VNG Realisatie

Gemeentelijk Gegevenslandschap

Aanleiding en verdieping

Leeswijzer

Dit document beschrijft de visie van VNG Realisatie ten aanzien van de ontwikkeling van de gemeentelijke informatievoorziening. In deze visie worden de gemeentelijke bewegingen op het gebied van de informatievoorziening geschetst, en wordt aan de hand van deze bewegingen een nieuwe, flexibele en meer generieke en gezamenlijke gemeentelijke informatievoorziening geschetst.

Dit document is bestemd voor informatiemanagers, adviseurs en architecten.

Het document is als volgt opgebouwd:

- Hoofdstuk 1 beschrijft inleiding;
- Hoofdstuk 2 beschrijft de huidige staat van het gegevenslandschap bij gemeenten;
- Hoofdstuk 3 beschrijft het toekomstige gemeentelijke gegevenslandschap;
- Hoofdstuk 4 beschrijft de uitwerking van het toekomstige gemeentelijke gegevenslandschap.

Dit document is in beheer bij VNG-Realisatie

Tabel 1. Documenthistorie

Versie	Toelichting	Datum	Opsteller(s)
0.1	Versie voor in- en externe review	3 november 2017	VNG Realisatie
0.2	Verwerking opmerkingen G4 CIO-adviseurs	19 april 2018	VNG Realisatie
0.3	Visie in lijn gebracht met Common Ground,	16 juli 2018	VNG Realisatie
0.4	Diverse aanpassingen	4 september 2018	VNG Realisatie
0.5	Aanpassing aan huisstijl VNG Realisatie	8 oktober 2018	VNG Realisatie
0.6	Verwerking opmerkingen architecten VNG-R	22 oktober 2018	VNG Realisatie
1.0	Goedgekeurde versie door squad architectuur	28 november 2018	VNG Realisatie
1.1	Aanpassingen aan hoofdstuk Uitwerking Gemeentelijk Gegevenslandschap	12 april 2019	VNG Realisatie

VNG Realisatie
Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

Inhoudsopgave

VNG Realisatie
Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

1. Inleiding

De gemeentelijke informatievoorziening voldoet in toenemende mate niet aan datgene dat gemeenten (mogen) verwachten van een moderne informatievoorziening. De huidige informatievoorziening is grotendeels domein specifiek en verkokerd ingericht. Deze verkokering heeft geleid tot een beperkt aantal leveranciers die informatiesystemen heeft ontwikkeld, en tot een complex applicatielandschap waarbij de informatiesystemen onderling niet geïntegreerd zijn, functioneel niet scherp zijn afgebakend en bovendien niet data-gedreven zijn. Uitwisseling tussen informatiesystemen vindt plaats via complexe berichten waarbij gegevens worden gekopieerd van de bron naar domein specifieke informatiesystemen. De-facto worden volledige gegevenssets overgedragen. Deze situatie leidt tot complex berichtenverkeer, synchronisatie- en koppelingsproblematiek en bovenal een dure (in 2016 circa €1,5 miljard) en inflexibele gemeentelijke informatievoorziening. Het gevolg is dat gemeenten (te)veel tijd en geld nodig hebben om hun interne ICT omgevingen op elkaar af te stemmen. Dat zorgt voor een te lage innovatiesnelheid. Gemeenten richten zich teveel op het oplossen van problemen in de interne operatie in plaats van het verbeteren van dienstverlening aan inwoners en ondernemers.

Bovenstaande achtergrond en probleemstelling is uiteraard niet nieuw; het advies van de Studiegroep Informatiesamenleving en Overheid “Maak waar!”[1] beschrijft dezelfde problematiek. In het recente verleden zijn er veel initiatieven gestart om naar een nieuwe, flexibele en meer generieke en gezamenlijke informatievoorziening te komen. Een aantal van deze initiatieven zijn succesvol maar vele ook niet. Eén van de aspecten die samenwerken op informatievoorziening bijzonder lastig maakt is de relatie tussen een gemeenschappelijk applicatielandschap en geharmoniseerde processen. Een discussie over gemeenschappelijke informatievoorziening wordt op die manier direct een discussie over beleidsvrijheid. Dit besef groeit en ideeën om deze situatie te doorbreken worden inmiddels omarmd door IMG100+, VIAG, de taskforce Samen Organiseren en VNG Realisatie.

[1] https://www.digitaleoverheid.nl/document/rapport-maak-studiegroep-informatiesamenleving-en-overheid/

1.1. Gemeentelijke bewegingen

Vanuit gemeenten zijn een aantal bewegingen georganiseerd rondom het verbeteren van de gemeentelijk informatievoorziening. Deze bewegingen streven allen naar een nieuwe inrichting van de gemeentelijke informatievoorziening waarbij standaardisatie en collectiviteit een grote rol spelen. Deze bewegingen zijn:

- **Samen organiseren** - beschrijft hoe gemeenten gezamenlijk (collectief) de gemeentelijke uitvoeringskract kunnen versterken;
- **De +1-gemeente** - beschrijft de gemeentelijke interactiestrategie naar burgers en ondernemers en de wijze waarop de gemeentelijke dienstverlening in de toekomst wordt vormgegeven;
- **Common Ground** - beschrijft hoe gemeenten samen organiseren kunnen vormgeven, en welke processen en technologieen in het voortbrengingsproces worden gebruikt.

De belangrijkste bewegingen worden in de onderstaande paragrafen kort beschreven.

1.1.1. Samen Organiseren[2]

Het belang om als gemeenten gezamenlijk te werken aan de gemeentelijke uitvoeringskracht is groot. Omdat de vraagstukken te divers en vaak ook te complex zijn om als gemeente zelfstandig op te pakken, en ook omdat er winst te behalen is om zaken samen te organiseren en uit te voeren. Winst in termen van verbetering van de kwaliteit en toegankelijkheid van de dienstverlening aan burgers en bedrijven en kostenbesparingen. Dáár staat de beweging Samen Organiseren voor. Samen Organiseren is het vliegwiel voor het verbinden en versnellen van de Gezamenlijke Gemeentelijke Uitvoering (GGU), onder meer op het gebied van dienstverlening en bedrijfsvoering. Samen Organiseren ondersteunt, organiseert, stimuleert, inventariseert en schaalt op onder het motto: één keer ontwikkelen, 380 maal toepassen.

De essentie van de werkwijze Samen Organiseren is dat het echt door en voor gemeenten is. Gemeenten staan zélf aan het roer: zij zijn eigenaar van datgene dat we gezamenlijk ontwikkelen. De VNG ondersteunt daarbij. Echt samen organiseren houdt in dat gemeenten standaarden afspreken, in eerste instantie op de terreinen informatiebeleid, informatietechnologie en dienstverlening. Zoals dat met de cao voor gemeenten al jaren gebeurt. Voor standaarden in informatiebeleid, informatietechnologie en dienstverlening hebben gemeenten het College van Dienstverleningszaken in het leven geroepen. Het College adviseert het VNG-bestuur over het vaststellen van standaarden en over initiatieven voor versnelling in de opschaling. Op zijn beurt wordt het College geadviseerd door de Taskforce Samen Organiseren, bestaande uit gemeentesecretarissen, directeuren Dienstverlening, een lid namens de ketenpartners en vertegenwoordigers van de koepelverenigingen VDP, IMG 100.000+, VIAG en FAMO. De financiering van de gezamenlijke gemeentelijke activiteiten verloopt via het ingestelde Fonds Gezamenlijke Gemeentelijke Uitvoering (GGU).

Door samen op te trekken wordt de gemeentelijke dienstverlening efficiënter, goedkoper en effectiever, zodat er tijd en geld overblijft om aandacht te besteden aan zaken die voor de lokale burgers van belang zijn, zoals

[2] https://www.vngrealisatie.nl/roadmap/samen-organiseren

zorg, digitale ondersteuning en veiligheid. In de Digitale Agenda is dat samengevat als: ‘Massaal-Digitaal – Maatwerk Lokaal.’

1.1.2. De +1-gemeente[3]

De samenleving wordt steeds complexer. Het is een belangrijke taak van de gemeente om inwoners en ondernemers hierin de weg te wijzen. Zodat bijvoorbeeld ouderen de hulp krijgen die er voor hen is en mensen met schulden de ondersteuning krijgen die ze nodig hebben. De gemeente is de meest nabije overheid en dient die rol effectief in te vullen. Dit vraagt om een organisatie die past bij deze tijd en is voorbereid op de toekomst. Dit betekent een klantgedreven dienstverlening en efficiënte bedrijfsvoering die optimaal gebruikmaken van digitale mogelijkhedenen en waar de menselijke maat leidend is. Een gemeente die waarde toevoegt aan de maatschappij, samen met haar partners in de samenleving. De +1-gemeente schetst de ‘ideale’ gemeentelijke organisatie.

De +1 gemeente weet zich ontzorgt door een uitstekende digitale infrastructuur, waarmee ze haar dienstverlening veilig en optimaal inricht. Efficiency is niet meer het doel, want dat de aanname is dat dat is geregeld. Het gaat om effectiviteit: doet de gemeente daadwerkelijk dat wat nodig is in de samenleving? Draagt ze bij aan een gezonde en veilige leefomgeving, faciliteert ze ondernemers zodanig dat de arbeidsmarkt wordt versterkt, ondersteunt ze inwoners zodat die zelf hun weg kunnen vinden in werk en leven?

De +1-gemeente werkt volgens een aantal leidende principes:

- De gemeente is van de samenleving, staat in de samenleving en werkt met de samenleving. Niet organisatorische grenzen en belangen of regels en procedures, maar wat inwoners, ondernemers en de samenleving als geheel nodig hebben zijn leidend.
- Elk vraagstuk heeft zijn eigen schaal. De inwoner en ondernemer bepalen de schaal waarop wordt geacteerd. Van landelijk tot persoonlijk.
- Eenvoud staat voorop. Als mensen vastlopen in de bureaucratie: maak het eenvoudiger. Dat geldt voor inwoners, ondernemers en medewerkers. Dus zowel voor dienstverlening als bedrijfsvoering.
- De overheid werkt transparant en open, ook in haar samenwerking met burgers, andere overheden en maatschappelijke partners.
- Gegevens zijn beschikbaar en toegankelijk en worden ingezet om de dienstverlening en bedrijfsvoering continu te verbeteren.
- Dienstverlening is digitaal waar het kan en persoonlijk waar gewenst.
- Bij de inrichting van de dienstverlening en bedrijfsvoering gaat het om effectiviteit.
- Inwoners en ondernemers hebben regie en zeggenschap over hun eigen gegevens.
- De overheid werkt en communiceert veilig en betrouwbaar.
- Zowel de organisatie als de medewerkers zijn flexibel, zodat ze zich kunnen blijven aanpassen aan veranderende omstandigheden.

[3] https://www.vngrealisatie.nl/nieuws/1-gemeente-de-organisatie-een-greenfield

Voor het realiseren van de +1-gemeente zijn een aantal randvoorwaarden nodig:

- Inwoners en ondernemers krijgen een digitale identiteit, die ze voor alle dienstverlening kunnen gebruiken. Deze regelt identificatie, authenticatie en veilige toegang tot data.
- Dankzij deze digitale identiteit krijgen zij zeggenschap over gebruik en toepassing van hun eigen gegevens.
- Processen worden ontworpen vanuit het doel van dat proces.
- Er is een generieke digitale infrastructuur waarmee gemeenten veilig kunnen werken en samenwerken.
- Gemeenten ontwikkelen waar gewenst samen: 1x ontwikkelen, 388x gebruiken.
- Doordat gemeenten en andere overheden dezelfde standaarden gebruiken, ontstaat er een ecosysteem van toepassingen die alle overheden kunnen gebruiken.
- In de informatie-architectuur zijn data losgekoppeld van applicaties. Zodat bijvoorbeeld gegevens uit dezelfde bron in meerdere processen gebruikt kunnen worden.
- Gemeenten kopen producten en diensten collectief in.

1.1.3. Common Ground[4]

Common Ground is een ontwerp en een veranderstrategie voor een nieuwe gemeenschappelijke gemeentelijke informatievoorziening. Deze maakt het mogelijk om de gemeentelijke dienstverlening en bedrijfsvoering snel en exibel te moderniseren.

Door de twee gemeentelijke koepelverenigingen voor I&A professionals IMG100.000+ en VIAG is een beweging gestart om het huidige te trage tempo van innovaties in dienstverlening aan inwoners en ondernemers te doorbreken. Deze ‘Common Ground’ beweging gaat uit van een radicale omkering: het bouwen van de digitale gemeente alsof geen rekening gehouden hoeft te houden met datgene wat er al is. Niet alleen op procesniveau, maar juist ook in techniek achtervolgt de erfenis van plm. 30 jaar automatisering in gemeenteland ons: we borduren voort op een allang achterhaald concept van systemen waarin gegevens, bedrijfslogica en gebruikersinterface met elkaar vervlochten zijn. We spreken van silo’s die met aanvullende software en kopieslagen van elkaars gegevens met elkaar communiceren. Hiertussen bestaan dure en risicovolle koppelingsmechanismen met als gevolg hoge beheerkosten, moeilijk beheersbare beleidsimplementaties, te hoge veiligheidsrisico's en aanhoudende koppelingsproblemen. Het is deze erfenis die daadwerkelijke vooruitgang in de weg staat en complexiteit in stand houdt.

