorginformatie;
- Registratie langdurige zorg van het CIZ;
- Registratie bij het AMHK;
- Registratie voortijdig schoolverlaten;
- Registratie aanraking met politie;
- Registratie betalingsachterstanden (zorgpremie, studieschuld, huur).

² https://www.vng.nl/files/vng/nieuws_attachments/2013/20130729-eindadvies-visd-vng-king.pdf

Protocollering

In de Wet bescherming persoonsgegevens (Wbp) zijn de nodige regels gesteld die erop gericht zijn om de persoonlijke levenssfeer te beschermen van de burgers over wie gegevens worden vastgelegd. Deze regels hebben onder andere betrekking op het recht van de burger op inzage, afschrift en correctie van de over hem vastgelegde gegevens. Ook heeft de burger het recht om te vernemen welk gebruik van de over hem vastgelegde gegevens wordt gemaakt. Op zijn verzoek dient hem mededeling te worden gedaan of en aan wie hem betreffende gegevens zijn verstrekt. Deze mededeling dient in begrijpelijke vorm de volgende zaken te bevatten

- een omschrijving van het doel of de doeleinden van de verwerking (de doelbinding);
- de categorieën van gegevens waarop de verwerking betrekking heeft;
- de ontvangers of categorieën van ontvangers;
- de beschikbare informatie over de herkomst van de gegevens.

Doel van het inzagerecht is betrokkene in staat te stellen erachter te komen of de gegevens die over hem verwerkt worden wel juist en rechtmatig zijn, en conform wetgeving zijn verwerkt (conform protocol). De Wbp geeft de betrokkene namelijk ook het recht om te eisen dat zijn gegevens worden verwijderd of gecorrigeerd. Die rechten kan iemand immers pas uitoefenen als er een mogelijkheid bestaat om erachter te komen welke gegevens er verwerkt worden.

Om te kunnen voldoen aan de bepalingen van Wbp protocollert het klantbeeld iedere verwerking van gegevens. Deze gegevens worden ter ondersteuning van de verantwoordingsfunctie gestructureerd ontsloten. Het moet mogelijk zijn om de protocollering te ontsluiten op basis van de onderstaande selectiecriteria:

- verstrekking van gegevens van een bepaalde persoon,
- verstrekkingen op een bepaalde dag,
- zoek opdrachten van specifieke gebruikers,
- verstrekkingen aan specifieke gebruikers, en
- bulkverstrekkingen.

De protocollering dient, mede gezien het belang van deze gegevens voor verantwoording van verwerkingen, onweerlegbaar te zijn en daarom beveiligd te zijn tegen mutaties en verwijderingen en bij voorkeur separaat opgeslagen te worden.

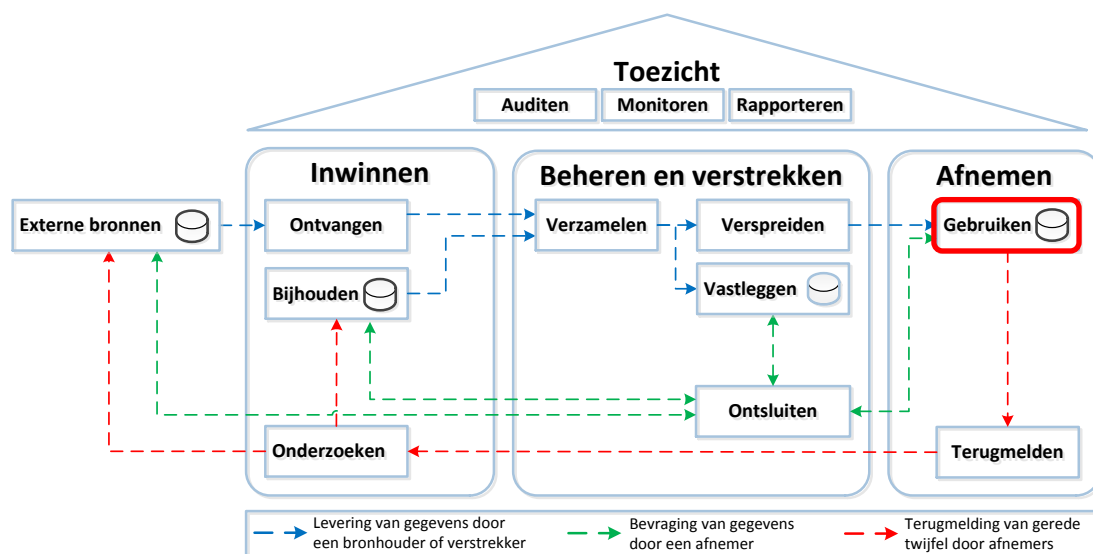
Onderdeel van de Operationele Baseline Informatiebeveiliging Gemeenten (BIG-OP) is een aanwijzing over logging³. In deze aanwijzing worden informatiebeveiligingsmaatregelen met betrekking tot logging en controle uitgewerkt, en worden handreikingen gegeven voor het logging-beleid en logging-procedures. Deze aanwijzing biedt praktische handvatten voor de inrichting van protocollering en het gebruik van de protocolleringsgegevens.

³ https://new.kinggemeenten.nl/sites/default/files/document/gr_1891/14-0106-Aanwijzing-Logging.pdf

Ontsluiten van klantbeeldgegevens

Door het klantbeeld worden diverse gegevens ontsloten naar professionals. Het klantbeeld vraagt gegevens op van verschillende bronnen en stelt deze vervolgens ter beschikking aan geautoriseerde gebruikers. Het opvragen van gegevens uit een bron verloopt bij voorkeur via een centrale gemeentelijke component. Deze centrale component is verantwoordelijk voor het koppelen aan de gewenste bron, het nagaan van autorisaties en het protocolleren van de aanvraag en verstrekking van de gegevens. In het (concept⁴) GEMMA 2.0 katern over gegevensmanagement is één en ander in detail beschreven.

Onderstaand figuur⁵ geeft de inrichting van het gemeentelijk gegevensmanagement op hoofdlijnen. Het klantbeeld geeft in deze inrichting invulling aan de functie 'Gebruiken'.



Figuur 3- Gegevensmanagement op hoofdlijnen

In bovenstaand figuur is weergegeven dat het klantbeeld gegevens kan opvragen via de 'Ontsluiten' functie van de 'Beheren en verstrekken' component van het gegevensmanagement. Deze functie kan de gewenste gegevens ophalen uit het gegevensmagazijn, lokale bronregistraties of externe bronnen. De bron van de gegevens is voor het klantbeeld niet relevant, de kwaliteit van de geleverde gegevens wel. De gegevens die aan het klantbeeld geleverd worden moeten voldoen aan de eisen die aan die gegevens gesteld worden door het klantbeeld.

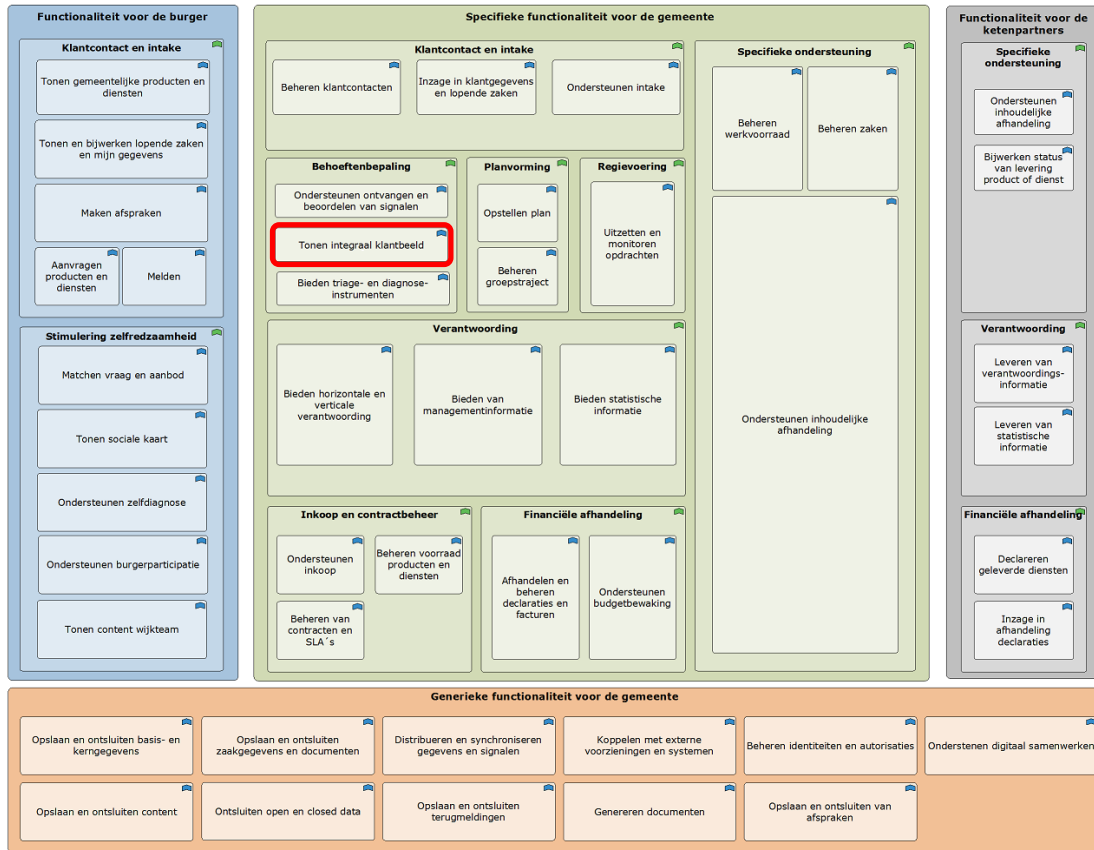
Het klantbeeld kan gegevens die opgehaald worden uit bronnen redundant opslaan in een eigen database en deze redundante gegevens vervolgens gebruiken voor het opbouwen van een klantbeeld. Aandachtspunt hierbij is wel de borging van de actualiteit en daarmee kwaliteit van de gegevens.