Common Ground volgt niet de traditionele top-down benadering van eerst uniformeren op procesniveau, invoeren en opschalen, maar bekijkt de opgave juist van een meer informatiekundigeinvalshoek. Wanneer een proces of gebruikersinterface moet worden aangepast beschouwen we het geheel aan informatiesystemen wat aangepast moet worden. Dat betekent dat juist op informatiekundig/technisch niveau gemeenten méér moeten uniformeren naar een eigentijdser gelaagd model. Naast de potentie die dit idee heeft voor versnelde verbetering van de dienstverlening aan inwoners en ondernemers biedt Common Ground ook een perspectief op een verbetering van de informatieveiligheid en bescherming van de privacy. Het opent de markt voor ICT leveranciers door het toe kunnen laten van nieuwe innovatieve spelers. Niet onbelangrijk: het biedt door een

[4] https://vng.nl/samen-organiseren/common-ground

gezamenlijk gegevensmanagement en ICT operatie perspectief op rationalisatie en kostenreductie. Common Ground sluit in haar filosofie en uitwerking volledig aan bij de uitgangspunten van het rapport “Maak Waar!”.

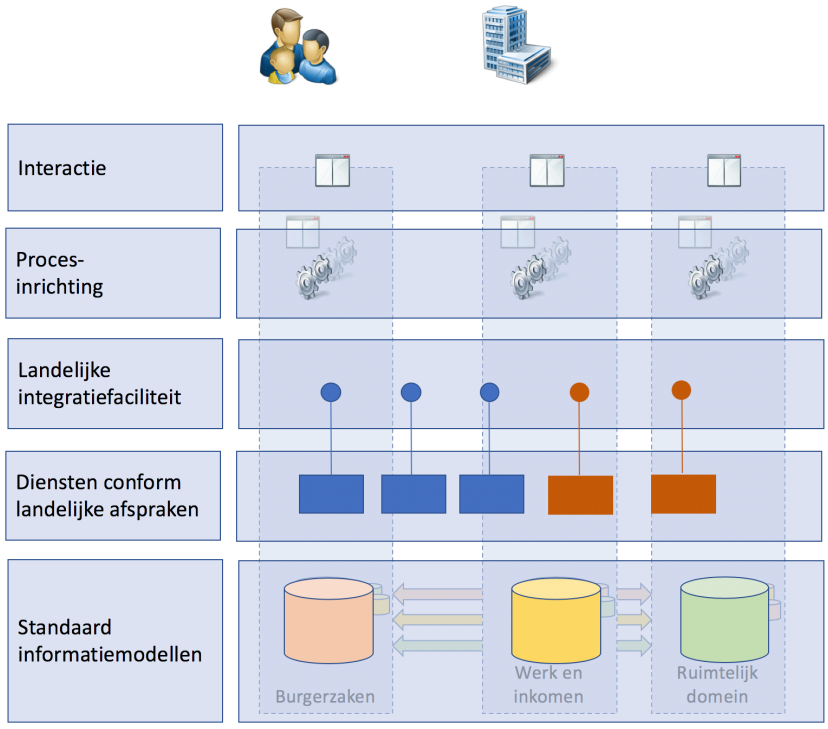
De kracht van Common Ground zit ook in de veranderstrategie die de werkwijze binnen de +1-gemeente mogelijk maakt. Een big bang invoering is niet nodig in deze filosofie. Gemeenten stappen over op het moment dat zij er aan toe zijn om deze stap te maken, bijvoorbeeld op het moment dat een grote vervangingsinvestering in de eigen infrastructuur aan de orde is.

Doelstellingen van de Common Ground beweging zijn[5]:

- Het faciliteren van een flexibelere informatievoorziening die sneller kan reageren op veranderingen;
- Benutten van schaalvoordelen om de kosten te drukken mede omdat dit platform eenvoudig te realiseren is in gezamenlijke rekencentra (gemeentelijke cloud);
- Oplossen en voorkomen van koppelproblemen;
- Verhogen van de kwaliteit van data door real-time gebruik en geen kopieverschillen;
- Meer aanbod creëren in de markt – meer ruimte voor innovatie;
- Delen van investeringen via hergebruik;
- Beheersing van informatieveiligheid (onder andere door het integraal gebruik van data in plaats van per kolom);
- Vergroten van de kwaliteit van de informatievoorziening (ook in termen van continuïteit en betrouwbaarheid);
- Ruimte te bieden voor lokale verbijzondering.

Het model wat door de Common Ground beweging wordt gehanteerd ter visualisering van bovenstaande doelen bestaat uit vijf lagen. De onderste drie lagen van het model omvatten de standaardisatie van semantiek en syntax van de ontsluiting van de gegevensbronnen, de daarbij behorende gestandaardiseerde diensten (APIs) en een gemeenschappelijke integratiefaciliteit. De bovenste twee lagen van het model omvatten de inrichting en ondersteuning van processen en interactie volgens lokale wensen.

[5] https://vng.nl/files/vng/common_ground_-_voorstel.pdf



Figuur 1 - Common Ground model

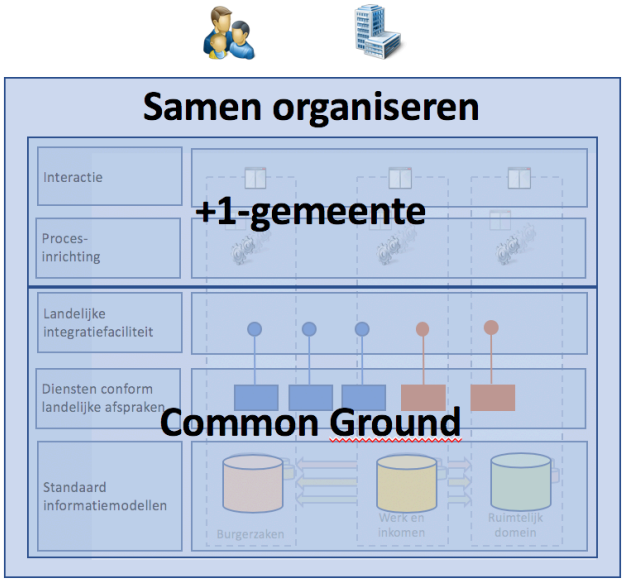
Uitgangspunt van het gemeentelijke Common Ground model is het collectief organiseren van voorzieningen en het standaardiseren van de diensten op de verschillende lagen van dit model. De standaardisatie binnen de Common Ground beweging richt zich in eerste aanleg met name op de onderste drie lagen van het model;

- de standaardisatie van gegevens via informatiemodellen,
- de ontsluiting van gegevens via landelijk gestandaardiseerde APIs en
- het beschikbaar maken van de APIs via een veilige infrastructuur.

1.2. Het gemeentelijk gegevenslandschap

De Common Ground, Samen Organiseren en +1-gemeente bewegingen zijn complementair aan elkaar. Ze gaan uit van het efficient inrichten van de bedrijfsvoering zodat de dienstverleningsprocessen richting de burger effectieveren kanb worden. Daarnaast richten deze bewegingen zich op het verbeteren van de informatiepositie van de burger inzake zijn eigen gegevens en het bieden van transparantie ten aanzien van het handelen van de (gemeentelijke)overheid naar burger en bestuurder. De Common Ground en +1-gemeente bewegingen richten zich op standaardisatie van de elementen op de verschillende architectuurlagen en de Samen Organiseren beweging richt zich op het collectief organiseren van deze gestandaardiseerde elementen.

In dit document worden de verschillende bewegingen bijeen gebracht en nader uitgewerkt en geduid binnen het 'Gemeentelijk Gegevenslandschap'. Het Gemeentelijk Gegevenslandschap geeft beschrijft aan welke principes dient het informatielandschap en de informatievoorzieningen van gemeenten dienen te voldoen, en waarom ze daar aan moeten voldoen. In deze uitwerking wordt het vijf-lagen architectuur model van de Common Ground beweging als basis gebruikt voor de indeling en visualisatie van de verschillende architectuurelementen.



Figuur 2 – Samenhang Common Ground en de +1-gemeente

Bovenstaand figuur geeft aan hoe binnen het vijf-lagen model de zwaartepunten van de verschillende bewegingen verdeeld zijn. Hierin wordt duidelijk dat de +1-gemeente zich met name richt op de procesinrichting en interactie met inwoners en ondernemers. De Common Ground beweging richt zich op de standaardisatie en ontsluiting van gegevens via een gemeenschappelijke veilige landelijke integratiearchitectuur. De Samen Organiseren beweging richt zich op alle aspecten uit de verschillende lagen van het model en organiseert en faciliteert daar waar gewenst collectiviteit.

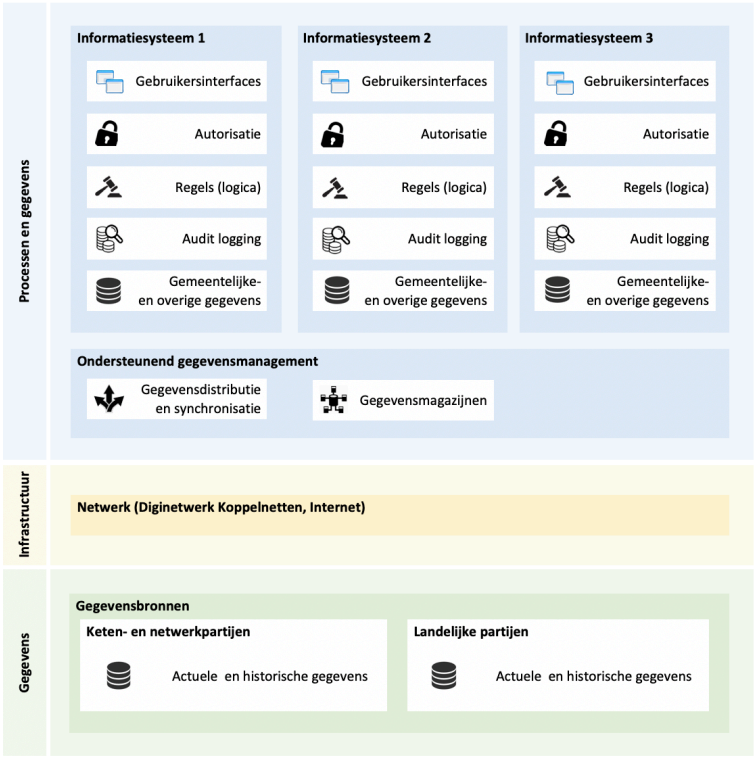
2. Huidige gemeentelijke situatie

2.1. Beschrijving huidige situatie

Gemeenten maken voor de uitvoering van hun taken gebruik van een groot aantal gegevensverwerkende informatiesystemen. Deze informatiesystemen zijn veelal gericht op de ondersteuning van de gemeente op een specifiek gemeentelijk taakvlak. Voorbeelden van dergelijke taakvlakken zijn werk en inkomen, belastingen, burgerzaken en de jeugdzorg. Daarnaast wordt door gemeenten gebruik gemaakt van informatiesystemen die een meer horizontale taak hebben. Voorbeelden hiervan zijn zaak- en documentsystemen en gegevensmagazijnen. De informatiesystemen worden zowel qua functionaliteit als gegevens die gebruikt worden door de leveranciers van de software afgebakend en zijn toepasbaar voor alle gemeenten. Daar waar mogelijk wordt door leveranciers gebruik gemaakt van nationale- en internationale standaarden, bijvoorbeeld op het gebied van informatiemodellen (denk aan het Suwi-Gegevensregister[6] en INSPIRE[7]).

Door leveranciers wordt relevante wet- en regelgeving voor het domein waarbinnen de applicatie wordt ingezet vertaald naar regels (programma logica). Deze programmalogica kan bij een groot deel van de applicaties niet door gemeenten geconfigureerd worden. Gemeenten worden hierdoor beperkt in de mogelijkheden om hun processen in te richten.

[6] https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/suwi-gegevensregister-sgr
[7] https://www.geonovum.nl/onderwerpen/inspire



Figuur 3 - Huidig gemeentelijk gegevenslandschap

Informatiesystemen verwerken zowel gemeentelijke sectorale gegevens als gegevens uit basisregistraties en landelijke voorzieningen. In het huidige gegevenslandschap worden gegevens uit basisregistraties door gemeenten gedupliceerd en opgeslagen binnen de sectorale informatiesystemen en gegevensmagazijnen. Deze gedupliceerde basisgegevens worden via een synchronisatie- en distributiemechanisme synchroon gehouden met de oorspronkelijke bron. Dit geldt ook voor gemeentelijke sectorale gegevens, ook deze worden binnengemeentelijk op grote schaal gedupliceerd en hergebruikt.

2.2. Huidige knelpunten

Gemeenten worden zich in toenemende mate bewust van het feit dat de huidige inrichting van de gemeentelijke informatievoorziening gezien de eisen die vanuit wet- en regelgeving gesteld worden niet houdbaar is. Het dupliceren van gegevens gaat in tegen het principe van bevraging bij de bron, het leidt tot inconsistenties in gegevens met alle gevolgen van dien, introduceert beveiligings- en privacy risico's en bemoeilijkt de transparantie ten aanzien van de verwerking van gegevens. Grip op de eigen informatievoorziening en overzicht op gegevensstromen is onvoldoende. Gemeenten zijn afhankelijk van hun softwareleveranciers voor inzichten in de gegevensstromen en worden hierdoor beperkt in hun handelen. Deze situatie is ontstaan door een combinatie van factoren.