⁴ Publicatie van de baseline gegevensmanagement wordt verwacht in de zomer van 2014

⁵ Bron: concept baseline strategisch gegevensmanagement GEMMA 2.0 (KING)

Het klantbeeld binnen de applicatiearchitectuur

In de applicatiearchitectuur van de decentralisaties⁶ is het klantbeeld gepositioneerd als een onderdeel van de *Behoeftenbepaling* bedrijfsfunctie voor professionals.



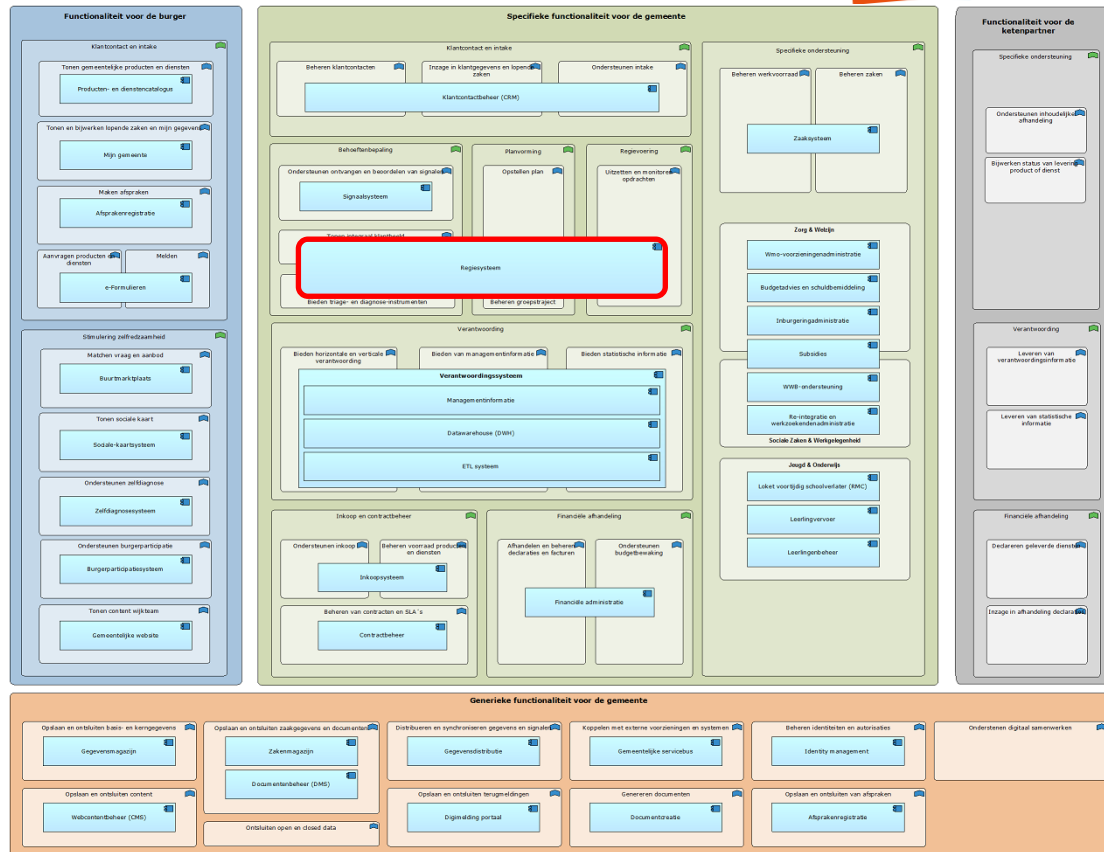
Figuur 4 - Positie van het klantbeeld in de applicatiearchitectuur

De applicatiefunctie *'Tonen integraal klantbeeld'* is de functie die verantwoordelijk is voor het ontsluiten van het klantbeeld naar de professionals. Deze applicatiefunctie is toebedeeld aan de referentiecomponent *'Regiesysteem'*. In de GEMMA softwarecatalogus⁷ zijn leveranciers van softwareproducten te vinden die een applicatie leveren die invulling geeft aan de functionaliteit van deze referentiecomponent.

Onderstaand figuur geeft de positionering van het klantbeeld als onderdeel van de referentiecomponent *'Regiesysteem'* weer.

⁶ http://www.gemmaonline.nl/index.php/Inleiding_op_3D_architectuur

⁷ <https://www.softwarecatalogus.nl/>



Figuur 5 - Referentiecomponenten sociaal domein

Ontsluiting van gegevensbronnen

Het klantbeeld verzameld vanuit diverse bronnen gegevens en ontsluit deze gegevens naar gebruikers. Deze bronnen bestaan deels uit binnengemeentelijke bronnen en deels uit externe bronnen. Voor alle gegevensbronnen geldt dat de koppelingen verlopen via de gemeentelijke servicebus. Het klantbeeld spreekt voor het ophalen van gegevens diensten (services) van de servicebus aan. Binnen de servicebus wordt via orkestratie ingesteld uit welke bron opgevraagde gegevens gelezen worden. De bron die benaderd wordt is (mede) afhankelijk van de kwaliteitseisen die door het klantbeeld aan de gegevens gesteld worden.

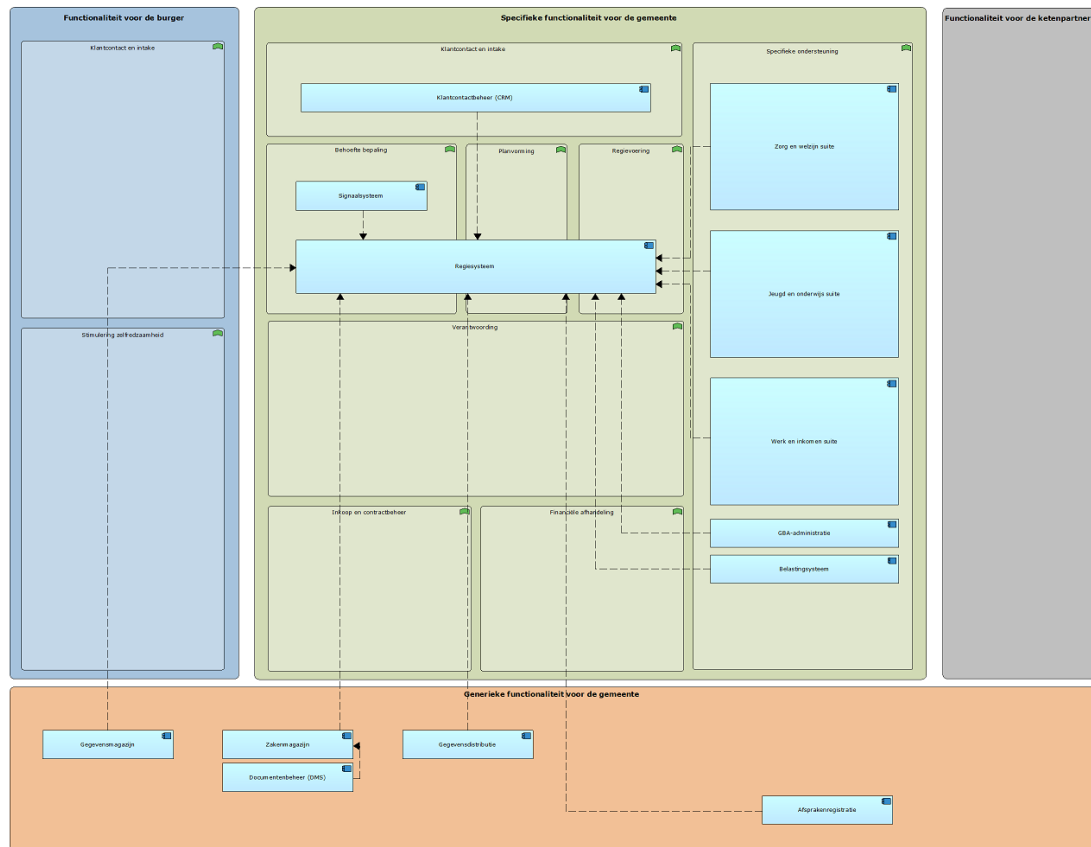
Binnengemeentelijke gegevensbronnen

Door het klantbeeld worden verschillende binnengemeentelijke bronnen die klantgegevens bevatten ontsloten. Deze bronsystemen zijn de onder meer GBA-administratie, het klantcontactbeheersysteem en het zakenmagazijn. In onderstaand figuur zijn deze koppelingen weergegeven. De koppelingen zijn weergegeven op het niveau van referentiecomponenten en softwaresuites. Referentiecomponenten zijn modulair opgezette, zelfstandig inzetbare en vervangbare delen van een systeem, die functionaliteit aanbieden via gedefinieerde interfaces. Leveranciers bieden softwareproducten die invulling geven aan één of meer referentiesystemen. In de GEMMA softwarecatalogus⁸ is per referentiecomponent opgenomen welke softwareproducten invulling geven aan de verschillende referentiecomponenten. De softwaresuites die in het figuur worden weergegeven zijn verzamelingen van

⁸ <https://www.softwarecatalogus.nl/>

referentiecomponenten die geboden worden op de beleidsterreinen van de decentralisaties. Figuur 4 geeft deze clustering van referentiecomponenten weer.

In onderstaand figuur is de gemeentelijke servicebus niet opgenomen. De feitelijke koppelingen met de gemeentelijke bronnen dienen echter via de servicebus te verlopen.