- **Falend gemeentelijk leveranciersmanagement**
  Gemeenten hebben onvoldoende hun opdrachtgeversrol ingevuld. Ze hebben te weinig invloed genomen op de functionaliteit die door de informatiesystemen wordt geboden, en hebben slechts beperkt invloed uitgeoefend op de gegevens die door deze systemen worden verwerkt. In plaats van het aanbesteden van gewenste functionaliteit hebben gemeenten alomvattende informatiesystemen aanbesteed. Bij de aanbesteding van deze systemen is door gemeenten in veel gevallen aangegeven dat deze aan de GEMMA moeten voldoen, maar wordt onvoldoende aandacht besteed aan een vertaling van de globale GEMMA-specificaties naar specifieke gemeentelijke eisen en wensen. Gemeenten worden hierdoor geconfronteerd met informatiesystemen die niet goed passen op de gemeentelijke processen en bedrijfsvoering en zitten voor jaren vast aan deze informatiesystemen en leveranciers.

- **Falende standaarden**
  Standaarden die gemeenten hadden moeten helpen bij de koppelvlakproblematiek, hebben gemeenten in onvoldoende mate ontzorgt. In de praktijk blijkt koppelingsproblematie ondanks de ontwikkelde standaarden weerbarstig. De ontwikkelde standaarden zijn vaak complex en bieden ruimte voor interpretatieverschillen. Hierdoor worden gemeenten geconfronteerd met lange implementatietrajecten en dure (maatwerk)koppelingen.

- **Gemeentelijke architectuur die uitgaat van gegevensreplicatie**
  De oude GEMMA-architectuur propageerd het repliceren van gegevens uit de informatiesystemen tebn behoeve van e-dienstverlening. Mede daardoor heeft de implementatie van gegevensmagazijnen en gegevensdistributiesystemen een grote vlucht genomen. Gevolg hiervan is dat bijvoorbeeld persoonsgegevens in een groot aantal applicaties worden opgeslagen en, in sommige gevallen, synchroon worden gehouden met de originele bron via een geautomatiseerd systeem van datadistributie en synchronisatie. In andere gevallen is het synchroniseren van de gegevens met de bron een handmatige actie. Mede ten gevolge van het binnengemeentelijk repliceren van gegevens is de complexiteit van het gemeentelijk gegevensmanagement hoog. Deze complexiteit leidt tot hoge kosten en kans op fouten.

- **Ontbreken van de juiste competenties**
  Gemeenten hebben moeite met de nieuwe werkwijze voor gemeenten rond privacy en security by-design. Elke gemeente moet zelf uitzoeken wat deze nieuwe wetgeving betekent voor haar processen. Lang niet

alle gemeenten hebben hiervoor de mensen met juiste competenties in huis. Gemeenten weten hierdoor onvoldoende welke eisen ze moeten stellen aan leveranciers.

Mede doordat gemeenten onvoldoende grip en invloed hebben op binnengemeentelijke gegevensstromen staat de compliance aan wet- en regelgeving onder druk. Daarnaast is het inspelen op maatschappelijke en organisatorische ontwikkelingen ingewikkeld en enkel tegen hoge inspanningen en kosten mogelijk. Uitdagingen waar gemeenten nu voor staan:

- **Compliancy aan wet- en regelgeving**
  Vanuit de Algemene Verordening Gegevensbescherming (AVG) worden de rechten van burgers, en de plichten van organisaties die persoonsgegevens verwerken, beschreven op het gebied van de bescherming van persoonsgegevens. Eisen worden onder andere gesteld aan de wijze waarop gegevens verwerkt worden en de wijze waarop hierover zowel in- als extern transparant verantwoord wordt. Daarnaast worden de rechten van burgers ten aanzien van ‘hun’ gegevens beschreven. Deze rechten zijn onder andere het inzagerecht, correctierecht en het recht om vergeten te worden. In de huidige situatie waarin gemeenten de applicaties van (veel) verschillende leveranciers gebruiken die elk op hun eigen manier de gegevensverwerking vormgeven is het voor de gemeente een complexe uitdaging volledig compliant te zijn met de AVG. Informatiesystemen zijn meestal niet ingericht op de eisen die vanuit de AVG gesteld worden. Principes zoals het kennen en vastleggen van een ‘doelbinding’ als grond voor een verwerking zijn bijvoorbeeld binnengemeentelijk niet eenduidig geïmplementeerd. Het is hierdoor voor gemeenten niet (eenvoudig) mogelijk om de verwerking van persoonsgegevens in- en extern op een adequate manier te verantwoorden. De opzet en complexiteit van het gemeentelijk applicatielandschap biedt ook niet de verwachting dat op korte termijn volledig aan de eisen vanuit de AVG voldaan kan worden.

  De Wet Digitale Overheid (invoering naar verwachting 2020) verplicht organisaties een sluitende audit trail van informatietransacties tussen gebruikers en de gemeente bij te houden. Het bijhouden van de complete audit-trail van een informatietransactie vraagt om een samenhangende gestandaardiseerde inrichting van de gemeentelijke informatiearchitectuur en het gegevenslandschap. In de huidige opzet van de gemeentelijke landschappen waarin er een groot aantal applicaties van diverse leveranciers gebruikt en standaarden ten aanzien van transparantie over verwerkingen ontbreken is het opbouwen van een complete audit trail niet geautomatiseerd mogelijk.

- **Ontkokering van de organisatie**
  De afgelopen jaren hebben gemeenten zich ontwikkelt zich van sectoraal verkokerde organisaties naar organisaties die in hoge mate integraal willen en moeten werken, zowel intern als met externe keten- en netwerkpartijen. De dienstverlening naar burgers en bedrijven wordt in een rap tempo ontschot, denk hierbij bijvoorbeeld aan de ontwikkelingen in het sociaal domein op het gebied van maatschappelijke ondersteuning, jeugdhulp en participatie en de omgevingswet. Deze ontwikkelingen stellen nieuwe eisen aan de gemeentelijk informatievoorziening op het vlak van de beschikbaarheid, herleidbaarheid en kwaliteit van functionaliteit en gegevens alsmede op beveiliging en de bescherming van de privacy.

- **Ondersteunen van de veranderende samenleving**
  De samenleving verandert door snelle technologische ontwikkelingen. Burgers krijgen een centrale rol, pakken steeds meer zelf de regie, organiseren zich in netwerken en oefenen invloed uit via nieuwe kanalen zoals bijvoorbeeld de sociale media. Er komen voortdurend nieuwe technologieën beschikbaar die burgers en bedrijven steeds sneller adopteren en gebruiken, bijvoorbeeld om onderling informatie uit te wisselen, te communiceren, zaken te doen en de bedrijfsprocessen te optimaliseren. Het faciliteren van de burger door het aansluiten van de gemeentelijke dienstverlening op de nieuwe kanalen en technologieën is door de wijze waarop de gemeentelijke informatievoorziening is georganiseerd ingewikkeld en duur. Gemeenten zijn hiervoor afhankelijk van de medewerking van de leveranciers van de gemeentelijke applicaties en het is door het gesloten karakter van de huidige informatiesystemen voor nieuwe spelers lastig om de gemeentelijke markt te betreden. Hierdoor ontbreekt het aan de benodigde innovatie en blijft de vernieuwing van de gemeentelijke dienstverlening achter.

- **Uitwisselbaarheid van gemeentelijke gegevens**
  Leveranciers zijn leidend in de vaststelling van de functionaliteit van hun informatiesystemen en de gegevens die door deze systemen verwerkt worden. Daarnaast beperken leveranciers de wijze waarop, en voorwaarden waaronder deze gegevens ontsloten worden. Hierdoor is er sprake van zeer beperkte onderlinge uitwisselbaarheid (portabiliteit) van gegevens. Dit gebrek aan standaardisatie leidt in de praktijk tot problemen bij het ontsluiten van gegevens uit applicaties, het combineren van gegevens uit verschillende applicaties en bij het overstappen van de ene naar een andere leverancier.
  De gebrekkige portabiliteit van gegevens is ook bij het vormen en exploiteren van samenwerkingsverbanden een probleem. Binnen samenwerkingsverbanden hebben de deelnemende gemeenten over het algemeen een scala aan leveranciers. Door de gebrekkige data-portabiliteit zijn synergievoordelen binnen het samenwerkingsverband lastig te bereiken doordat de gegevens van aan de samenwerking deelnemende gemeenten qua syntax, structuur en soms ook semantiek niet gelijk zijn.

- **Vrije toegang tot gemeentelijke gegevens**
  De ambities van gemeenten op het gebied van het zowel in- als extern ontsluiten van gesloten en open data sluiten niet aan op de manier waarop de informatiearchitectuur van de gemeente nu is georganiseerd. De gemeentelijke applicaties zijn gesloten en niet, tot zeer matig, gestandaardiseerd qua gegevensmodellering en -ontsluiting. Het beschikbaar maken van gegevens voor zowel in- als extern gebruik is ingewikkeld en vraagt om inspanning van de verschillende betrokken gemeentelijke softwareleveranciers. Deze inspanning betreft vaak het laten ontwikkelen van maatwerksoftware. Gemeenten zijn hierdoor afhankelijk van leveranciers bij het ontsluiten van hun eigen gegevens.

- **Vendor lock-in**
  Het gebrek aan goede standaarden gecombineerd met het gebrek aan regie van gemeenten op de functionaliteit van applicaties heeft geleid tot een gemeentelijk landschap waarin applicaties zeer beperkt zijn gestandaardiseerd qua koppelvlakken en functionaliteit. Leveranciers hebben naast de landelijk vastgestelde koppelvlakken op het gebied van gemeentelijke basisgegevens specifieke koppelvlakken geïmplementeerd voor uitwisseling van sectorale gegevens. Deze niet gestandaardiseerde koppelvlakken maken het overstappen naar een andere leverancier ingewikkeld en duur. Bij de vervanging van een

applicatie moeten immers alle koppelingen met andere applicaties in kaart worden gebracht en moet de impact van de voorgenomen overstap naar een nieuwe applicatie ingeschat worden. Door de verwevenheid van het gemeentelijk applicatielandschap is de impact van de overgang naar een nieuwe leverancier vaak zo complex en duur dat de business case voor een overstap negatief uitvalt. De complexiteit van het huidige landschap speelt daarmee de huidige leveranciers in de kaart. Dit werkt sterk beperkend voor nieuwe toetreders tot de markt.

Een relatief nieuwe ontwikkeling is het leveren van functionaliteit uit de cloud door softwareleveranciers. Hoewel dit op het eerste oog gemeenten ontzorgt, introduceert het soms ook een verdere afhankelijkheid van de leverancier. Op het moment dat applicaties vanuit een cloud of shared services center constructie worden aangeboden hebben gemeenten als ze daar geen afspraken over hebben gemaakt met de leverancier geen toegang meer tot hun eigen gegevens. Ze zijn daarmee geheel afhankelijk van de leverancier voor het ter beschikking stellen van gegevens aan de gemeente. Ook als de gemeente wel afspraken heeft gemaakt over toegang tot de gegevens blijkt het, mede door de hoge eisen die leveranciers op onder andere informatiebeveiligingsvlak stellen aan het koppelen op hun cloud omgeving lastig. De huidige opzet en implementatie van cloud oplossingen dreigt daarmee tot een nieuwe vorm van vendor lock-in te leiden.

- **Niet meer passende gemeentelijke standaardisatie**
  De afgelopen jaren is landelijk veel tijd en geld geïnvesteerd in het standaardiseren van koppelvlakken tussen gemeentelijke applicaties. Op het gebied van de uitwisseling van basisgegevens zijn stappen gezet, maar op het gebied van de standaardisatie van uitwisseling van sectorale gegevens is deze voortgang slechts beperkt. De inspanning in tijd en geld die in de standaardisatie van de uitwisseling van gegevens zijn gestoken zijn fors terwijl de geboekte resultaten te beperkt zijn. Implementaties van koppelvlakken blijken keer op keer vast te lopen op verschil van interpretatie van het koppelvlak tussen leveranciers. Hierdoor blijft de interoperabiliteit tussen applicaties te beperkt. Toepassing van de huidige StUF-koppelvlakstandaarden hebben de verkokering van applicaties niet kunnen doorbreken.

3. Toekomstig gegevenslandschap

3.1. Inleiding

In het voorgaande hoofdstuk is de huidige inrichting van de gemeentelijke informatiearchitectuur beschreven en zijn de knelpunten van deze inrichting beschreven. De conclusie vanuit de knelpunten is dat het huidig landschap onvoldoende mogelijkheden biedt om de ambities van gemeenten op het vlak van het ondersteunen van burgers, bedrijven en de interne organisatie te realiseren. Processen die op de gegevens worden uitgevoerd zijn niet gestandaardiseerd, niet afzonderlijk en autonoom aan te spreken of uit te voeren, niet herbruikbaar aan te spreken door verschillende actoren en niet eenduidig en onweerlegbaar vastgelegd. De huidige inrichting vraagt veel inspanning om onder andere te voldoen aan de eisen die er vanuit de privacywetgeving aan gemeenten worden gesteld. Om deze doelen wel eenvoudig te kunnen bereiken is het nodig om over te gaan op een andere inrichting van het gemeentelijk gegevenslandschap. De belangrijkste doelen die met de nieuwe inrichting worden nagestreefd zijn:

- Interne en externe transparantie over de verwerking van gegevens
- De burger faciliteren in zijn of haar rol als regisseur van de eigen gegevens
- Gemeenten de regie geven over de eigen gegevens
- Verhogen van de portabiliteit van gegevens
- Compliancy aan vigerende (privacy)wetgeving
- Stimuleren van innovatie van eindgebruikerstoepassingen

Gemeenten moeten groeien naar een situatie waarin burgers eenvoudig kunnen worden gefaciliteerd in hun rechten. Daarnaast moet de gemeente op eenvoudige, en liefst geautomatiseerde wijze, inzage kunnen geven welke medewerker of rol, op welk moment toegang heeft gehad tot persoonsgegevens of deze heeft bewerkt. Per gemeentelijk proces moet worden bepaald welke functionaliteiten moeten worden ondersteund en voor wie (rol). Om de bovenstaande doelen te kunnen realiseren dienen onderstaande elementen van het gegevenslandschap (her)ingericht te worden.

- Scheiding van processen van gegevens;
- Toepassing van privacy-by-design en privacy-by-default concepten;
- Standaardisatie van semantiek, syntax en samenhang van gemeentelijke gegevens;
- Standaardisatie van de toegang tot, en ontsluiting van, gegevens;
- Standaardisatie van autorisatiemechanismen en doelbinding concepten;
- Standaardisatie van logging van verwerkingen;
- Bevraging van gegevens bij de bron.

Door toepassing van het bovenstaande kunnen gegevens, de ontsluiting van gegevens en de verantwoording over de verwerking van de gegevens worden gestandaardiseerd. Hierdoor kunnen gemeenten compliant zijn

aan wet- en regelgeving, kan de burger in staat worden gesteld om regie te voeren over de eigen gegevens en kunnen gegevens zowel in- als extern beter benut worden.

3.2. Scheiding van processen van de procesgegevens

Kern van de nieuwe inrichting van de gemeentelijke informatiearchitectuur is de scheiding van proceslogica en procesgegevens. Daar waar informatiesystemen nu zowel proceslogica als de voor de processen benodigde gegevens bevatten zullen deze in de toekomst hoofdzakelijk proceslogica bevatten. Gegevens die door de proceslogica worden gebruikt zullen in de nieuwe inrichting separaat van de proceslogica opgeslagen en beschikbaar worden gesteld. Een harde scheiding wordt hiermee aangebracht in de uitvoering van de processen en de levering van de gegevens die nodig zijn voor de uitvoering van de processen. Ook worden verantwoordelijkheden anders belegd. Daar waar in de huidige situatie leveranciers van gemeentelijke applicaties voor zowel de inrichting van processen als de modellering van de gegevens verantwoordelijk zijn nemen in de nieuwe inrichting gemeenten de regie ten aanzien van het vormgeven van de gegevens en bijbehorende gegevensontsluiting. Gegevens worden gestandaardiseerd qua semantiek, syntax en samenhang en worden via landelijk gestandaardiseerde diensten[8] (APIs) ontsloten naar afnemers. Leveranciers kunnen op basis van de onder gemeentelijke regie gepubliceerde specificaties via gestandaardiseerde diensten gegevens afnemen en beschikbaar stellen. Leveranciers kunnen op basis van deze gestandaardiseerde APIs procesapplicaties ontwikkelen.

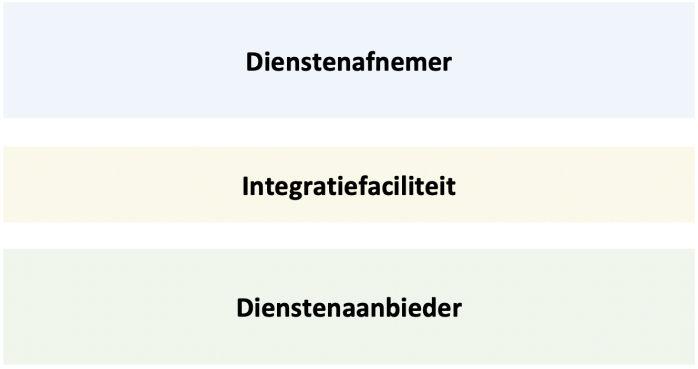
Binnen deze inrichting van het gegevenslandschap nemen gemeenten regie op de modellering en ontsluiting van de gemeentelijke architectuur. Daarnaast liggen ook op het vlak van de procesinrichting kansen voor een nieuwe inrichting. Doordat gemeenten regie nemen over de modellering van de gegevens qua syntax en samenhang en hierdoor standaardisatie van de ontsluiting van deze gegevens afdwingen wordt het eenvoudiger om ook op het gebied van de inrichting van processen standaardisatie door te voeren.

[8] https://www.geonovum.nl/themas/kennisplatform-apis

3.3. Opzet gemeentelijk gegevenslandschap

De voorgaande paragraaf beschrijft de kern van de vernieuwde inrichting van het gegevenslandschap, namelijk het scheiden van processen en gegevens en wijziging van de verantwoordelijkheden ten aanzien van de wijze van modellering en ontsluiting van gegevens.

Hierbij gaat het zowel om de basisgegevens als om de gemeentelijke sectorale gegevens. Deze gegevens worden in de toekomst niet meer door leveranciers, maar onder regie van gemeenten en bronhouders gestandaardiseerd conform landelijk, of sectoraal vastgestelde informatiemodellen. Deze informatiemodellen standaardiseren objecten en attributen zowel qua syntax als onderlinge samenhang. Partijen die diensten aanbieden (dienstenaanbieders) en partijen die deze diensten gebruiken (dienstenafnemers) conformeren zich aan deze informatiemodellen en de daarop gebaseerde standaarden. Een dienstenaanbieder kan iedere organisatie zijn die gegevens of informatie beschikbaar stelt aan andere partijen via APIs die conformeren aan de landelijke afspraken. Voorbeelden van dergelijke dienstenaanbieders zijn de basisregistraties van de GDI en netwerk- en ketenpartijen.



Figuur 4 – Lagen van het gegevenslandschap

In de nieuwe inrichting worden twee rollen onderscheiden; leveranciers van diensten (dienstenaanbieders) en afnemers van diensten (dienstenafnemers) welke onderling worden verbonden door een gestandaardiseerde integratiefaciliteit.

- **Dienstenafnemer** – in deze rol levert een leverancier de gebruikersinterfaces en procesinrichting voor eindgebruikers. De gebruikersinterfaces kunnen bijvoorbeeld de vorm hebben van een mobiele applicatie of traditionele procesapplicatie. De gebruikersinterfaces maken (beperkt) gebruik van bedrijfsregels voor bijvoorbeeld het valideren van de door een eindgebruiker ingevoerde gegevens. Denk hierbij aan bijvoorbeeld de validatie van een ingevoerd BSN of eenvoudige controles van combinaties van ingevulde gegevens. Daarnaast zal er beperkt sprake zijn van de opslag van lokale configuratie en procesgegevens. Voor het ophalen en wegschrijven van de gegevens die gebruikt worden bij de uitvoering van processen worden gestandaardiseerde diensten (APIs) gebruikt die door dienstenaanbieders vanuit de dienstenlaag beschikbaar worden gesteld.

  De dienstenafnemer is verantwoordelijk voor het authenticeren en autoriseren van eindgebruikers en dient in de interne processen te borgen dat enkel geautoriseerde gebruikers gebruik kunnen maken van

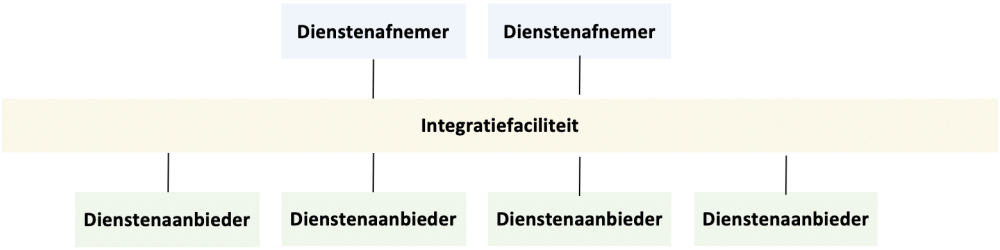
functies van de gebruikersinterfaces. Denk hierbij aan toepassing van DigiD en eHerkenning voor inwoners en ondernemers en Role Based Access (RBAC) voor het verlenen van toegang tot applicatiefuncties.

Bij het gebruik van diensten dient de dienstenafnemer aan te geven voor welk doel en met welke wettelijke grondslag de dienstenafnemer de dienst gaat gebruiken[9];

- **Dienstenaanbieder** – de dienstenaanbieder levert diensten (APIs) aan afnemers. De APIs die door de dienstenafnemer worden aangeboden conformeren zich aan de landelijk gemaakte afspraken ten aanzien van APIs. De dienstenaanbieder geeft organisaties waarmee afspraken zijn gemaakt over het afnemen van diensten toegang tot APIs. Het gebruik van diensten door dienstenafnemers wordt ten behoeve van transparantie en verantwoordingsdoeleinden in logbestanden bijgehouden;

- **Integratiefaciliteit** – de door dienstenaanbieders beschikbaar gestelde diensten worden via een veilige infrastructuur ontsloten naar dienstenafnemers. Diensten worden gepubliceerd binnen een centrale dienstencatalogus welke door ontwikkelaars kan worden geraadpleegd. De infrastructuur die hiertoe wordt gebruikt is opgebouwd uit onder andere bouwstenen van de landelijke Gemeenschappelijke Digitale Infrastructuur (GDI) en collectief opgezette gemeentelijke voorzieningen zoals de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI).

Dienstenafnemers nemen de diensten van dienstenaanbieders af zonder tussenkomst van een centrale component. De verbindingen tussen de dienstenafnemer en dienstenaanbieder zijn peer-to-peer verbindingen.



Figuur 5 - Netwerk van dienstenaanbieders en dienstenafnemers

3.3.1. Privacy en security

Het gemeentelijk gegevenslandschap gaat uit van privacy en security 'by design'. Dit houdt in dat met prioriteit aandacht besteed wordt aan maatregelen die de privacy en de informatiebeveiliging verhogen. De onderstaande maatregelen en uitgangspunten zijn binnen het gegevenslandschap benoemt.

- Geen lokale bijhouding van redundante gegevens maar bevraging bij de bron. Hierdoor wordt de kans op datalekken en onbevoegde verwerkingen van gegevens verkleind doordat gegevens nog maar op één plek worden bijgehouden;

[9] Zie ook 3.3.2 - Doel en grondslag van gegevensverwerkingen

- Diensten worden ‘smal’ gehouden en zijn toegespitst op de levering van gegevens voor een specifiek doel. Hierdoor is gegevens en informatieverstrekking naar afnemers proportioneel;
- Toegang tot diensten wordt verleend onder voorwaarde van doelbinding;
- Logging van alle activiteiten waar men vanuit wetgeving toe verplicht is, of waaraan vanuit de business of beveiliging behoefte aan waardoor auditing op de verwerking van gegevens en diensten mogelijk is;
- Afstemming van het beveiligingsniveau van de diensten met het authenticatiemiddel van de afnemer van de dienst.

Naast deze uitgangspunten vanuit de architectuur worden bij implementatie van een voorziening uiteraard ook specifieke maatregelen genomen. Deze maatregelen zijn op hoofdlijnen beschreven in de Baseline Informatiebeveiliging Gemeenten (BIG)[10].

3.3.2. Doel en grondslag van gegevensverwerkingen

Voor de verwerking van gegevens is een doel en een verwerkingsgrondslag vereist. De grondslag kan bijvoorbeeld een wettelijke verplichting, of toestemming die een persoon heeft afgegeven ten aanzien van de verwerking van zijn of haar gegevens, betreffen. Het doel geeft aan waarvoor de gegevens verwerkt worden. In dit document noemen we de combinatie van doel en grondslag de *doelbinding*. Uitgangspunt binnen het gemeentelijk gegevenslandschap is dat afnemers bij ieder verzoek om gegevens de doelbindingsclaim aangeven voor de verwerking. Indien vanuit een eindgebruikersfunctie gegevens worden ‘verwerkt’[11] dan wordt door deze functie de doelbindingsclaim voor de verwerking vastgelegd. Deze doelbindingsclaim is een verklaring van de afnemer over doel en grondslag van de verwerking. Deze claim wordt bij elke verwerking ten behoeve van transparantie en verantwoordingsdoeleinden in logbestanden wordt vastgelegd. In de logbestanden worden de gebruikte dienst, de eindgebruiker en de doelbindingsclaim vastgelegd. Via deze logging kan achteraf via een audit worden vastgesteld of de verwerking door een afnemer rechtmatig was.

De doelbindingsclaims voor gemeenten worden, tot zover dat mogelijk is, gestandaardiseerd. Dit betreft zowel de verwerkingsgronden die een wettelijke grondslag kennen, voortkomen uit een lokale verordening als de doelbindingen die op basis van een toestemming van een burger verleend kunnen worden. Door deze standaardisatie wordt geborgd dat de verwerkingsgronden tussen gemeenten onderling vergelijkbaar, en juridisch gevalideerd zijn.

[10] https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/
[11] EU-AVG artikel 4: "verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens

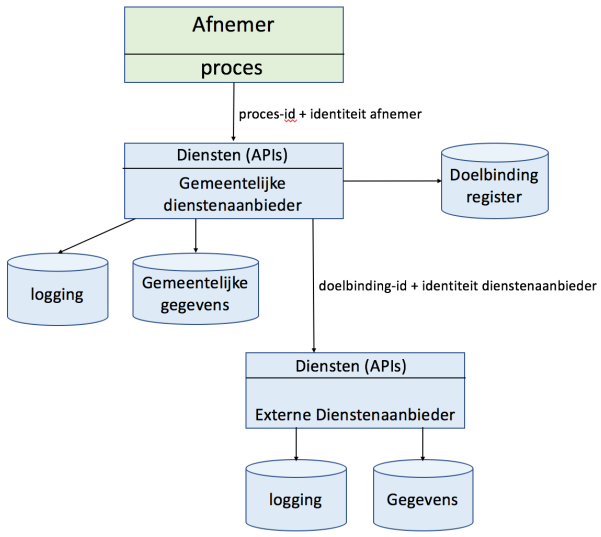
3.3.3. Autorisatie en logging

Uitgangspunt bij de autorisatie in het gegevenslandschap is dat gemeenten intern zelf de authenticatie en autorisatie van gebruikers regelen. Binnen de autorisaties regelt de gemeente welke medewerker, of rol, bevoegd is voor het gebruiken van welke functie van een informatiesysteem. Hierbij heeft het de voorkeur om hiervoor een systeem te implementeren waarbij de autorisaties centraal worden bijgehouden (via een IAM of IdM systeem) zodat grip gehouden kan worden op de verschillende toegekende autorisaties.