Figuur 6 - Binnengemeentelijke gegevensbronnen

Binnengemeentelijke bronnen leveren gegevens aan het klantbeeld. De onderstaande tabel geeft een overzicht van deze gegevens en de referentiecomponenten en software suites die deze gegevens leveren.

Klantgegevens	Mogelijke bronnen
Betalingsachterstanden gemeentelijke belastingen	Belastingstelsel
Geleverde en lopende dienstverlening	Zaakstelsel, Zorg en Welzijn suite, Jeugd en Onderwijs suite, Werk en Inkomens suite
Inwonenden	GBA-administratie
Persoonsgegevens	GBA-administratie
Contactgegevens regisseur	Regiesysteem
Signalering einde zorg	Zaakstelsel, Regiesysteem
Toelichtende opmerkingen over voortgang	Regiesysteem
Signalering indien zaak niet tijdig afgehandeld	Zaakstelsel
Afgesproken activiteiten	Regiesysteem
Afspraken	Afsprakenregistratie
Signalen en meldingen	Signaalsysteem

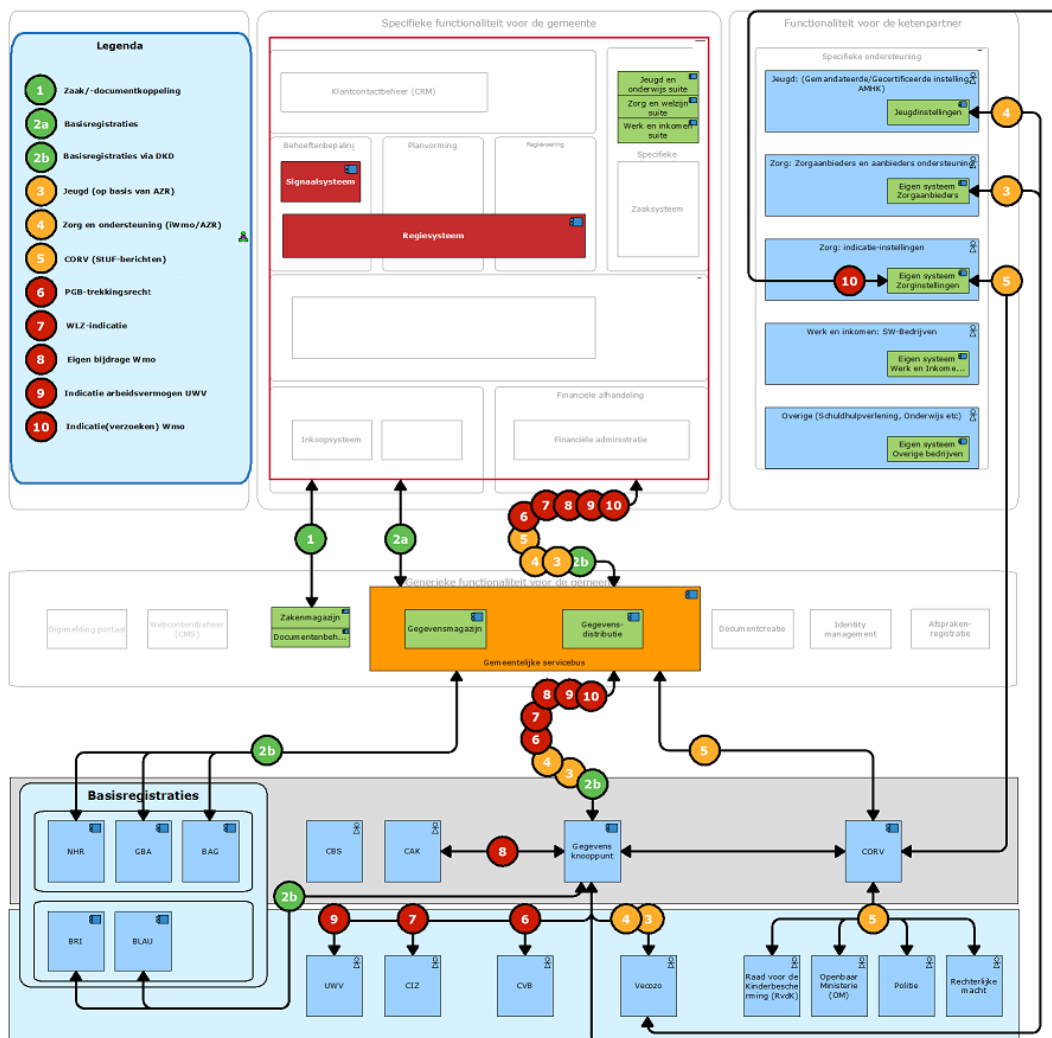
Een aantal van de binnengemeentelijke bronnen is te ontsluiten via standaard koppelvlakken en berichtstandaarden. Deze standaarden zijn de volgende:

Systemen en suites	Standaard koppelvlak/berichtstandaard
Zorg en welzijn suite	<i>Geen standaard koppelvlak beschikbaar</i>
Werk en inkomens suite	<i>Geen standaard koppelvlak beschikbaar</i>
Jeugd en onderwijs suite	<i>Geen standaard koppelvlak beschikbaar</i>
Afsprakenregistratie	<i>Geen standaard koppelvlak beschikbaar</i>
Signaalsysteem	<i>Geen standaard koppelvlak beschikbaar</i>
Klantcontactbeheer (CRM)	<i>Geen standaard koppelvlak beschikbaar</i>
Documentenbeheer (DMS)	Zaak-DMS koppelvlak voor zaakgerelateerde documenten
GBA-administratie	StUF-BG
Belastingstelsel	<i>Geen standaard koppelvlak beschikbaar</i>
Zakenmagazijn	StUF-ZKN, Zaak-DMS koppelvlak
Gegevensmagazijn	StUF-BG

Systemen en suites waarvoor (nog) geen standaard koppelvlak of berichtstandaard beschikbaar is kunnen ontsloten worden via niet gestandaardiseerde leverancier-specifieke koppelvlakken. Beschikbaarheid van deze koppelvlakken is leverancier afhankelijk.

Externe gegevensbronnen

Binnen het VISD programma worden de ketens en standaarden waarmee de verschillende externe bronnen worden benaderd nader geïnventariseerd. Onderstaand figuur geeft een idee van de verschillende externe bronnen die via de servicebus ontsloten worden.



Figuur 7 - Buitengemeentelijke gegevensbronnen

Een aantal van de externe bronnen is te ontsluiten via standaard koppelvlakken en berichtstandaarden. De vigerende standaarden zijn de volgende:

Gegevens	Wat / dat	Bron	Koppelvlak / berichtstandaard
Leerplicht/RMC	Wat	<i>nog te bepalen</i>	<i>nog te bepalen</i>
Medische zorginformatie	Wat	<i>nog te bepalen</i>	<i>nog te bepalen</i>
Re-integratiegegevens	Wat	Suwinet	SuwiML
Woningbezit	Wat	Suwinet	SuwiML
Contactgegevens hulpverlener en hulpverlenende	Wat	Verwijsindex risicojongeren (VIR)	<i>nog te bepalen</i>

organisatie			
Registratie betalingsachterstand premie zorgverzekeringen	Dat	<i>nog te bepalen</i>	<i>nog te bepalen</i>
Registratie betalingsachterstand studieschuld	Dat	<i>nog te bepalen</i>	<i>nog te bepalen</i>
Registratie Indicatie langdurige zorg	Dat	CIZ	<i>nog te bepalen</i>
Registratie bij het AMHK	Dat	AMHK	<i>nog te bepalen</i>
Registratie voortijdig schoolverlaten	Dat	DUO	<i>nog te bepalen</i>
Registratie aanraking met politie	Dat	CORV	<i>nog te bepalen</i>

Redundante opslag van gegevens

Leveranciers van het klantbeeld kunnen er voor kiezen om geen koppelingen te realiseren naar de verschillende interne en externe bronnen. In plaats daarvan kan er voor gekozen worden om de gegevens uit een eigen redundante gegevensopslag te lezen. Het is hierbij vereist dat de gegevens uit de verschillende bronnen worden gekopieerd naar de redundante opslag van het klantbeeld. Bij redundante opslag van brongegevens binnen het klantbeeld blijven de wettelijke eisen die ten aanzien van de verwerking van die gegevens gelden onverkort van kracht.

Het overnemen van gegevens kan worden gerealiseerd via hetzij een zogenaamd ETL-proces (Extract, Transform and Load) hetzij via kennisgevingen uit bronsystemen.

ETL - Bij een ETL-proces worden alle gegevens die in het klantbeeld van een bronsysteem benodigd zijn door het betreffende bronsysteem geëxporteerd, vervolgens indien nodig getransformeerd en daarna door het klantbeeld geïmporteerd in de eigen database.

Kennisgevingen – Door verschillende bronsystemen wordt een systeem gehanteerd waarbij na een wijziging van de brongegevens een kennisgeving van deze wijziging verzonden wordt naar geabonneerde afnemers. De afnemers kunnen deze kennisgevingen gebruiken voor het bijwerken van de lokale redundante gegevensopslag. Deze wijze van distributie van gegevens wordt onder andere toegepast door de BRP en NHR basisregistraties.

Redundante opslag van gegevens kent een aantal belangrijke voor- en nadelen. Deze voor- en nadelen worden in onderstaande paragrafen besproken.

Voordelen van redundante opslag

Het redundant opslaan van brongegevens en het gebruiken van een ETL-proces kent een aantal belangrijke voordelen:

- **Rapportages en selectie** – Het maken van selecties en rapportages die over combinaties van gegevens uit verschillende bronnen is eenvoudig te realiseren op het moment dat gegevens opgeslagen zijn in dezelfde bron;
- **Responsiviteit** – Het lezen van gegevens uit een bronsysteem kost altijd tijd. Hoeveel tijd dit kost is onder andere afhankelijk van het gebruikte koppelvlak, het aantal componenten wat gebruikt wordt om de vraag te beantwoorden en fysieke componenten. Een vraag die via Structured Query Language (SQL) aan een lokale gegevensopslag gesteld kan worden zal altijd responsiever zijn dan een vraag die via een webservice aan een externe bron gesteld wordt. Het klantbeeld benadert gegevens uit een aantal interne en externe bronnen. De totale tijd die nodig is voor het lezen van benodigde gegevens kan door het aantal bronnen flink oplopen. Door de benodigde gegevens lokaal redundant op te slaan kunnen ze eenvoudig gelezen worden waardoor het klantbeeld goed responsief zal zijn;
- **Eenvoud van realisatie** - Voor leveranciers is het importeren van gegevens over het algemeen eenvoudiger te implementeren is dan het realiseren van een koppeling naar een bronsysteem.

Nadelen van redundante opslag

Het redundant opslaan van brongegevens en het gebruiken van een ETL-proces kent een aantal belangrijke nadelen en risico's:

- **Actualiteit van gegevens** – gegevens die worden overgenomen via een ETL-proces zijn feitelijk al verouderd op het moment dat ze worden ingelezen. Wijzigingen in het bronsysteem worden niet doorgegeven aan de redundante opslag van het klantbeeld en het klantbeeld kent dus alleen een momentopnamen van de gegevens uit een bron. De actualiteit van de gegevens wordt bepaald door de frequentie van het inlezen van de ETL gegevens door het klantbeeld. Op het moment dat ETL-extracten uit verschillende bronnen worden gebruikt bestaat het risico dat deze op verschillende dagen of tijden zijn aangemaakt. Door de verschillende tijden waarop extracten aangemaakt zijn kan het voorkomen dat gegevens in het klantbeeld van de verschillende bronnen qua onderlinge relaties inconsistent zijn.

Bij redundante gegevens die worden bijgewerkt op basis van een abonnementen systematiek via kennisgevingen geldt dit risico niet;

- **Privacy risico's** – Door gegevens redundant op te slaan wordt een veiligheids- en privacy risico geïntroduceerd. Hoe meer kopieën er van gegevens bestaan hoe hoger het risico dat onbevoegden zich toegang verschaffen tot deze gegevens. Het redundant opslaan van gegevens maakt het ook mogelijk om (onrechtmatig) gegevens te combineren. Het maken van deze combinaties kan inzichten opleveren welke op zich weer privacy gevoelig kunnen zijn. Mede hierom is het, gezien de gevoeligheid van de gegevens, aangeraden om gegevens versleuteld op te slaan om zo misbruik van de gegevens moeilijker te maken.

Bij het gebruik van ETL-processen kunnen ook de ETL-extracten uit de verschillende bronsystemen een potentieel beveiligingsrisico vormen. Deze bestanden dienen

daarom beveiligd te worden tegen ongeautoriseerde toegang;

- **Beperkingen vanuit wet- en regelgeving** – Ten aanzien van het ETL-proces geldt dat, om redenen van bescherming van de privacy en beperkingen die voortvloeien uit nationale en sectorale wetgeving niet alle bronsystemen extracten van hun gegevens zullen mogen leveren aan afnemers.

Beveiliging

Algemeen

Door het klantbeeld wordt een grote verzameling van gevoelige persoonsgegevens ontsloten. Delen van die gegevens worden wellicht zelfs redundant opgeslagen ten behoeve van het klantbeeld. De burger heeft een wettelijk recht op privacy en bescherming van zijn gegevens, bijvoorbeeld tegen hackers. Het adequaat beschermen van de persoonsgegevens is daarom verplicht.

Bescherming van de gegevens tegen verlies en onrechtmatig gebruik dient op verschillende niveaus met een samenhangende set van maatregelen geborgd te worden. De Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)⁹ beschrijft het afgewogen minimale beveiligingsniveau waaraan een gemeente moet voldoen. De BIG staat niet op zichzelf, maar is een samenhangende set van maatregelen die in overeenstemming gebracht is met andere initiatieven zoals de Baseline Informatiebeveiliging voor het Rijk (BIR). Daarnaast zijn er initiatieven bij onder andere de waterschappen en provincies, die in lijn met de BIG lopen. Alle varianten van de Baseline Informatiebeveiliging Nederlandse Gemeenten hebben gemeen dat ze gebaseerd zijn op de ISO 27001 en 27002. Deze normen gelden als verplichte open standaard voor de overheid en staan op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Door de BIG te implementeren kan een gemeente borgen dat aan vigerende wetgeving op het gebied van de privacy voldaan wordt.

Ondersteuning mobiele toegang

Indien het klantbeeld via mobiele apparaten (telefoons, tablets, laptops) ontsloten wordt dienen specifieke beveiligingsmaatregelen getroffen te worden. De Baseline Informatiebeveiliging voor Gemeenten heeft maatregelen beschreven die te maken hebben met het gebruik van mobiele apparaten, zie hiervoor hoofdstuk 6.4 in het gemeentelijk informatie beveiligingsbeleid en hoofdstuk 7.1.3 van de BIG. De handreiking Mobile Device Management¹⁰ van de informatiebeveiligingsdienst bevat nadere informatie om goede keuzes te maken en bewustwording te creëren met betrekking tot mobile device management.

Maatregelen die op dit vlak door de gemeente genomen kunnen worden zijn onder meer:

- Vaststellen en Implementeren gemeentelijke mobiele apparaten beleidsregels
- Implementeren apparaat encryptie, in ieder geval beveiligde opslag van gemeentelijke gegevens als die al worden toegestaan op het device. Waar mogelijk zero footprint software gebruiken (zoals een VDI omgeving)
- Implementeren apparaat authenticatie

⁹ http://new.kinggemeenten.nl/sites/default/files/document/gr_1891/13-0506%20Tactische%20Baseline%20Informatiebeveiliging%20Nederlandse%20Gemeenten%20v1.0.pdf

¹⁰ https://new.kinggemeenten.nl/sites/default/files/document/gr_1891/13-1007-Mobile-Device-Management.pdf

- Implementeren kanaal encryptie en 2-factor authenticatie
- Specifiek aandacht voor beveiligingsissues in bewustwordingscampagnes

Functionele eisen aan het klantbeeld

Al de voorgaande paragrafen in overwegende nemen kunnen er minimale functionele en technische eisen gesteld worden aan het klantbeeld. In onderstaande tabel worden de minimale technische en beheer functies genoemd die door het klantbeeld ingevuld moeten worden.

Autorisatie en authenticatie

Authenticeren van gebruikers	Het authenticeren van gebruikers via een gebruikersnaam en wachtwoord combinatie of een sterkere authenticatie methode
Beheren van doelbinding	Het beheren van doelbinding definities. Onder het beheer valt: <ul style="list-style-type: none"> • aanmaken en verwijderen van doelbinding definities; • toekennen van gegevensautorisaties aan doelbinding definities; • toekennen van doelbindingen aan gebruikers of rollen.
Beheren van rollen	Het beheren van rollen. Onder het beheer valt: <ul style="list-style-type: none"> • aanmaken en verwijderen van rollen; • het toekennen van functieautorisaties aan rollen; • toekennen van rollen aan gebruikers.
Autoriseren van gebruikers	Toekennen van rollen aan gebruikers op basis van een besluit van een proceseigenaar/manager Vastleggen toegekende autorisatiebesluiten. Maandelijks rapportage over toegekende en in gebruik zijnde autorisaties.

Verantwoording

Protocolleren verwerking gegevens	Protocolleren van de verwerking van categorieën van gegevens door het klantbeeld. In de protocollering wordt opgenomen wie, welke gegevens, op welk moment en voor welk doeleinde heeft verwerkt.
Inzien protocolleringgegevens	Inzage bieden in de protocolleringgegevens ten behoeve van audits en verantwoording. Het gebruik van deze functie dient geprotocolleerd te worden.

Opslag van gegevens (optioneel)

Inlezen ETL bronbestand	Inlezen, en desgewenst transformeren, en verwerken in de lokale gegevensopslag van een extract-bestand wat door een bronsysteem van het klantbeeld is aangemaakt.
Plaatsen abonnementen	Het plaatsen, en verwijderen, van afnemerindicaties bij bronapplicaties
Verwerken kennisgevingen	Ontvangen van kennisgevingen en verwerken van deze kennisgevingen in de lokale gegevensopslag

Beveiliging

Versleutelen redundante opslag	Versleuteling van de redundante opslag om ongeautoriseerde toegang tot de gegevens zo moeilijk mogelijk te maken. Deze functie hoeft alleen ingevuld te worden indien gebruik wordt gemaakt van redundante opslag van privacy gevoelige gegevens.
--------------------------------	---

In onderstaande tabel worden de minimale eindgebruiker functies beschreven die door het klantbeeld ingevuld moeten worden.

Ontsluiten klantgegevens

Zoeken van een persoon	Zoeken naar de gegevens van een persoon op basis van identificerende attributen zoals het BSN en het adres. Bij de zoekopdracht dient aangegeven te worden wat de doelbinding van de zoekopdracht is. Zoek opdrachten dienen gelogged te worden.
Tonen van klantgegevens	Tonen van de klantgegevens uit de verschillende gemeentelijke en externe bronnen op basis van een BSN. De gegevens die worden weergegeven zijn afhankelijk van doelbinding van de gebruiker. Het tonen van de (categorieën van) gegevens dient gelogd te worden.