De functies van een informatiesysteem die door de gebruiker gebruikt worden dienen een bepaald proces. Het doel en de grondslag van de verwerkingen en gegevens die door dit proces worden verwerkt dient bekend te zijn. De functie is bij iedere verwerking van gegevens via een gegevensdienst (API) verplicht om aan te geven wat de doelbindingsclaim is voor de verwerking. De dienstenaanbieder die de API aanbiedt controleert niet of de doorgegeven doelbindingsclaim klopt, maar slaat deze wel op in logbestanden. Ook de aanroepende functie heeft de plicht de verwerking te loggen. Hierdoor ontstaat een keten van logbestanden die samen een audit log vormen. Op basis van de inhoud van deze audit log kan achteraf bepaald worden of een verwerking rechtmatig was.

Binnen het gegevenslandschap wordt het principe van gedelegeerde autorisatie gebruikt. Indien een dienst gegevens afneemt van een externe dienstenaanbieder dan is het uitgangspunt dat deze externe dienstenaanbieder de API authenticeert op het niveau van de identiteit van de aanroepende afnemer. Er is dus sprake van de aggregatie van identiteit van een specifiek niveau (bijvoorbeeld een gemeentelijke professional) naar een generiek niveau (de gemeente).

Bij een aanroep van een dienstenaanbieder worden als metagegevens onder andere de identiteit van de aanroepende partij en de doelbindingsclaim voor de verwerking doorgegeven. Beide metagegevens worden door de dienstenaanbieder in logging opgenomen zodat verantwoording over het gebruik van de diensten mogelijk is. Onderstaand figuur illustreert het systeem van gedelegeerde autorisatie en logging van verwerkingen.



Een voorbeeld ter illustratie van het bovenstaande:

> *Functionaliteit voor het afgeven van een gemeentelijke parkeervergunning raadpleegt de GBA-V. Bij de aanroep van de GBA-V wordt door gemeente de identiteit van de gemeentelijke professional omgezet naar "gemeente xxx". Door de GBA-V wordt vervolgens geautoriseerd op niveau "gemeente xxx mag inwoners muteren en de rest van Nederland raadplegen". Door de gemeente wordt vastgelegd welke gemeentelijke professional de persoonsgegevens heeft geraadpleegd in het kader van het afgeven van een gemeentelijke parkeervergunning en door de GBA-V wordt vastgelegd dat de gemeente xxx een raadpleging van een persoon heeft gedaan in het kader van het afgeven van een gemeentelijke parkeervergunning.*

Via de inrichting van gedelegeerde autorisatie en expliciete duiding van de doelbindingsclaim door de afnemer kan auditing achteraf plaatsvinden. Toetsing of elke organisatie rechtmatig heeft gehandeld is eenvoudig in te richten. Doelbinding wordt vooraf bepaald en achteraf wordt via audits bepaald of de door een organisatie gebruikte doelbindingsclaims rechtmatig waren; '*vertrouwen vooraf, controle achteraf*'. Dit leidt tot een beheersbare en overzichtelijke inrichting van autorisaties.

De burger wordt via gegevensdiensten (APIs) die de audit logging ontsluiten gefaciliteerd in het inzien van verwerkingen van zijn of haar gegevens. Rechten die de burger heeft gekregen vanuit de AVG, zoals het recht op inzage kunnen hierdoor eenvoudig ingevuld worden. Burgers krijgen direct online inzicht in de actuele verwerking van hun gegevens en de daarvoor gehanteerde doelbindingsclaims.

3.3.4. Standaardisatie van gegevens

Binnen de inrichting van het gegevenslandschap nemen gemeenten de regie over de standaardisatie van de gemeentelijke gegevens. Daar waar anno 2018 slechts een klein deel van de gemeentelijke gegevens via informatiemodellen is gestandaardiseerd (RSGB, RGBZ, ImZTC, ImGeo en Raadsinformatie) worden in de nieuwe inrichting alle gegevens gestandaardiseerd via informatiemodellen. Dit betekent dat informatiemodellen ontwikkeld worden voor bijvoorbeeld het sociaal- en het belastingen domein en dat aansluiting gezocht wordt bij bestaande informatiemodellen in bijvoorbeeld de openbare ruimte zoals het IMBOR[12]. Het is mogelijk dat binnen omvangrijke domeinen een opsplitsing naar sub-domeinen of thema's wordt gemaakt en daardoor binnen een domein meerdere informatiemodellen ontstaan. Denk hierbij bijvoorbeeld aan het sociaal domein, dit domein omvat een groot aantal taken, opsplitsing in kleinere delen ligt voor de hand. Te denken valt dan bijvoorbeeld aan aparte informatiemodellen voor de Jeugdzorg, Maatschappelijke Ondersteuning en Werk en Inkomen. Onderling worden deze modellen wel verbonden om silovorming op gegevensmodelleringsgebied binnen domeinen te voorkomen.

Door de standaardisatie van gegevens en onderlinge samenhang via informatiemodellen is ook standaardisatie van de toegang tot gegevens via APIs mogelijk. Deze standaardisatie van gegevensontsluiting draagt bij aan het op een eenduidige manier worden vormgegeven van processen, onafhankelijk van onderliggende leverancier-specifieke applicaties.

[12] https://www.geonovum.nl/geo-standaarden/overzicht-informatiemodellen-nen3610-familie/informatiemodel-beheer-openbare-ruimte

De vraag of, en welke, processen worden gestandaardiseerd qua inrichting zal vanuit de wensen van gemeenten moeten worden beantwoord. Op het gebied van Werk en Inkomen en Belastingen zijn de eerste initiatieven om te komen tot een dergelijke standaardisatie al gestart door gemeenten[13].

3.3.5. Historie van gegevens

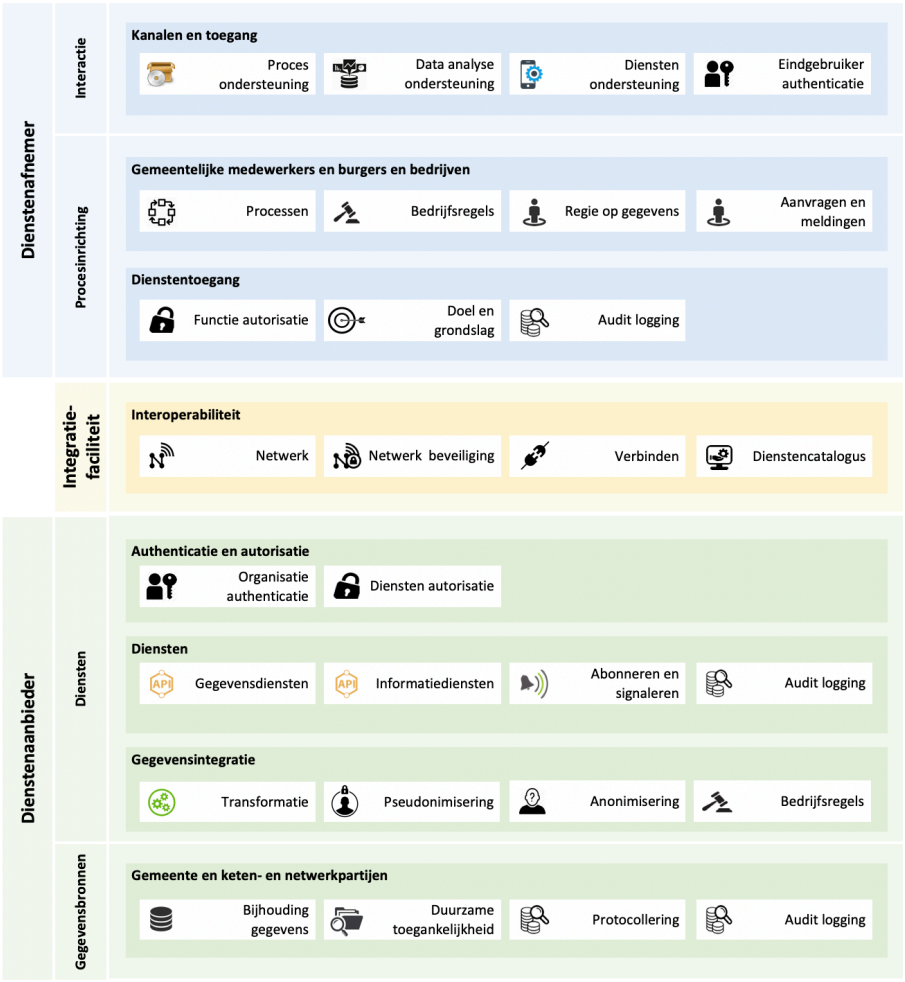
In de voorgaande paragrafen is beschreven dat gegevens ontsloten worden via door informatiemodellen gestandaardiseerde APIs. Dit geldt zowel voor gemeentelijke basis- als sectorale gegevens[14]. Binnen de informatiemodellen worden afspraken gemaakt over de wijze waarop gegevens worden gemodelleerd. Een belangrijk aspect bij deze modellering is de historie van objectgegevens. De historie van een object kent twee 'werkelijkheden': de formele historie (dat wat wijzigt in de registratie) en de materiële historie (dat wat wijzigt in de werkelijkheid). Het is voor veel registraties van belang dat elke relevante toestandsverandering van een object, zowel formeel als materieel, in de registratie van het object wordt opgenomen. Deze registratie van de toestand van een object door de tijd heen maakt bevraging op peildatum mogelijk, hetgeen voor veel afnemers randvoorwaardelijk is. Indien een bron dit ondersteund dan verdwijnt ook de noodzaak voor een afnemer om deze gegevens redundant op te slaan. Via de formele- en materiële historie van een object kunnen afnemers dan immers de gegevens van het object op ieder gewenst moment in de tijd opvragen bij de bron. Indien formele- en materiële historie niet bijgehouden worden terwijl daar wel vraag naar is dan zal bij afnemers waarvoor deze historie van belang is de noodzaak blijven bestaan om lokaal gegevens redundant bij te houden.

Kanttekening hierbij is dat niet alle objectregistraties op dezelfde manier met historie om hoeven te gaan - informatieobjecten hebben bijvoorbeeld een geheel eigen systematiek met Record Management, en er zijn ook objectregistraties waar het bijhouden van formele en materiele historie minder van belang is. Daar waar formele en materiele historie wel van belang is wordt de vastlegging van deze historie gestandaardiseerd.

[13] http://www.gbi-gemeenten.nl/
[14] Zie ook paragraaf 0

4. Uitwerking gemeentelijk gegevenslandschap

Onderstaand figuur toont het uitgewerkte model van het gemeentelijk gegevenslandschap. In dit model gebruiken gemeenten, keten- en netwerkpartijen en burgers en bedrijven (eindgebruikers) gebruikersinterfaces die geboden worden vanuit proces- en analysesystemen en mobiele applicaties. De gegevens die door deze systemen worden verwerkt worden via een veilige landelijke infrastructuur via gestandaardiseerde diensten (APIs) afgenomen van dienstenafnemers.



Figuur 6 – Gemeentelijk gegevenslandschap

VNG Realisatie
Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

Onderstaande paragrafen beschrijven de verschillende onderdelen van het gemeentelijk gegevenslandschap op hoofdlijnen.

4.1. Interactie

De interactielaag is verantwoordelijk voor het ontsluiten van de gebruikersinterfaces naar de eindgebruiker. Deze eindgebruiker kan een medewerker van de gemeente zijn, maar ook een inwoner of ondernemer. Het type systeem waarmee de interactie met de eindgebruiker wordt vormgegeven hangt af van het type eindgebruiker. Een medewerker van de gemeente zal in de regel gebruik maken van een gemeentelijk processysteem, zoals bijvoorbeeld een uitkeringentoepassing, terwijl inwoners en ondernemers de interactie met de gemeente meestal via mobiele applicaties vormgegeven zal worden.

4.1.1. Procesondersteuning

Ondersteuning voor de gemeentelijke processen zoals het heffen van belastingen, het uitkeren van uitkeringen, het ondersteunen van burgers die maatschappelijke ondersteuning nodig hebben en het onderhouden van de openbare ruimte wordt geboden door informatiesystemen. Deze informatiesystemen houden slechts minimaal procesgegevens bij. Gegevens worden in beginsel door de informatiesystemen uit de bron opgehaald. Er zijn ook scenarios denkbaar waarbij gegevens wel binnen een procesondersteunend informatiesysteem worden vastgelegd:

- Indien geen bronsysteem beschikbaar is en er geen sprake is van (potentieel) meervoudig gebruik van de gegevens;
- Indien gegevens nodig zijn voor de correcte werking van het informatiesysteem maar niet binnen de uitvoering van de processen worden gebruikt. Denk hierbij bijvoorbeeld aan configuratiegegevens ten aanzien van gebruikers en systeeminstellingen.

Procesondersteunende informatiesystemen worden primair gebruikt door medewerkers van de gemeente. Het is echter ook mogelijk met name ondernemers procesondersteunings systemen gebruiken in combinatie met gegevens van de overheid. Denk hierbij bijvoorbeeld aan een architectenbureau dat ontwerpsoftware (CAD-systeem) gebruikt en daarbij gegevensbronnen van de overheid ontsluit.

4.1.2. Data analyse ondersteuning

Ondersteuning voor de de analyse van gemeentelijke gegevens en, of in combinatie met, gegevens van keten- en netwerkpartijen via onder andere beschrijvende en inferentiële statistiek. Ondersteuning wordt geboden door gespecialiseerde informatiesystemen. Door gemeenten worden onder andere data warehouse- en analytics systemen ingezet om rapportages en trendanalyses mee te genereren. Deze systemen maken gebruik van grote hoeveelheden, vaak samengestelde, gegevens. Het gegevenslandschap faciliteert deze systemen via specifieke gegevensdiensten die de gegevens leveren aan de afnemer. Het streven is om real-time analyses op gegevens uit te kunnen voeren. Daar waar dit wegens technologische of technische beperkingen nog niet mogelijk is wordt een (asynchrone) levering van gegevens aan afnemers gefaciliteerd. Dit houdt in dat een vraag om een set van gegevens wordt uitgevoerd op een moment dat dit voor het gegevenslandschap opportuun is. Voor gegevensvragen die grote sets van gegevens opleveren kan dit betekenen dat de vraag, in verband met belasting van de infrastructuur, na kantoortijd wordt uitgevoerd. Terugkoppeling van de resultaten vindt plaats op een wijze die in overeenstemming is met de gevoeligheid van

de gegevens. Voor gegevenssets die geen privacygevoelige gegevens bevatten kan dit bijvoorbeeld via een open data portaal of (s)ftp-verbinding en voor andere gegevens zal dit via een beveiligd portaal of 'zandbak' omgeving verlopen.

De gegevensdiensten die gegevens bieden voor analysediensten zijn in staat om op aanvraag van de afnemer de gegevens te anonimiseren of te pseudonimiseren.

Data analyse systemen worden gebruikt door medewerkers van de gemeente maar kunnen ook door inwoners en ondernemers worden gebruikt. De gegevens die binnengemeentelijk worden gebruikt voor data analyse zullen veelal closed data zijn die vanuit het oogpunt van de privacy niet met derden gedeeld worden. De overheidsdata die door ondernemers en burgers gebruikt worden voor data analyse zijn de open data[15] die door de verschillende overheden ter beschikking worden gesteld.

4.1.3. Diensten ondersteuning

Het kenmerk van applicaties die diensten ondersteunen is dat ze gericht zijn op een specifiek stuk dienstverlening, ontworpen worden vanuit de vraag van een eindgebruiker en relatief snel kunnen worden ontwikkeld. Deze applicaties zijn voor het overgrote deel mobiele applicaties. Onder een mobiele applicatie – of app - wordt verstaan software die specifiek gemaakt is voor het gebruik op mobiele apparaten (als tablets, smartphones, wearables, etc.) en responsive webapplicaties[16]. Daar waar vroeger werd gesproken over e-formulieren als gebruikersinterface voor burgers en bedrijven om diensten en producten mee aan te vragen wordt deze functionaliteit in het gegevenslandschap gepositioneerd als een mobiele applicatie. E-formulieren worden daarmee dus niet meer als apart type gebruikersinterface onderkend.

Voorbeeld van de toepassing van een mobiele applicatie voor gemeentelijke professionals is een app die BOA's informeert over situaties die om aandacht vragen. De BOA kan via een app geïnformeerd worden over de situatie en kan ter plekke een rapport opstellen en foto's van de situatie toevoegen. Ook dergelijke apps maken gebruik van de gegevensdiensten van het gemeentelijk gegevenslandschap om gegevens mee op te halen en weg te schrijven. Voorbeeld van een app voor burgers is een app op het gebied van parkeren. Als de gemeente de gegevens van beschikbare vrije parkeerplaatsen in de gemeente als gestandaardiseerde open data aanbiedt dan kunnen leveranciers deze gegevens gebruiken om apps mee te ontwikkelen. Deze leveranciers kunnen bijvoorbeeld de gps-locatie van het mobiele device van de burger combineren met de door de gemeente ter beschikking gestelde open data om zo de burger te helpen met het vinden van een beschikbare parkeerplek in de directe omgeving.

Uitgangspunt is dat apps geen gegevens op het mobiele apparaat opslaan. Apps bevatten enkel configuratiegegevens die nodig zijn voor de werking van de app. Denk hierbij bijvoorbeeld aan configuratiegegevens. Mobiele applicaties dienen verder te voldoen aan de eisen die gesteld worden vanuit de Europese richtlijn voor de toegankelijkheid van websites en mobiele applicaties[17].

[15] https://nl.wikipedia.org/wiki/Open_data
[16] Bron: GEMMA Katern Mobiel (https://www.gemmaonline.nl/index.php/MOB_Inleiding)
[17] https://www.forumstandaardisatie.nl/standaard/digitoegankelijk-en-301-549-met-wcag-20

4.1.4. Eindgebruiker authenticatie

Het is de verantwoordelijkheid van de dienstenafnemer om daar waar nodig gebruikers te authenticeren. De dienstenafnemer dient hierbij te borgen dat het gebruikte authenticatiemiddel past bij het betrouwbaarheidsniveau van de dienst of functie die de gebruiker gaat gebruiken. Indien binnen een functie bijvoorbeeld jeugdzorggegevens worden verwerkt dan zal een hoger authenticatieniveau vereist zijn dan als alleen 'gewone' persoonsgegevens verwerkt worden. In het geval dat jeugdzorggegevens verwerkt worden zal naar verwachting gezien de gevoeligheid van de gegevens een middel op niveau 'Hoog' vereist zijn terwijl bij gewone persoonsgegevens een middel op niveau 'Laag' of 'Substantieel' voldoende zal zijn.

De beschikbare authenticatiemiddelen voor inwoners worden vastgesteld in het landelijke eID-programma[18]. Het gaat hierbij om door de overheid verschafte middelen op de niveaus laag, substantieel en hoog en één of meer private middelel op niveaus substantieel en hoog. De middelen die door de overheid voor het BSN-domein worden verschaft betreffen de DigiD middelen. De private middellen voor het BSN-domein moeten nog worden aanbesteed[19]. Voor bedrijven, en ook voor medewerkers van de gemeente, kan gebruik worden gemaakt van een eHerkenningsmiddel[20] voor authenticatie. De eHerkenningsmiddelen zijn op verschillende betrouwbaarheidsniveaus beschikbaar.

Naast de landelijke authenticatiemiddelen heeft de gemeente voor de authenticatie van de binnen de gemeente werkzame personen uiteraard de mogelijkheid om hiervoor een lokaal identiteit management oplossing te gebruiken.

4.2. Procesinrichting

4.2.1. Processen

De procesondersteuning faciliteert de gemeente in het inrichten van haar processen. Wet- en regelgeving is voor alle gemeenten gelijk en de processen zijn dan ook op hoog niveau grotendeels vergelijkbaar. Hierdoor is het mogelijk om standaardisatie op het gebied van gemeentelijke processen door te voeren. Met de invoering van het nieuwe gemeentelijk gegevenslandschap is dit ook het nadrukkelijke streven. Het motto hierbij is standaardisering waar het kan, en verschil in uitvoering aanbrengen waar nodig of gewenst. Verschil in de uitvoering kan bijvoorbeeld ontstaan als een gemeente specifiek lokaal beleid opstelt ten aanzien van de uitvoering van taken, de zogenaamde 'couleur locale'.

Gebruik van gestandaardiseerde gegevensdiensten door processen zal naar verwachting leiden tot convergentie van de inrichting van de processen en procesapplicaties.

4.2.2. Bedrijfsregels

Binnen de uitvoering van processen worden bedrijfsregels toegepast. Een voorbeeld van een dergelijke regel is het controleren van de syntactische juistheid van een ingevoerd BSN. Een ander voorbeeld is het op basis van zaaktype eigenschappen nagaan of alle benodigde documenten bij een zaakstatus aanwezig zijn. Er zijn geen vastgestelde regels ten aanzien van welke bedrijfsregels in de procesinrichting gehanteerd mogen

[18] https://www.digitaleoverheid.nl/dossiers/eid/
[19] Situatie april 2019
[20] https://www.digitaleoverheid.nl/dossiers/eherkenning/

worden. Het is wel het overwegen waard om bedrijfsregels die dicht op de gegevens moeten worden uitgevoerd binnen de diensten op te nemen die de gegevens leveren. Op die manier wordt geborgd dat deze regels altijd worden uitgevoerd als gegevens uit een bron worden verwerkt.

Een overweging om bepaalde bedrijfsregels binnen de procesinrichting op te nemen is de klantervaring tijdens het uitvoeren van het proces. Voor de eindgebruiker is het bijvoorbeeld prettiger om bij de invoer van een foutief BSN direct een foutmelding te krijgen in plaats van dat deze melding pas naar voren komt nadat een dienst uit de dienstenlaag wordt aangeroepen. Uiteraard moet de dienstenlaag wel borgen dat deze controle op geldigheid wordt uitgevoerd, deze laag heeft immers de verantwoordelijkheid om de kwaliteit van de gegevens te borgen. Het is dus mogelijk dat identieke bedrijfsregels zowel binnen de proces- als dienstenlaag wordt geimplementeerd.

4.2.3. Regie op gegevens

Het dienstenaanbod richting burgers en bedrijven omvat een aantal diensten op het gebied van regie op gegevens door de burger, ook wel Persoonlijk Data Management (PDM) genoemd. Vanuit privacy wet- en regelgeving (Wbp, AVG) hebben burgers onder andere recht op inzage en correctie van hun gegevens en recht op het inzien van de verwerkingen van hun gegevens door gemeenten en ketenpartijen. Vanuit het gegevenslandschap worden deze rechten gefaciliteerd via:

- Diensten waarmee inzage gegeven kan worden in de ‘eigen’ gegevens;
- Diensten waarmee inzage wordt gegeven in het gebruik van gegevens van de burger door afnemers. Deze afnemers kunnen binnengemeentelijke afnemers zijn, maar ook keten- en netwerkpartijen;
- Diensten waarmee de burger de gemeente kan verzoeken om gegevens die naar zijn of haar mening incorrect zijn te veranderen;
- Diensten waarmee de burger regie kan voeren op de uitwisseling van zijn haar gegevens tussen gemeenten en keten partijen daar waar deze uitwisselingen bovenwettelijk zijn. De burger kan per gegevensuitwisseling aangeven met welke partijen de gemeente deze partijen gegevens mag delen;
- Diensten waarmee de burger actief geïnformeerd wordt op het moment dat een verwerking van zijn of haar gegevens plaatsvindt.

Door invulling te geven aan bovenstaande rechten verbetert de transparantie en daarmee het vertrouwen in de overheid, neem de kwaliteit van gegevens toe en wordt de informatiepositie van de burger versterkt. Dit persoonlijk datamanagement (PDM) draagt bij aan transparantie, inzage en correctie, digitale zelfbeschikking, privacy, dataminimalisatie, de kwaliteitsverbetering van gegevens en zelfredzaamheid van mensen. Daarmee is PDM tevens een uitwerking van de beginselen zoals die gehanteerd worden bij *privacy-by-design* en *security-by-design*.

4.2.4. Aanvragen en meldingen

Inwoners en ondernemers hebben de mogelijkheid om meldingen te doen bij de gemeente en producten aan te vragen. Denk hierbij bijvoorbeeld aan het melden van een niet werkende lantarenpaal via een melding openbare ruimte (MOR) of het aanvragen van een uittreksel uit de gemeentelijke basisregistratie personen. Door de gebruikers wordt over het algemeen de website van de gemeente of een mobiele app gebruikt om toegang te krijgen tot deze processen. Voor meldingen geldt daarbij dat deze veelal op anonieme basis kunnen worden gedaan zodat authenticatie van de gebruiker niet nodig is. Daar waar het wel van belang is om de identiteit van de gebruiker te kennen worden deze processen pas beschikbaar gesteld als de gebruiker zich via een middel heeft geauthenticeerd.

Voor zowel het doen van meldingen als het aanvragen van producten geldt dat deze processen zeer geschikt zijn voor landelijke standaardisatie.

4.2.5. Functie autorisatie

Op het moment dat een gebruiker een functie wil gebruiken moet bepaald worden of de gebruiker hiertoe de vereiste rechten heeft. Deze bepaling start met het bepalen van de identiteit van de gebruiker via een authenticatiemiddel. Nadat de identiteit van de eindgebruiker met het voor de functie vereiste betrouwbaarheidsniveau is bepaald dient te worden bepaald welke rechten de gebruiker heeft ten aanzien van de beschikbare functies. Dit kan worden bepaald door gebruikers aan functies toe te kennen, of door gebruikers aan rollen toe te kennen en vervolgens rollen aan functies toe te kennen. Het laatste staat bekend als Role Based Access Control (RBAC)[21].

Inregelen van autorisaties voor gebruikers en rollen vindt bij voorkeur op een centrale plek in de organisatie plaats. Het centraal inrichten van toegangscontrole op functieniveau geeft de meeste waarborgen voor het up-to-date houden van autorisaties.

Voor het inrichten van autorisaties kan gebruik worden gemaakt van een Identity en Access Management (IAM) tool.

4.2.6. Doel en grondslag

Op het moment dat een functie door een geauthenticeerde en geautoriseerde eindgebruiker wordt gestart worden door deze functie gegevens verwerkt. Denk bijvoorbeeld aan een functie die persoonsgegevens bijwerkt in de basisregistratie personen of een functie die ten behoeve van de gemeentelijke belastingen de gegevens van een kadastraal perceel ophaalt. Voor iedere verwerking van gegevens geldt dat de gemeente een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel moet hebben voor de gegevensverwerking. De voorwaarde ‘welbepaald’ houdt in dat de doelomschrijving duidelijk moet zijn. Het moet tijdens het verzamelproces een kader bieden waaraan getoetst kan worden of de gegevens wel of niet nodig zijn voor dat doel. Daarnaast moet er ook sprake zijn van een wettelijke grondslag voor de verwerking. Voorbeelden van een dergelijke grondslag zijn de toestemming van een betrokkene en een wettelijke verplichting.

Bij het gebruik van een functie dient aangegeven te worden voor welk doel en met welke grondslag de functie wordt gebruikt. De combinatie van doel en grondslag wordt in dit document aangeduid als de ‘*doelbindingsclaim’*. Via deze doelbindingsclaim wordt aangegeven wat het verwerkingsdoel bij het gebruik van de functie is. Een functie kan worden gebruikt ten behoeve van meerdere doelbindingsclaims. Het is de verantwoordelijkheid van de dienstenafnemer om bij het gebruik van een functie de juiste doelbindingsclaim te hanteren. De dienstenafnemer dient interne processen ingericht te hebben waarmee geborgd wordt dat enkel bevoegden gebruik kunnen maken van functies.

De doelbindingsclaims worden landelijk gestandaardiseerd en bijgehouden in een verwerkingenregister. Het is de verplichting van een dienstenafnemer een dergelijk register bij te houden en te hanteren. Voor een aantal doelbindingsclaims uit het verwerkingenregister zal gelden dat de grondslag voor de verwerking de expliciete toestemming van de burger betreft. Indien een dienstenafnemer van een dergelijke doelbindingsclaim gebruik

[21] https://nl.wikipedia.org/wiki/Role-based_access_control

maakt dan zal deze onomstotelijk moeten kunnen aantonen dat deze expliciete toestemming van de burger voor de verwerking van de gegevens ten tijde van de verwerking verleend was. De burger kan deze toestemmingen beheren, en dus ook verwijderen, via de regie op gegevens diensten.

4.2.7. Audit logging

Een essentieel onderdeel van het gebruik van diensten door eindgebruikers en het aanroepen van diensten van dienstenaanbieders betreft het loggen van deze verwerkingen. Ten behoeve van transparantie naar burger en bestuur en ook ten behoeve van audits is de dienstenafnemer verplicht om het gebruik van functies en het aanroepen van diensten vast te leggen in logbestanden. In de logbestanden dient naast een datum en tijd opgenomen te worden welke functie of dienst gebruikt is, wie de eindgebruiker is die de dienst of functie gebruikt en wat de gehanteerde doelbindingsclaim is.

Logbestanden worden richting de burger gebruikt voor het inzage geven in verwerkingen van zijn of haar gegevens, en ze worden gebruikt om achteraf te bepalen of een gemeente rechtmatig heeft gehandeld. De integriteit van logbestanden dient daarom bewaakt te worden. Mutaties in logbestanden moeten voorkomen worden, en logbestanden dienen duurzaam toegankelijk gehouden te worden[22].

4.3. Integratiefaciliteit

4.3.1. Netwerk

Diensten worden naar burgers en bedrijven en gemeenten en ketenpartners ontsloten via een netwerk infrastructuur. Afhankelijk van de diensten die geboden worden is dit een privaat of een openbaar netwerk. Netwerken die gebruikt kunnen worden voor het benaderen van diensten zijn onder andere internet en Diginetwerk koppelnetwerken zoals GGI-Netwerk. Door burgers en bedrijven zal met name gebruik worden gemaakt van Internet voor het benaderen van de gemeentelijke diensten. Door gemeenten en ketenpartners kan ook gebruikt worden gemaakt van Diginetwerk koppelnetwerken. De keuze voor een netwerk is mede afhankelijk van het betrouwbaarheidsniveau van de dienst die wordt afgenomen. Het betrouwbaarheidsniveau van een dienst wordt bepaald door de dienstenaanbieder en is onder andere afhankelijk van de gevoeligheid van de gegevens die via de dienst worden verwerkt en de integriteit van gegevens. Diensten die open data verwerken kennen vanuit het oogpunt van gevoeligheid van gegevens een laag betrouwbaarheidsniveau. Deze diensten kunnen aan externe afnemers beschikbaar worden gesteld via Internet. Indien een afnemer ook hoge eisen stelt aan de integriteit van de open gegevens, en zeker wil weten dat gegevens tijdens transport niet gewijzigd zijn dan kan gekozen worden voor transport via een veiliger netwerk zoals een Diginetwerk koppelnetwerk.

4.3.2. Netwerkbeveiliging

Het beveiligen van de communicatienetwerken maakt deel uit van de bredere informatiebeveiliging in het algemeen omschreven als het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit of vertrouwelijkheid en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de

[22] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf

continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

Om Informatiebeveiliging op de digitale infrastructuur in de moderne informatie maatschappij effectief te doen zijn is het inzetten van de “klassieke” preventieve middelen zoals firewalls, antivirus, mail filtering, indringer detectiesystemen, etc. niet meer voldoende. Continue monitoring en analyse van acties en gedrag op de digitale infrastructuur is daarbij een noodzakelijke aanvullende maatregel om voldoende weerbaar te zijn tegen de dreigingen op de informatieveiligheid. De geldende wet- en regelgeving vormt een belangrijke driver voor het nemen van deze aanvullende maatregel.

Het component ‘Netwerkbeveiliging’ geeft invulling aan de continue monitoring en analyse van het dataverkeer over het netwerk en de daaraan gekoppelde signaleringsfuncties. Via het GGI-Veilig portfolio kan invulling worden gegeven aan de preventieve als detectieve maatregelen op het gebied van netwerk beveiliging.

4.3.3. Verbinden

Een essentieel onderdeel van de integratiefunctionaliteit is de verbindingsfunctie. Belangrijkste verantwoordelijkheid van de verbindingsfunctie is het tot stand brengen van een veilige verbinding tussen de aanbieder- en afnemer van de dienst zodat een afnemer op een veilige wijze de diensten van een aanbieder kan aanroepen.

Deze functie maakt gebruik van de dienstencatalogusfunctie om te bepalen waar een aanbieder van een dienst zich bevindt. Vervolgens maakt de functie voor het opbouwen van de verbinding tussen aanbieder en afnemer gebruik van client en server certificaten (tweeweg TLS). Voor het transport van de gegevens tussen de aanbieder en de afnemer wordt gebruik gemaakt van de netwerkfunctie .

4.3.4. Dienstencatalogus

Het volledige dienstenaanbod dat beschikbaar is voor dienstenafnemers is vastgelegd in een centrale dienstencatalogus. In deze catalogus worden de diensten vastgelegd die door dienstenaanbieders worden aangeboden voor gebruik. De diensten worden in deze catalogus beschreven conform de daartoe binnen de overheid vastgestelde Open API Strategie (OAS) versie 3.x. De dienstencatalogus is gericht op ontwikkelaars van afnemende applicaties of processen. Via de dienstencatalogus wordt aan afnemers informatie geboden over de beschikbare diensten, en worden per dienst de authenticatiemogelijkheden en testfaciliteiten beschreven. Via de servicecatalogus kunnen potentiële afnemers een dienst testen zodat ze de werking van de dienst in de praktijk kunnen uitproberen.

De dienstencatalogus biedt de volgende diensten aan ontwikkelaars:

- Overzicht van diensten (APIs)
- API life-cycle informatie
- Criteria voor gebruik (API key, PKI, ..)
- API documentatie
- Test / uitprobeer faciliteit

De dienstencatalogus heeft enkel design-time een functie. Op run-time niveau, dus tijdens de uitvoering van processen, wordt de dienstencatalogus niet gebruikt. De centrale dienstencatalogus vormt dus geen ‘single point of failure’ in de communicatie tussen dienstenafnemer en dienstenaanbieder.

4.4. Authenticatie en autorisatie

Dienstenaanbieders die diensten beschikbaar stellen aan dienstenafnemers hebben de verantwoordelijkheid om transparantie te kunnen bieden over welke diensten door wie gebruikt zijn. Tevens dienen zij te kunnen verantwoorden welke gegevens door een dienst geleverd zijn. Dienstenafnemers dienen van een dienstenafnemer onomstotelijk de identiteit vast te stellen en zij dienen per afnemer te bepalen of deze wel of niet geautoriseerd is voor het gebruik van een dienst. Alle verzoeken tot het gebruik van een dienst en het daadwerkelijke gebruik van diensten dient in het kader van transparantie en auditing vast gelegd te worden in logbestanden.

4.4.1. Organisatie authenticatie

Een dienstenaanbieder stelt diensten ter beschikking aan dienstenafnemers. Het is van belang dat bij het gebruik van een dienst onomstotelijk vaststaat wat de identiteit de identiteit van de dienstenafnemer is. Het leveren van een dienst aan een verkeerde dienstenaanbieder zou immers kunnen leiden tot een datalek, misbruik van gegevens en potentieel schade voor ondernemers en inwoners.

Binnen de overheid wordt voor de identificatie van organisaties gebruik gemaakt van PKIoverheid-certificaten. Het PKIoverheid-certificaat is een computerbestand dat fungeert als een digitaal paspoort. Een PKIoverheid services certificaat is gebonden aan een organisatie en wordt uitgegeven aan apparaten of servers, of groepen individuen. Het certificaat wordt gebruikt om de communicatie te beveiligen tussen elektronische overheidsapplicaties en diensten. Door het toepassen van PKIoverheid-certificaten tussen dienstenaanbieders en dienstenafnemers weten zowel de dienstenaanbieder als de dienstenafnemer zeker dat ze met de juiste partij communiceren.

Uitgangspunt in het gegevenslandschap is dat voor de communicatie tussen dienstenaanbieders en dienstenafnemers gebruik wordt gemaakt van PKIoverheid services certificaten voor zowel de aanbieder als de afnemer (TLS met cliënt authenticatie).

4.4.2. Diensten autorisatie

Binnen het gegevenslandschap wordt het principe van gedelegeerde autorisatie gebruikt. Indien een dienstenafnemer gegevens nodig heeft van een dienstenaanbieder dan is het uitgangspunt dat deze dienstenaanbieder deze aanvraag niet opnieuw autoriseert op het niveau van de identiteit van de eindgebruiker maar in plaats daarvan de autorisatie uitvoert op het niveau van de identiteit van de aanroepende dienstenaanbieder. De dienstenaanbieder autoriseert dus haar diensten op het niveau van een organisatie. Er is hierbij sprake van de aggregatie van identiteit van een specifiek niveau (bijvoorbeeld een gemeentelijke professional of burger) naar een generiek niveau (de gemeente). De autorisatie wordt afgeleid vanuit afspraken die tussen de dienstenaanbieder en dienstenafnemer zijn gemaakt ten aanzien van de uitwisseling van gegevens. Deze afspraken, ook wel gegevensleveringsovereenkomsten (GLO) genoemd, dienen door de dienstenaanbieder vertaald te worden naar autorisatieprofielen. Per organisatie kan in een autorisatieprofiel worden vastgelegd voor welke diensten een geauthenticeerde dienstenafnemer is geautoriseerd. Enkel de diensten waarvoor de dienstenafnemer is geautoriseerd kunnen door de dienstenafnemer worden gebruikt.

4.5. Diensten

De diensten die door een dienstenaanbieder worden geboden worden gepubliceerd via de dienstencatalogus en in de vorm van APIs ontsloten. De diensten (APIs) worden via in REST/JSON en, indien nodig SOAP/XML-interfaces en worden beschreven via het OAS 3.x protocol. Diensten die in de vorm van REST/JSON worden aangeboden conformeren zich aan de standaarden die hier landelijk voor gelden[23].

4.5.1. Gegevensdiensten

Diensten die gericht zijn op het ontsluiten en bijwerken van gegevensverzamelingen (CRUD-functionaliteit[24]) worden in dit document aangeduid als *gegevensdiensten*. Een voorbeeld van een gegevensdienst is een dienst waarmee een klant wordt toegevoegd aan een klantenregistratie.

Een gegevensdienst heeft als kenmerk dat het als één geheel wordt uitgevoerd en dient te voldoen aan de ACID-eigenschap[25] voor diensten. Dit staat voor **a**tomair, **c**onsistent, **i**soleerbaar en **d**uurzaam.

- Atomair; de dienst slaagt of faalt als een geheel. Indien een dienst meerdere taken verricht dan slagen deze taken dus allemaal, of ze falen allemaal.
- Consistent; de dienst creëert gegevens die voldoen aan de consistentieregels. Als een fout optreedt dan worden gegevens in hun oude staat teruggebracht.
- Isoleerbaar; een dienst die wordt uitgevoerd maar nog niet is afgerond mag geen invloed hebben op andere diensten die worden uitgevoerd.
- Duurzaam; gegevens worden op een dusdanige wijze opgeslagen dat deze na een systeemcrash of herstart in hun correcte staat beschikbaar zijn.

De gegevensdiensten definiëren bij de uitvoering van de dienst de grenzen van de uit te voeren transactie. De dienst start en beëindigd dus zelf de transactie waarin de dienst wordt uitgevoerd.

4.5.2. Informatiediensten

Diensten die gegevens uit gegevensverzamelingen interpreteren, gegevens combineren en op basis daarvan informatie leveren worden in dit document *informatiediensten* genoemd. Een voorbeeld van een informatiedienst is een dienst die op basis van een BSN als resultaat geeft of de betreffende persoon ouder is dan 18. Informatiediensten hebben als voordeel dat ze het mogelijk maken om proportioneel en subsidiair gegevens te verstrekken. Een drankenwinkel heeft bijvoorbeeld als wettelijke verantwoordelijkheid om na te gaan of iemand ouder dan 18 is voordat aan diegene alcoholhoudende drank wordt verkocht. Een simpel ‘ja, ouder dan 18’ of ‘nee, jonger dan 18’ voldoet hierbij. De betreffende winkelier hoeft niet de actuele leeftijd of de geboortedatum te kennen.

[23] Binnen het landelijk Gemeenschappelijke Afspraken Berichten (GAB) overleg is een voorstel ingebracht ten aanzien van de te volgen API en URI-strategie. Zolang deze strategie nog niet landelijk is vastgesteld wordt de DSO API en URI-strategie van toepassing verklaard.
[24] https://nl.wikipedia.org/wiki/CRUD
[25] ISO/IEC 10026-1:1992 Section 4

4.5.3. Abonneren en signaleren

Sommige dienstenaanbieders bieden de mogelijkheid om abonnementen af te sluiten op wijzigingen in een gegevensbron. Een afnemer kan bij de bron aangeven op welke gegevens of gegevensgroepen een abonnement wordt afgesloten. De dienstenaanbieder borgt daarbij dat de afnemer enkel abonnementen op gegevens waarvoor de afnemer is geautoriseerd kan afnemen. Op het moment dat er een wijziging optreedt in de gegevensbron zal de dienstenaanbieder iedere abonnee van die wijziging een notificatiebericht sturen. Het notificatiebericht bevat naast sleutelgegevens van het object waarover de notificatie gaat en de context van de notificatie (wat is er gebeurd en waarom) geen andere inhoudelijke gegevens. De ontvanger van de notificatie kan vervolgens de detailgegevens van het object ophalen bij de bron door deze op sleutelgegevens te bevragen. De context van de notificatie geeft aan de ontvanger aan waarom de notificatie verzonden is.

Een voorbeeld van het bovenstaande is een afnemer die een abonnement afsluit op de persoonsgegevens van een bepaald BSN. Op het moment dat in de persoonsregistratie een wijziging optreedt, de persoon verhuisd bijvoorbeeld, zal de persoonsregistratie een notificatie van deze wijziging sturen naar de geabonneerde afnemers. De afnemer kan zien dat het een wijziging van de persoonsgegevens van een bepaald BSN betreft in het kader van een verhuizing. De afnemer kan dan besluiten om wel of niet hierop actie te ondernemen.

4.5.4. Audit logging

Alle aanroepen van diensten, of deze nu succesvol zijn geweest of niet worden door de dienstenaanbieder zowel in verband met verantwoording naar burger en bestuur als voor auditdoeleinden in logbestanden vastgelegd. In de logbestanden wordt naast de datum en tijd van de aanroep een aantal meta-attributen vastgelegd. Deze attributen omvatten onder andere het OIN van de organisatie die de dienst heeft aangeroepen, de door de organisatie meegegeven doelbindingsclaim en een uniek ID waarmee de aanroep herleid kan worden naar de logging aan de kant van de dienstenafnemer. Door de logging van de dienstenaanbieder te combineren met de logging van de dienstenafnemer kan een sluitende audit-log worden samengesteld. Deze audit-log kan worden gebruikt om vast te stellen of een dienstenafnemer rechtmatig heeft gehandeld.

4.6. Gegevensintegratie

In de integratielaag van de gegevensdiensten zijn een aantal diensten gepositioneerd die bewerkingen op gegevens van een gegevensbron uitvoeren. Of een dienstenaanbieder dergelijke functies toepast is afhankelijk van de soort diensten die door de dienstenaanbieder worden geboden.

4.6.1. Transformatie

Het is mogelijk dat gegevens getransformeerd alvorens ze via een dienst geleverd worden moeten worden getransformeerd. Dergelijke transformaties kunnen bijvoorbeeld het transformeren van gegeven in yyyymmdd naar dd-mm-yyyy datumnotatie zijn maar ook complexere transformaties zijn mogelijk.

4.6.2. Pseudonimisering

Ten behoeve van bijvoorbeeld analyse toepassingen kan het nodig zijn om gegevens te pseudonimiseren. Met deze techniek worden de identificeerbare elementen van een van een dataset zoals een BSN en een naam verwijderd en omgecodeerd tot een betekenisloos nummer. Het is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het algoritme kan voor een persoon altijd hetzelfde pseudoniem bepalen, waardoor informatie over de persoon, ook uit verschillende bronnen, kan worden gecombineerd[26]. Bij pseudonimisering is het voor de bronhouder nog mogelijk om de gepseudonimiseerde gegevens te herleiden naar de persoon. Het kan dus gezien worden als een beveiligingsmaatregel. Het vermindert het privacy risico van de betrokkenen en het bewerkingsrisico voor de organisatie(s). Gepseudonimiseerde gegevens zijn echter nog steeds persoonsgegevens en dienen conform de eisen uit de privacywetgeving behandeld te worden.

Vanuit de privacywetgeving is het pseudonimiseren van gegevens in sommige gevallen verplicht. In de handreiking “Stroomschema pseudonimisering (AVG)[27]” is een stappenplan opgenomen wat gebruikt kan worden om te toetsen of het gebruik van gepseudonimiseerde gegevens toegestaan is.

4.6.3. Anonimisering

Ten behoeve van bijvoorbeeld de publicatie van open data kan het nodig zijn om gegevens te anonimiseren. Net als bij pseudonimisering worden identificerende gegevens hierbij met een bepaald algoritme worden vervangen door versleutelde gegevens. Het verschil met pseudonimisering is dat het van geanonimiseerde gegevens niet mogelijk is om deze terug te herleiden naar de oorspronkelijke identiteit. Het is een onomkeerbaar proces. Geanonimiseerde gegevens zijn dan ook geen persoonsgegevens meer en de AVG is niet van toepassing op deze gegevens.

Belangrijke randvoorwaarde bij anonimiseren is dat alle herleidbare persoonsgegevens gemaskeerd worden. Het anonimiseren dient daarnaast te gebeuren door daartoe geautoriseerde personen en binnen de geldende regels. Vóór het anonimiseren zijn het namelijk nog wel persoonsgegevens die vallen onder de AVG regels.

[26] https://nl.wikipedia.org/wiki/Pseudonimiseren
[27] https://www.rijksoverheid.nl/documenten/richtlijnen/2018/02/15/stroomschema-pseudonimisering-avg

4.6.4. Bedrijfsregels

Diensten die door gegevensbronnen worden geboden kunnen bedrijfsregels implementeren. Deze regels kunnen bijvoorbeeld de samenhang tussen gegevensobjecten afdwingen en de integriteit van onderliggende data-attributen borgen. Een voorbeeld van het afdwingen van samenhang is dat het object ‘aanvraag’ alleen kan worden geregistreerd als deze kan worden gekoppeld aan een burger of een bedrijf. De bewaking op de geldigheid van een BSN is een voorbeeld van de bewaking van integriteit van attributen.

Sommige bedrijfsregels kennen hun oorsprong in wet- en regelgeving. Door deze bedrijfsregels zo dichtbij mogelijk op de gegevens te implementeren wordt geborgd dat de gegevens conform vigerende wet- en regelgeving verwerkt worden.

4.6.5. Bijhouding gegevens

Door gegevensbronnen worden gegevens bijgehouden en worden CRUD-diensten geleverd voor het aanmaken, onderhouden, verwijderen en ontsluiten van de gegevens. Uitgangspunt van het gegevenslandschap is dat gegevensbronnen qua syntax en samenhang gestandaardiseerd zijn door de bronhouder. Onderdeel van deze standaardisatie is het beschrijven van de syntax en samenhang van gegevens via een informatiemodel. Het informatiemodel vormt de formele beschrijving van alle informatie die van belang is binnen een gegeven domein en beschrijft het domein in termen van objecten, gegevens (attributen) daarvan en relaties daartussen.

Om alle informatiemodellen in Nederland nog beter op elkaar aan te laten sluiten hebben VNG Realisatie, Kadaster en Geonovum gezamenlijk een metamodel ontwikkeld voor informatiemodellering: het Metamodel voor Informatiemodellen (MIM)[28]. Met het metamodel voor informatiemodellen is een gemeenschappelijk vertrekpunt opgesteld voor het maken van informatiemodellen. Het model bevat duidelijke afspraken over het vastleggen van gegevensspecificaties en biedt tegelijkertijd ruimte aan de verschillende niveaus van modellering. Bijzonder aan het model is dat de afspraken over meerdere bestuurslagen heen gaan.

De gemeentelijke gegevens worden onder regie van gemeenten gestandaardiseerd via informatiemodellen. Het gaat hierbij om sectorale/domein specifieke gegevens en gemeentelijke kerngegevens. Daar waar landelijke vastgestelde catalogi bestaan ten aanzien van de gegevens worden deze gevolgd. Een voorbeeld van een dergelijke catalogus is het is Suwi gegevensregister (SGR)[29].

[28] http://www.gemmaonline.nl/images/gemmaonline/6/66/Metamodel_informatiemodellen_KING_Kadaster.pdf
[29] https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/suwi-gegevensregister-sgr/

4.6.6. Duurzame toegankelijkheid

Digitale informatieobjecten die verwerkt worden bij de uitvoering van taken bij gemeenten en hun keten- en netwerkpartners moeten voldoen aan de eisen uit de Archiefwet. Er moet worden voldaan aan de DUTO kwaliteitscriteria: informatieobjecten moeten vindbaar, beschikbaar, leesbaar (en bruikbaar), interpreteerbaar en betrouwbaar (authentiek en integer) zijn. Het is de verantwoordelijkheid van de dienstenaanbieder om te borgen dat aan deze eisen wordt voldaan ten aanzien van de informatieobjecten (gegevensobjecten en documenten) die door de dienstenaanbieder worden beheerd.

Een kerngedachte hierbij is dat informatieobjecten (archiefbescheiden) altijd moeten zijn voorzien van een minimale set van verplichte metagegevens (compliance metadata) en zijn vastgelegd in een duurzaam formaat. Er wordt daarbij gestreefd naar de inzet van by-design principes: hiermee wordt beoogd om metadata automatisch te creëren, updaten en gebruiken in processen en/of services om te kunnen voldoen aan de eisen van de Archiefwet en aanbepalende eisen vanuit de AVG en WOB/WHO/WOO.

Het heeft de voorkeur om moderne technologieën toe te passen om vindbaarheid en toegang mogelijk te maken; denk hierbij aan het publiceren, ontsluiten en relateren van informatieobjecten op basis van bijvoorbeeld Linked (Open) Data.

4.6.7. Protocollering

Iedere vorm van administratie kent methoden om de juistheid van een administratieve handeling te waarborgen. Een onjuiste handeling die niet wordt opgemerkt, kan leiden tot fouten in de administratie. Daardoor kunnen de belangen van degenen die gegevens uit die administratie gebruiken, ernstig worden geschaad. Het is daarom van belang dat nagegaan kan worden of uitgevoerde administratieve handelingen juist zijn uitgevoerd. In de Wet Basisregistratie Personen (BRP) is voorgeschreven dat alle handelingen van het systeem wat de Wet implementeert in beginsel door het systeem zelf dienen te worden vastgelegd. Deze vastlegging wordt ‘protocolleren’ genoemd. In de protocollering wordt ook vastgelegd welke gegevens uit de registratie wanneer, door wie, over wie en aan wie zijn verstrekt.

Het op deze manier vastleggen van administratieve handelingen en ook gegevensverstrekkingen heeft twee functies. Ten eerste kan uit de protocollen worden afgeleid of het systeem de verstrekking juist heeft uitgevoerd. Dat is in feite de functie van systeembeheer. Ten tweede is de vastlegging van een gegevensverstrekking een belangrijk bestanddeel in het stelsel tot bescherming van de persoonlijke levenssfeer van de burger. Het is het sluitstuk. Achteraf kan dan immers worden herleid of de gegevensverstrekking rechtmatig heeft plaatsgevonden: dit wordt de privacyfunctie genoemd.

Hoewel protocollering als term als oorsprong de Wet Basisregistratie Personen kent zou iedere bronregistratie protocollering moeten bijhouden zodat op detailniveau verantwoording kan worden afgelegd over de uitgevoerde administratieve handelingen.

4.6.8. Audit logging

Een essentieel onderdeel van het gebruik van gegevens uit bronbestanden betreft het loggen van deze verwerkingen. Ten behoeve van transparantie naar burger en bestuur en ook ten behoeve van audits is iedere dienstenafnemer verplicht om de verwerking van gegevens vast te leggen in logbestanden. In deze logbestanden dient naast een datum en tijd opgenomen te worden door wie, met welke doelbinding welke gegevens(categorieen) verwerkt zijn.

Deze logbestanden worden richting de burger gebruikt voor het inzage geven in verwerkingen van zijn of haar gegevens, en ze worden gebruikt om achteraf te bepalen of een gemeente rechtmatig heeft gehandeld. De integriteit van logbestanden dient daarom bewaakt te worden. Mutaties in logbestanden moeten voorkomen worden, en logbestanden dienen duurzaam toegankelijk gehouden te worden[30].

[30] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf