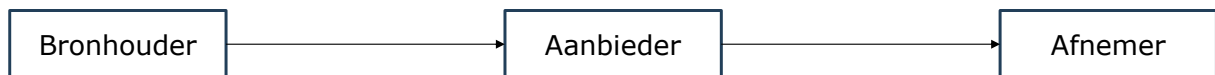


MIDO/GDI

Domeinarchitectuur Gegevensuitwisseling

Datum: 12 september 2024
Versie: 2.0
Status: Vastgesteld



Projectnaam MIDO
Organisatie Bureau MIDO
Contact postbus.pgdi@minbzk.nl

Versiehistorie

Datum	Versie	Opmerkingen
14-09-2023	1.0	Domeinarchitectuur Gegevensuitwisseling, Deel-1
23-05-2024	1.9	Concept van vernieuwde versie van domeinarchitectuur ten behoeve van review door Programmeringstafel Gegevensuitwisseling, brede klankbordgroep en CDO-raad
11-07-2024	1.91	Versie voor interne review binnen de werkgroep
21-08-2024	1.92	Versie ter goedkeuring door de Programmeringstafel Gegevensuitwisseling en de Architectuurraad Digitale Overheid
02-09-2024	1.93	Versie ter vaststelling door de Programmeringsraad GDI
12-09-2024	2.0	Versie die is goedgekeurd door de Architectuurraad Digitale Overheid en vastgesteld door de Programmeringsraad GDI

Inhoud

Managementsamenvatting	4
1 Inleiding	5
1.1 Aanleiding.....	5
1.2 Dit document	5
1.3 Documentstructuur	6
1.4 Relatie met andere architecturen	6
1.5 Relatie met andere initiatieven	7
2 Kernbegrippen	8
2.1 Gegevens en informatie.....	8
2.2 Rollen.....	9
2.3 Functies.....	10
3 Veranderfactoren	11
3.1 Beleid.....	11
3.2 Wet- en regelgeving	12
3.3 Ontwikkelingen.....	14
3.4 Knelpunten	16
3.5 Capability's	17
4 Gewenste situatie	19
4.1 Architectuurvisie.....	19
4.2 Architectuurprincipes.....	26
4.3 Veranderinitiatieven	39
5 Verdieping	43
5.1 Verdieping: gegevensruimtes	43
5.2 Verdieping: metagegevens.....	52
5.3 Verdieping: communicatieprotocollen	62
5.4 Verdieping: historie.....	67
5.5 Verdieping: notificeren	70
6 Bijlagen	74
6.1 Functies.....	75
6.2 Bedrijfsobjecten	80
6.3 Rollen.....	83
6.4 Huidige voorzieningen	83
6.5 Standaarden	85
6.6 Begrippen	90
6.7 Relatie van architectuurprincipes met ADO en NORA	93
6.8 Betrokkenen	97

Managementsamenvatting

Dit document is de uitwerking van de GDI meerjarenvisie en de Architectuur Digitale Overheid 2030 op het onderwerp gegevensuitwisseling. Het geeft inzicht in de impact van nieuwe ontwikkelingen, beleid en wet- en regelgeving op het uitwisselen van gegevens tussen overheidsorganisaties. Het beschrijft de gewenste inrichting in de vorm van een visie, principes en voorgestelde veranderinitiatieven. Daarmee geeft het richting aan de doorontwikkeling van de digitale overheid op het onderwerp.

De domeinarchitectuur is een doorontwikkeling van een eerdere versie, die in 2023 is opgeleverd en goedgekeurd door de Architectuurraad Digitale Overheid. Deze versie biedt een breder perspectief op het onderwerp, heeft een geheel andere structuur en bevat veel nieuwe informatie. Het geeft inhoudelijke verdieping op een aantal onderwerpen die actueel zijn op het gebied van gegevensuitwisseling: gegevensruimtes (data spaces), metagegevens, communicatieprotocollen, historie en notificatie.

Er zijn een aantal kernboodschappen onderdeel van dit document, die op verschillende plaatsen in het document verder zijn uitgewerkt:

- Gegevens moeten beschikbaar zijn voor hergebruik door anderen en voldoen aan de FAIR principes: vindbaar, toegankelijk, interoperabel en herbruikbaarheid.
- Metagegevens zijn een kritische succesfactor voor gegevensuitwisseling en moeten op allerlei niveaus, aan elkaar verbonden en als Linked Data beschikbaar zijn.
- Gegevens moeten contextrijk worden vastgelegd, inclusief historie, om discussie over de feiten, de herkomst en de betekenis van gegevens zoveel mogelijk te voorkomen.
- De betekenis en structuur van gegevens moet expliciet worden gemaakt in begrippen, informatie- en gegevensmodellen, aan elkaar verbonden en traceerbaar naar de wet.
- De kwaliteit van gegevens moet inzichtelijk zijn in de metagegevens, conform het landelijke raamwerk, zodat gebruikers kunnen bepalen of gegevens passen bij hun gebruik.
- De verantwoordelijkheden van bronhouders, aanbieders, afnemers moeten duidelijk zijn, zodat gegevensuitwisselingen efficiënt, rechtmatig en ethisch verantwoord kunnen zijn.
- Gegevens moeten beschikbaar zijn als herbruikbare gegevensdiensten, conform open standaarden, waarbij de standaarden van Forum Standaardisatie leidend zijn.
- Overheidsorganisaties moeten in staat zijn om elkaar te notificeren over belangrijke gebeurtenissen, zodat snel en pro-actief kan worden gehandeld.

Het document is tot stand gekomen in een interbestuurlijke werkgroep met architecten van verschillende overheidsorganisaties, gefaciliteerd vanuit bureau MIDO. Er heeft een brede review op een conceptversie van dit document plaatsgevonden. Daarbij is gebruik gemaakt van een brede klankbordgroep, de leden van de Programmeringstafel Gegevensuitwisseling en de leden van de interdepartementale CDO-raad.

1 Inleiding

1.1 Aanleiding

De overheid digitaliseert en dat roept vragen op over hoe overheidsorganisaties hun processen, gegevens en systemen moeten inrichten. De Generieke Digitale Infrastructuur (GDI) ondersteunt de digitale overheid met afspraken, standaarden en voorzieningen. In de governancestructuur van het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO) werken overheidsorganisaties samen aan de doorontwikkeling van de digitale overheid en de GDI. Er is vanuit deze governance een [meerjarenvisie](#) en een [Architectuur Digitale Overheid 2030](#) opgesteld die op hoofdlijnen beschrijft hoe de digitale overheid zich de komende jaren zou moeten doorontwikkelen. De Architectuur Digitale Overheid wordt nader uitgewerkt in vier domeinarchitecturen op het gebied van interactie, toegang, gegevensuitwisseling en infrastructuur.

Gegevensuitwisseling is het domein dat gaat over het uitwisselen van gegevens tussen de informatiesystemen van overheidsorganisaties en met andere organisaties. Deze gegevens worden richting gebruikers ontsloten in de context van het domein interactie. De beveiligde toegang tot gegevens is onderdeel van het domein toegang. Domein infrastructuur ondersteunt de andere domeinen met infrastructurele voorzieningen, zowel software- als hardwarematig.

Het uitwisselen van gegevens vindt op veel plaatsen en niveaus plaats. Het is een inherent onderdeel van wat organisaties doen. Het zou daarom een onderdeel van de cultuur, besturing en competenties van organisaties moeten zijn. In de praktijk blijkt dat organisaties er vaak onvoldoende aandacht aan geven, waardoor het uiteindelijk meer tijd en geld kost, onvoldoende aansluit bij behoeften van gebruikers en niet voldoet aan relevante wet- en regelgeving. Daarnaast zijn er allerlei ontwikkelingen die om aandacht vragen. Zo komt er nieuwe wet- en regelgeving vanuit Europa die aandacht vraagt en nemen de behoeften van gebruikers alleen maar toe. De Europese datastrategie stelt voor om gegevensruimtes in te richten die drempels moeten wegnemen voor het delen en hergebruiken van gegevens. De impact daarvan op overheidsorganisaties wordt steeds duidelijker, maar moet nog verder uitkristalliseren.

1.2 Dit document

Dit document beschrijft de domeinarchitectuur voor gegevensuitwisseling, als onderdeel van de Generieke Digitale Infrastructuur. Het is opgesteld in een interbestuurlijke werkgroep met vertegenwoordigers van verschillende overheidsorganisaties. Deze zijn ondersteund door bureau MIDO van het ministerie van BZK. Het beschrijft relevant beleid, wet- & regelgeving en ontwikkelingen, en vertaalt deze naar een visie en richting voor de inrichting van gegevensuitwisseling bij overheidsorganisaties. De architectuur geeft richting aan ontwerpkeuzes die worden gemaakt bij het doorontwikkelen van de GDI of bij het aansluiten op de GDI. Het speelt een formele rol in de kaderstelling, toezicht en monitoring van programma's en projecten die gefinancierd worden vanuit de MIDO governancestructuur. Het document is vooral gericht op enterprise-, informatie- en data-architecten bij overheidsorganisaties.

Het document is een doorontwikkeling van een eerdere versie van de domeinarchitectuur, maar kent een bredere scope en een andere structuur en opzet. Gegevensuitwisseling is breder geïnterpreteerd dan alleen de technische uitwisseling; het is alles wat nodig is om ervoor te zorgen dat gegevens in een registratie beschikbaar zijn voor gebruik. Het omvat ook dat wat in andere contexten "delen", "verstrekken" of "databeschikbaarheid" wordt genoemd. Het inwinnen, beheren, gebruiken en archiveren van gegevens is buiten scope omdat het geen aspecten zijn van uitwisseling. Tegelijkertijd is wel het onderwerp metagegevens onderdeel van de scope. De reden is dat metagegevens horen bij de gegevens die worden uitgewisseld en essentieel zijn voor een

goede en betekenisvolle uitwisseling van gegevens. Daarmee zijn aspecten voor het creëren en publiceren van dit soort metagegevens wel meegenomen.

Er is voor gekozen om de architectuur in de modelleertaal ArchiMate uit te werken en de details ervan alleen online beschikbaar te stellen. Dit document is daarmee een samenvatting en verwijzing naar details die online te vinden zijn. Het bevat dan ook allerlei links die toegang geven tot meer informatie. De architectuur wordt online ook doorontwikkeld en beheerd in [GitHub](#), waardoor de meest actuele versie daar te vinden is. Daar zijn ook bestanden te vinden die direct kunnen worden ingelezen in het Open Source modelleertool Archi.

1.3 Documentstructuur

De architectuur is ingedeeld in vijf onderdelen:

- De **kernbegrippen** zijn de kern van de taal zoals deze gehanteerd wordt in dit document en de bijbehorende tekst is een samenvatting van zaken die zijn beschreven in de bijlagen.
- De **veranderfactoren** geven richting aan de architectuur, en bestaan uit beleid, wet- en regelgeving, ontwikkelingen, knelpunten en capability's.
- De **gewenste situatie** beschrijft een architectuurvisie, architectuurprincipes en voorgestelde veranderinitiatieven. De architectuurprincipes zijn de overtuigingen die het hart van de architectuur vormen en die als richtinggevende uitspraken zijn opgeschreven.
- De **verdieping** beschrijft een uitwerking van de architectuurvisie en architectuurprincipes op de onderwerpen gegevensruimtes, metagegevens, communicatieprotocollen, historie en notificeren. De verdiepende delen zijn vooral bedoeld als uitleg van de architectuurprincipes. Ze geven aanvullende inzichten en handreikingen.
- In de **bijlagen** zijn meer algemene modellen en beschrijvingen opgenomen van de functies, objecten, voorzieningen, standaarden en begrippen die van toepassing zijn op gegevensuitwisseling. Het beschrijft ook de relatie van de architectuurprincipes met de Architectuur Digitale Overheid en NORA en de betrokkenen bij de totstandkoming van dit document.

1.4 Relatie met andere architecturen

Deze domeinarchitectuur is sterk gerelateerd aan de domeinarchitectuur toegang. Dat komt enerzijds omdat het uitwisselen van gegevens in veel gevallen om toegang vraagt en anderzijds omdat er gegevens moeten worden uitgewisseld om te bepalen of toegang kan worden verstrekt. Er is bewust voor gekozen om geen grote delen uit de domeinarchitectuur toegang in te kopiëren in deze architectuur, zodat er één duidelijke bron van informatie over gegevensuitwisseling is. De consequentie hiervan is dat lezers wordt gevraagd om de [domeinarchitectuur toegang](#) ook te lezen om een volledig beeld van gegevensuitwisseling te krijgen. De belangrijkste relaties tussen de beide domeinarchitecturen zijn:

- De functie "verlenen toegang" in domeinarchitectuur gegevensuitwisseling is te beschouwen als een samenvoeging van de functies "authenticeren", "autoriseren" en "auditing en monitoring" in de domeinarchitectuur toegang.
- Functies voor het maken van verifieerbare verklaringen en het gebruik van verifieerbare verklaringen voor het verstrekken van toegang zijn onderdeel van de domeinarchitectuur toegang. Functies voor het beschikbaar stellen en valideren van verifieerbare verklaringen zijn onderdeel van de domeinarchitectuur gegevensuitwisseling.
- Regie op gegevens, Self Sovereign Identity en de EDI wallet zijn sterk aan elkaar gerelateerd. De domeinarchitectuur gegevensuitwisseling beschrijft de ontwikkeling en een principe m.b.t. regie op gegevens. De domeinarchitectuur toegang beschrijft de

ontwikkeling en geeft toelichting op Self Sovereign Identity. De EDI wallet wordt in beide domeinarchitecturen beschreven.

- Gegevensruimtes zijn te zien als een meer geavanceerde vorm van gegevensuitwisseling waarbij datasoevereiniteit en vertrouwen centraal staan. Dat vraagt vooral mechanismen voor toegang. Gegevensruimtes worden daarom in beide domeinarchitecturen beschreven en domeinarchitectuur toegang gaat dieper in op de toegangsaspecten, waarbij vooral Policy Based Access Control relevant is.

Er is ook een relatie met de [domeinarchitectuur interactie](#):

- Regie op gegevens, de EDI wallet en het Once Only Technical System (OOTS) zijn sterk aan elkaar gerelateerd en relevant vanuit gegevensuitwisseling en interactie. Beide architecturen besteden aandacht aan regie op gegevens. De domeinarchitectuur gegevensuitwisseling geeft een beschrijving van de EDI wallet en OOTS. De domeinarchitectuur interactie positioneert de EDI wallet in de waardeestroom van interactie.
- De domeinarchitectuur interactie gaat uit van service-oriëntatie en benoemt het belang van het publiceren van metagegevens om informatie te kunnen vinden. De domeinarchitectuur gegevensuitwisseling geeft een uitwerking van soorten metagegevens.
- De uitwisseling van berichten voor burgers en bedrijven is belangrijk vanuit het perspectief van interactie, maar niet uitgewerkt in domeinarchitectuur interactie. De domeinarchitectuur gegevensuitwisseling besteedt hier ook geen aandacht aan.

Deze domeinarchitectuur is nadrukkelijk afgestemd op de [Architectuur Digitale Overheid 2030](#) en de [NORA](#). Hierdoor is deze domeinarchitectuur te beschouwen als een doorvertaling en concretisering van deze overkoepelende architecturen. Er is een specifieke bijlage in dit document waarin de relatie is gelegd tussen de architectuurprincipes in deze domeinarchitectuur en uitspraken in de Architectuur Digitale Overheid en NORA.

1.5 Relatie met andere initiatieven

Er zijn allerlei andere initiatieven die zijn gerelateerd aan gegevensuitwisseling. Het belangrijkste programma dat er op het moment van schrijven van dit document loopt is het programma Federatief Data Stelsel (FDS), als onderdeel van het programma Interbestuurlijke Data Strategie (IBDS). Er is regelmatig afgestemd met programma FDS om conflicten en overlap te voorkomen. De nadruk in programma FDS ligt op het op een verantwoorde wijze delen van gegevens tussen sectoren. De nadruk in deze architectuur ligt op het in meer algemene zin beschrijven van hoe met gegevensuitwisseling wordt omgegaan. De architectuur van het federatief datastelsel is een verdere concretisering van de domeinarchitectuur, waarin meer specifieke keuzes worden gemaakt.

Andere belangrijke programma's die impact hebben op gegevensuitwisseling zijn het programma Regie op Gegevens, het programma EDI-stelsel NL en het programma Single Digital Gateway (SDG). De eerste twee programma's hebben onderling een sterke relatie, omdat ze eigenlijk beiden aandacht geven aan de implementatie van de nieuwe eIDAS verordening en het gebruik van European Digital Identity Wallets. Er is afgestemd met deze programma's om dat wat hierover duidelijk is in de architectuur een plek te geven. Dat geldt ook voor het programma Single Digital Gateway, in het kader waarvan het Once Only Technical System (OOTS) wordt geïmplementeerd.

2 Kernbegrippen

Dit hoofdstuk is bedoeld om de belangrijkste terminologie zoals gebruikt in dit document te verduidelijken. Een is een samenvatting en meer toegankelijke beschrijving van informatie die ook aanwezig is in de begrippenlijst, het functiemodel, het bedrijfsobjectmodel en de rollen. Voor een meer uitgebreide lijst van begrippen wordt dan ook naar de bijlage verwezen.

2.1 Gegevens en informatie

Dit document gaat over de uitwisseling van **gegevens**. Alhoewel de termen “gegevens” en “data” vaak als synoniem worden gebruikt, gebruiken we in dit document vooral de term “gegevens”. Dat doen we omdat vooral geïnteresseerd zijn in betekenisvolle eenheden en niet in de grondstof die eraan ten grondslag ligt (die je dan data zou kunnen noemen). Vanuit dat perspectief zijn gegevens beweringen over objecten, zoals “Jan is geboren op 1 januari 1945”. Gegevens zijn daarmee het gevolg van **feiten**; gebeurtenissen of omstandigheden waarvan de werkelijkheid vaststaat.

Om over de betekenis van gegevens te kunnen spreken is het belangrijk om de begrippen die eraan ten grondslag liggen expliciet te maken. Een **begrip** is in de basis een eenheid van denken; dat wat we ons voorstellen als we een term horen. Door de term te voorzien van een definitie maken we de betekenis expliciet. Gegevens spelen een rol in een bepaald **domein**. Dat is een deel van de werkelijkheid waarover we spreken. Dat kan een sector zijn zoals onderwijs of zorg, maar het kan ook een heel ander gebied zijn waarin gegevens een rol spelen zoals bijvoorbeeld een keten.

Als gegevens moeten worden vastgelegd of uitgewisseld dat is het belangrijk om hun betekenis voldoende duidelijk maken, zodat systemen en gebruikers het kunnen gebruiken. We leggen de precieze betekenis in eerste instantie vast in een **informatiemodel**, dat verwijst naar de begrippen die expliciet zijn gemaakt. Op basis daarvan maken we **gegevensmodellen** die beschrijven in welke structuur de gegevens worden uitgewisseld.

Gegevens worden vastgelegd in een **registratie**; de plaats waarin ze worden verzameld. Deze registratie vormt een **bron** voor de verdere verwerking en het gebruik van deze gegevens. Een deel van de gegevens in een registratie kan beschikbaar worden gesteld aan anderen. Dit heet een **dataset**. Om het mogelijk te maken dat systemen deze gegevens kunnen uitwisselen zijn er **gegevensdiensten** nodig. Dat zijn geautomatiseerde functies die worden aangeboden door systemen. Het is in sommige situaties logischer om een gegevensdienst te gebruiken die niet direct bij de bron hoort, maar bij een kopie van deze bron. Een dergelijke gegevensdienst noemen we een **verstrekkingpunt**.

Als partijen gegevens willen gebruiken dan moeten ze deze eerst kunnen vinden. Gegevens moeten daarom vindbaar zijn in een (data)**catalogus**. In een dergelijke catalogus staan niet de gegevens zelf, maar alleen een beschrijving van deze gegevens; de **metagegevens**. Hiermee kan de inhoud, betekenis en locatie van de gegevens worden gevonden.

Uiteindelijk moeten gegevens vooral waardevol zijn voor gebruikers. Deze hebben bepaalde vragen die moeten worden beantwoord in de context van hun werk. De behoefte aan antwoorden noemen we een **informatiebehoefte**. Het antwoord op de vragen is **informatie**. Daarvoor worden gegevens omgevormd naar een geheel waaruit deze informatie kan worden afgeleid. Dit geheel noemen we een **informatieproduct**, en is een speciale vorm van een dataset. Als de vraag nog niet zo duidelijk is, maar gebruikers wel weten welke gegevens ze daarvoor nodig hebben dan hebben ze een **gegevensbehoefte**.

Rondom gegevens spelen allerlei regels een rol. In de meest algemene zin van het woord zijn dat voorschriften. De belangrijkste soorten regels vanuit het perspectief van gegevensverwerking zijn beperkingsregels en afleidingsregels. **Beperkingsregels** beschrijven binnen welke grenzen de gegevens zich mogen begeven, welke waarden ze mogen aannemen. Deze regels horen al in een gegevensmodel expliciet te zijn gemaakt. Dit soort regels worden ook gebruikt om de kwaliteit van gegevens mee te controleren. We noemen ze dan **kwaliteitsregels**. De andere belangrijke categorie van regels zijn **afleidingsregels**. Dat zijn regels die beschrijven hoe bepaalde soorten gegevens kunnen worden afgeleid uit andere soorten van gegevens. Dat is bijvoorbeeld nodig om informatieproducten te kunnen maken, of om vertalingen tussen gegevens uit te voeren.

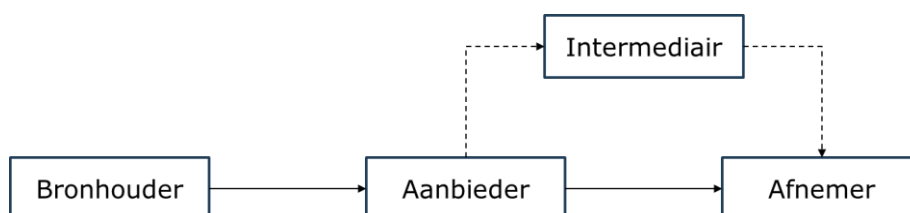
2.2 Rollen

Bronhouders zijn verantwoordelijk voor het inwinnen en beheren van gegevens. Onderdeel daarvan is het verbeteren van de kwaliteit van gegevens. Aan de andere kant zijn er **afnemers** van gegevens. Dat zijn organisaties waar **gebruikers** allerlei toepassingen en gebruik kennen van gegevens, waarbij toenemend allerlei vormen van data science en kunstmatige intelligentie worden toegepast. Om ervoor te zorgen dat gegevens kunnen worden uitgewisseld moeten ze worden aangeboden in een vorm die bruikbaar is voor afnemers. Dit is de rol van een **aanbieder** (ook wel: verstrekker of leverancier) die hiervoor gegevensdiensten aanbiedt.

Een partij die bronhouder is kan zelf ook aanbieder zijn of kan zich laten ontzorgen door een andere partij. Een voorbeeld van een aanbieder is Publieke Dienstverlening op de Kaart (PDOK), een dienst die wordt aangeboden door het Kadaster voor het ontsluiten van geografische gegevens. De rol van aanbieder is expliciet benoemd bij de basisregistraties (en wordt daar verstrekker genoemd). Zo zijn bijvoorbeeld gemeenten bronhouder van de basisregistratie personen (BRP), maar is de Rijksdienst voor Identiteitsgegevens de aanbieder van de gegevens, die hiervoor de landelijke voorziening biedt. De BRP kent heel veel verschillende overheidsorganisaties als afnemers, inclusief gemeenten zelf. Een partij die bronhouder is kan ook de rol van afnemer hebben als er gegevens worden ingewonnen door andere partijen.

Een **intermediair** is een partij die in de keten tussen een aanbieder en een afnemer toegevoegde waarde kan leveren in de uitwisseling. Er zijn allerlei soorten intermediairs te onderkennen. Zo zijn er intermediairs die gespecialiseerd zijn in het samenbrengen, combineren en afleiden van verschillende soorten gegevens. Een voorbeeld van een dergelijke partij is het Inlichtingenbureau dat slimme dienstverlening biedt aan gemeenten op onderwerpen zoals werk- en bestaanszekerheid, onderwijs en belastingen. Er zijn ook intermediairs die vooral gericht zijn op het vertalen van gegevens. Een voorbeeld van een intermediair in deze categorie is stichting RINIS, die vooral technische vertalingen uitvoert. Er kunnen ook intermediairs zijn die zich specifiek richten op het ondersteunen van het abonneren op, en notificeren over gebeurtenissen.

In dit document spreken we in verband met leesbaarheid vaak over bronhouder, aanbieder, intermediair en afnemer alsof ze een organisatie zijn, maar daarmee bedoelen we een organisatie die een dergelijke rol heeft en die ook andere rollen kan hebben. Het moet per context worden bepaald welke rollen door welke organisaties worden ingevuld.

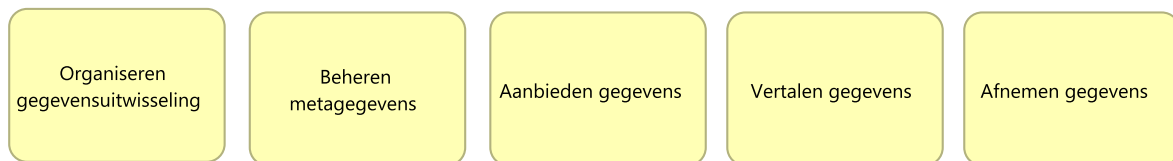


Figuur 1: Rollen: bronhouder, aanbieder, intermediair en afnemer

2.3 Functies

In deze domeinarchitectuur hebben we functies benoemd die in het algemeen relevant zijn voor gegevensuitwisseling. In deze paragraaf beschrijven we de hoofdfuncties, die activiteiten op organisatieniveau beschrijven (het zijn bedrijfsfuncties). Deze functies worden gebruikt om andere zaken op te plotten en aan te relateren. Figuur 2 geeft een overzicht van deze functies. In de bijlage zijn ook de meer gedetailleerde functies beschreven.

Het is door organisaties zelf te bepalen aan welke partijen en afdelingen zij de functies in hun context toekennen. Er zijn wel een aantal functies specifiek gekoppeld aan rollen zoals beschreven in deze domeinarchitectuur. Zo hoort de hoofdfunctie "Aanbieden gegevens" bij de rol aanbieder en hoort de hoofdfunctie "Afnemen gegevens" bij de rol afnemer. Hieruit volgt dat de overige functies aan verschillende rollen en partijen gekoppeld kunnen worden, afhankelijk van de context.



Figuur 2: Functiemodel op hoofdlijnen

Organiseren gegevensuitwisseling	Het organisatorisch inregelen van afspraken over hoe gegevens worden uitgewisseld.
Beheren metagegevens	Het creëren en beschikbaar stellen van gegevens over gegevens.
Aanbieden gegevens	Het beschikbaar stellen van gegevens.
Vertalen gegevens	Het uitvoeren van bewerkingen op gegevens.
Afnemen gegevens	Het ervoor zorgen dat er gegevens afgenomen worden en daardoor beschikbaar zijn voor gebruik.

3 Veranderfactoren

Dit hoofdstuk geeft een overzicht van de veranderfactoren die richting geven aan de architectuur. Het beschrijft de belangrijkste beleid en wet- en regelgeving die van toepassing zijn, de ontwikkelingen die spelen en de knelpunten die er op dit moment bestaan.

3.1 Beleid

De domeinarchitectuur beschrijft een aantal belangrijke beleidsdocumenten die invloed hebben op gegevensuitwisseling. Overheidsorganisaties zouden zich bewust moeten zijn van dit beleid en dit mee moeten nemen in hun eigen beleidsvorming.

A European strategy for data

Vanuit de Europese datastrategie wil de Commissie de ontwikkeling van gemeenschappelijke Europese gegevensruimtes (data spaces) in strategische economische sectoren en gebieden van algemeen belang bevorderen. Deze sectoren of domeinen zijn die waar het gebruik van data een systemische impact zal hebben op het hele ecosysteem, maar ook op burgers. De EU-brede gegevensruimte is waar alle aspecten uit de Data Governance Act, Data Act en Open Data Directive tot praktische uitdrukking komen. In de visie van de Europese strategie voor gegevens is de totstandbrenging van gemeenschappelijke, interoperabele gegevensruimtes in de hele EU in strategische sectoren gericht op het wegnemen van belemmeringen voor het delen van gegevens door de nodige instrumenten en infrastructuren te combineren en vertrouwenskwesties aan te pakken door middel van gemeenschappelijke regels.

Interbestuurlijke Datastrategie

De interbestuurlijke datastrategie schetst op hoofdlijnen hoe de overheid met data maatschappelijke opgaven beter kan adresseren, waarbij risico's van datagebruik goed worden afgewogen. Daarnaast bevat de datastrategie eerste suggesties voor verdere uitwerking van systeemfuncties. De IBDS is het resultaat van nauwe samenwerking tussen departementen, uitvoeringsorganisaties en koepels van medeoverheden. Samen zetten zij met deze strategie een ambitieuze stap. Eén van de middelen bij die strategie is het opzetten van een Federatief Datastelsel (FDS): een geoptimaliseerd stelsel voor het verantwoord gebruiken van data uit verschillende gegevensbronnen. Het doel is dat het stelsel via afspraken en oplossingen data beschikbaar maakt voor zo breed mogelijk gebruik.

Werkagenda Waardengedreven Digitaliseren

Als we willen dat digitale technologie vóór onze samenleving blijft werken, als we kansen willen benutten en risico's willen mitigeren, dan moet digitalisering waardengedreven en mensgericht zijn vormgegeven en moeten we als samenleving, bedrijfsleven en overheid samen optrekken. Het kabinet Rutte-IV heeft hier werk van gemaakt, onder meer door een eerste coördinerend bewindspersoon voor Digitalisering aan te stellen die met haar collega-bewindspersonen deze waardengedreven digitalisering verder vormgeeft. Op 4 november 2022 is de Werkagenda Waardengedreven Digitaliseren aan de Tweede Kamer aangeboden. De Werkagenda is een uitwerking van elementen uit de brief Hoofdlijnen Beleid Digitalisering met concrete doelen en acties. Hij omvat 5 sporen: meedoen, vertrouwen en regie in de digitale samenleving, een goede digitale overheid

en het versterken van de digitale samenleving in het Caribisch deel van het Koninkrijk.

GDI-Meerjarenvisie 2024-2028

Deze meerjarenvisie biedt in eerste instantie inzicht en overzicht in de relevante politieke, beleidsmatige en technische ontwikkelingen, ook internationaal, en geeft op basis daarvan richting aan de doorontwikkeling van de GDI. Ook benoemt het principes en uitgangspunten die worden gehanteerd bij de stapsgewijze realisatie van de beschreven ambities. Het MIDO is daarmee de concretisering van datgene dat interbestuurlijk gezamenlijk wordt georganiseerd aan afspraken, standaarden en voorzieningen om de ambities uit de Werkagenda Waardengedreven Digitaliseren waar te maken.

I-strategie Rijk

In deze I-strategie 2021-2025 staan de gezamenlijke prioriteiten van de Chief Information Officers (CIO's) van het rijk voor de informatievoorziening. Iedere prioriteit is uitgewerkt in een aantal actiepunten. Data is een expliciet aandachtspunt in deze I-strategie. Datamogelijkheden zijn geen sluitstuk, maar het vertrekpunt. Met data zijn we in staat om onze processen te verbeteren en vernieuwen, en betere en innovatievere besluiten te nemen. Ook zijn we wendbaarder wanneer we door inzet van data sneller inspelen op maatschappelijke veranderingen.

Baseline Informatiebeveiliging Overheid

De Baseline Informatiebeveiliging Overheid (BIO) is een normenkader voor informatiebeveiliging en geeft het basisniveau voor informatiebeveiliging waar alle overheidspartijen aan moeten voldoen. Door dit eenduidige normenkader binnen de overheid, wordt een stevige basis gelegd voor de verdere optimalisering van informatiebeveiliging binnen de gehele overheid en ontstaat een gemeenschappelijke taal die bijdraagt aan veilige samenwerking in ketens binnen de overheid. De BIO is gebaseerd op de NEN-ISO/IEC 27002.

3.2 Wet- en regelgeving

De domeinarchitectuur beschrijft de belangrijkste wet- en regelgeving die van toepassing is op gegevensuitwisseling. Dat betreft met name nieuwe wet- en regelgeving vanuit Europa, inclusief de Nederlandse invulling daarvan, gegeven dat dit een belangrijke bron voor verandering is voor gegevensuitwisseling. Er heeft geen detailanalyse van de wet- en regelgeving plaatsgevonden. Daarmee kan er ook geen garantie worden gegeven dat het volgen van deze architectuur automatisch leidt tot het volledig voldoen aan de wet- en regelgeving.

Data Governance Act

Deze verordening is het eerste wetgevend voorstel uit de Europese datastrategie en heeft als doel databeschikbaarheid voor hergebruik in de EU te faciliteren door vertrouwen in data-tussenpersonen te vergroten en datadeelmechanismen in de EU te versterken. De verordening heeft vier hoofdonderdelen: hergebruik van beschermde gegevens in het beheer van openbare lichamen, voorwaarden voor datadeeldiensten, data-altruïsme en een Europese Data Innovatie Raad. Daarnaast gaat de verordening in op handhaving en toezicht en de internationale datastromen die verbonden zijn aan bovenstaande onderdelen.

General Data Protection Regulation

Deze verordening standaardiseert de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de Europese Unie. Het doel van de verordening is het garanderen van de bescherming van persoonsgegevens binnen de Europese Unie en het

waarborgen van het vrije verkeer van gegevens binnen de Europese interne markt. In Nederland staat de verordening bekend als de Algemene Verordening Gegevensbescherming (AVG).

Interoperable Europe Act

Deze Europese verordening heeft als doel om de samenwerking en digitale uitwisseling tussen overheidsorganisaties in de hele EU te verbeteren. De inzet van het kabinet op de Interoperable Europe Act is dat burgers en bedrijven in de toekomst laagdrempeliger en sneller bediend kunnen worden bij het aanvragen van diensten. De verordening doet dit onder andere door het stimuleren van het delen en hergebruiken van bestaande softwareoplossingen, het afspreken van standaarden en het delen van goede voorbeelden tussen lidstaten. Door analyses te verplichten bij nieuwe wet- en regelgeving worden interoperabiliteitsproblemen eerder in het proces gevonden, voordat wetteksten definitief zijn. Digitale overheidsdiensten die goed samenwerken zijn cruciaal voor het vertrouwen van burgers in de overheid. Het European Interoperability Framework (EIF) is een belangrijke pijler onder de verordening en zal worden gebruikt als toetskader.

Open Data Directive

In de open data directive is ingezet op het volledig kunnen benutten van het potentieel van overheidsinformatie ten behoeve van de Europese economie en samenleving door de richtlijn aan te passen aan de nieuwste ontwikkelingen op het gebied van databeheer en -gebruik. De Open Data Directive is geïmplementeerd in de Nederlandse Wet hergebruik van overheidsinformatie.

Wet hergebruik overheidsinformatie

De Wet hergebruik overheidsinformatie (Who) is bedoeld om de openheid en het hergebruik van gegevens, die door organisaties met een publieke taak worden beheerd, te verbeteren. Dit om de waarde van die informatie voor het maatschappelijk en economisch verkeer te ondersteunen en vergroten. Veel informatie is daarom openbaar, vrij te gebruiken en te verspreiden. Personen kunnen, volgens de Who, een verzoek indienen om hergebruik van informatie mogelijk te maken. Als deze informatie vervolgens geleverd wordt, moet deze in een open en machineleesbaar formaat aangeboden worden. De aanpassing van de Who aan de Open Data Directive zorgt ervoor dat er meer soorten organisaties aan de wet moeten voldoen. Andere nieuwe verplichtingen hebben betrekking op onder meer specifieke hoogwaardige gegevenssets, dynamische gegevens en onderzoeksgegevens.

Single Digital Gateway

In de SDG-verordening staat welke informatie en procedures online aangeboden moeten worden en vanaf wanneer dat moet worden gedaan. Het portaal Your Europe is de centrale toegangspoort en verwijst gebruikers door naar de juiste websites in de verschillende lidstaten. Via Your Europe kunnen burgers en bedrijven op een eenvoudige manier betrouwbare informatie vinden over overheidsdiensten, -producten en -procedures in Europa. Sommige procedures kunnen ze bovendien online doorlopen. Bij het verlenen van toegang tot procedures is het Once-Only Principe (Eenmaligheidsbeginsel) van belang zodat burgers, instellingen en bedrijven bepaalde informatie slechts één keer hoeven aan te leveren aan de overheid. Het Once Only Technical System (OOTS) ondersteunt de gewenste gegevensuitwisseling.

Wet digitale overheid	De Wet digitale overheid (Wdo) faciliteert de uitvoering van de initiële eIDAS verordening uit 2014 in Nederland. De Wdo regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers over elektronische identificatiemiddelen (eID) kunnen beschikken met een substantiële of hoge mate van betrouwbaarheid. De wet bevat ook regels over het gebruik van standaarden. Zo beschrijft deze dat standaarden voor elektronisch verkeer kunnen worden aangewezen bij algemene maatregel van bestuur. Daarmee kunnen dus standaarden die essentieel zijn voor gegevensuitwisseling wettelijk verplicht worden gesteld.
Wet open overheid	De Wet open overheid (Woo) regelt welke overheidsinformatie openbaar is en hoe iemand die kan aanvragen. Door de Woo moet duidelijker worden wat de overheid doet en waarom. Overheidsinformatie is openbaar, behalve als er een reden is waarom dat niet kan. De overheid moet uit zichzelf zoveel mogelijk informatie openbaar maken als dat zonder grote moeite of hoge kosten kan. Overheden beoordelen zelf welke documenten hieronder vallen. Daarnaast kunnen burgers een verzoek indienen tot openbaarmaking van informatie.
eIDAS 2.0	De afkorting eIDAS staat voor 'electronic IDentities And Trust Services'. De verordening regelt een Europees kader voor digitale identiteiten waarmee het makkelijker en veiliger wordt om binnen Europa online zaken te regelen. De herziene versie van de verordening introduceert Europese digitale identiteitswallets waarmee burgers en organisaties gebruik kunnen maken van digitale diensten. Het gebruik van de wallet is op basis van vrijwilligheid en maakt het mogelijk voor burgers en organisaties om controle te hebben over hun persoonsgegevens. De wallet kan gebruikt worden als een identificatiemiddel, voor machtigen en vertegenwoordigen, voor elektronisch ondertekenen en als een middel voor het veilig delen van gegevens.

3.3 Ontwikkelingen

In deze architectuur beschrijven we een aantal belangrijke (vooral technische) ontwikkelingen op het gebied van gegevensuitwisseling. De impact van deze ontwikkelingen is meegenomen in de beschrijving van de architectuur.

De hoeveelheid gegevens groeit	Door de versnelde digitalisering van veel bedrijfsprocessen neemt het volume van uitgewisselde gegevens sterk toe. Er wordt een toename van 530% van het wereldwijde gegevensvolume verwacht in de periode 2018–2025 (bron: Europese datastrategie). Het aantal organisaties dat gegevens uitwisselt, ook binnen de overheid, neemt sterk toe. De rol van gegevens en de uitwisseling daarvan wordt steeds belangrijker. Bijvoorbeeld voor analyse, besluitvorming en ontwikkeling en gebruik van kunstmatige intelligentie.
Kunstmatige intelligentie (AI)	Mede door de toegenomen hoeveelheid beschikbare gegevens is er veel aandacht voor kunstmatige intelligentie. Er ontstaan allerlei nieuwe mogelijkheden in het gebruik van gegevens. Daarmee is er ook een grotere behoefte aan de beschikbaarheid en uitwisseling van gegevens. Tegelijkertijd ontstaan er allerlei nieuwe risico's en dilemma's bij het

gebruik van kunstmatige intelligentie, met name op het gebied van privacy en ethiek.

Toenemende zorg over privacy en ethiek

Initieel gedreven vanuit de Algemene Verordening Gegevensbescherming is er steeds meer aandacht gekomen rondom privacy. De aandacht voor datalekken en de kosten daarvan, neemt toe. In bredere zin ontstaat steeds meer discussie wat de morele grenzen van het gebruik van gegevens zijn. Er ontstaan ethische toetsingscommissies die hier oordelen over moeten geven. Gegevensuitwisseling wordt vaker 'gelokaliseerd' zodat gegevens alleen beschikbaar komen in landen waar de Europese wet- en regelgeving geldt.

Regie op eigen gegevens

Burgers en organisaties verwachten steeds meer dat ze zelf in control zijn over hun eigen gegevens. Ze willen zelf bepalen aan wie ze hun gegevens verstrekken. Dit is grotendeels hetzelfde als wat ook wel Self Sovereign Identity heet. Daarbij hoort dat je ook zelf je eigen identiteit wilt creëren en niet afhankelijk wil zijn van derde partijen die je mogelijk niet vertrouwt. Gebruikers kunnen hun identiteit voorzien van allerlei verklaringen, die deels van henzelf komen en die deels afkomstig zijn van anderen. De basis voor al dit soort ideeën is de behoefte aan autonomie en privacy.

Gebruikersbehoeften nemen toe

Afnemers verwachten snel en eenvoudig over actuele (en historische) gegevens van derden te kunnen beschikken. Ze verwachten ook toenemend dat gegevens voldoen aan hun eigen behoeften en gebruik en dat ze in een voor hen bruikbare vorm worden verstrekt.

API economie

Organisaties gebruiken in toenemende mate API's. API's zijn de standaard manier geworden om systemen en gegevens te integreren. Er is binnen de Nederlandse overheid ook veel aandacht voor de inzet en het gebruik van API's. Zo is er een kennisplatform API's, een Nederlandse API strategie en het portaal developer.overheid.nl waarin API's kunnen worden gepubliceerd.

Common Ground

Common Ground is de informatiekundige visie waarmee gemeenten collectief de informatievoorziening eenvoudiger, flexibeler en slimmer willen inrichten. Daardoor willen ze hun dienstverlening en bedrijfsvoering verbeteren en beter ze in staat zijn om flexibel in te spelen op maatschappelijke opgaven. Het is gebaseerd op het inzicht dat de huidige manier van gegevens uitwisselen traag verloopt, kostbaar is en foutgevoelig. Basisgedachten daarbij zijn dat gegevens moeten worden losgekoppeld van processen en applicaties, en dat data bij de bron moet worden gehaald.

Cloud computing

Organisaties maken toenemend gebruik van cloudvoorzieningen voor hun systemen en gegevens. Hierdoor verloopt ook een toenemende hoeveelheid uitwisseling van gegevens binnen en tussen cloudomgevingen. Daarbij ontstaan vragen over performance, soevereiniteit, informatiebeveiliging en licentiekosten.

Data clean rooms

Een data clean room is een veilige, gecontroleerde omgeving waar verschillende partijen gevoelige gegevens kunnen delen en analyseren zonder de onderliggende gegevens daadwerkelijk te onthullen aan elkaar. Dit concept wordt vaak gebruikt in situaties waarin privacy en vertrouwelijkheid van groot belang zijn, zoals bij samenwerking tussen bedrijven of in de gezondheidszorg.

Veel Europese regelgeving

Europa streeft actief naar ongehinderd gegevensverkeer binnen de EU en tussen sectoren, met toepassing van de Europese regels en waarden, met name die ter bescherming van persoonsgegevens. Er wordt vanuit Europa allerlei nieuwe wet- en regelgeving opgesteld rondom gegevens. Deze wet- en regelgeving vraagt ook integratie van gegevens op Europees niveau. Daarmee wordt veel van de verandering rondom gegevensuitwisseling bepaald vanuit Europa. Dit vraagt veel van overheidsorganisaties en genereert allerlei vragen bij de implementatie.

3.4 Knelpunten

Knelpunten zijn omstandigheden in de huidige situatie die ertoe leiden dat organisaties niet kunnen voldoen aan beleid of wet- en regelgeving. Er heeft in het kader van de domeinarchitectuur een globale analyse van knelpunten plaatsgevonden. De resultaten van de analyse zijn samengevat en opgenomen in de architectuur.

Het kost tijd en inspanning om afspraken te maken

Het kost in de praktijk veel tijd en inspanning om een gegevensuitwisseling tot stand te brengen. Een belangrijke oorzaak daarvan ligt in de tijd die het kost om afspraken te maken. Het uitwisselen van gegevens vraagt allerlei afspraken tussen partijen waarbij allerlei mensen moeten worden betrokken en waarover discussie kan ontstaan. Denk aan financiële, juridische, organisatorische, procesmatige, informatiekundige en technische aspecten. Er blijkt niet altijd een juridische grondslag voor het delen van gegevens en privacy wordt al snel als struikelblok ervaren, ook als dat niet nodig is. Er zijn ook niet altijd voldoende prikkels voor bronhouders om gegevens beschikbaar te stellen.

Gegevens worden niet altijd rechtmatig uitgewisseld

Het is niet altijd duidelijk voor welk origineel doel gegevens in het verleden zijn ingezameld. Mede hierdoor voldoen gegevensuitwisselingen niet altijd aan op dit moment geldende wet- en regelgeving, bijvoorbeeld op het gebied van privacy. Gegevens mogen niet worden uitgewisseld als daar geen wettelijke grondslag voor is. Er worden niet altijd voldoende beveiligingsmaatregelen genomen om beschikbaarheid, integriteit en vertrouwelijkheid te borgen. Daarnaast zijn gegevens in niet alle gevallen duurzaam toegankelijk, zoals noodzakelijk is vanuit de archiefwet.

Gegevens voldoen niet altijd aan behoeften van gebruikers

Er is onvoldoende afstemming over de precieze informatiebehoeften van gebruikers, waardoor ze onvoldoende aansluiten bij hun gebruiksdoel. gebruikersgroepen en hun behoeften zijn niet altijd scherp in beeld. Veel gegevens die worden gedeeld zijn ingewonnen voor een specifiek doel en zijn dus niet zomaar in een andere context bruikbaar.

Gegevens zijn beperkt voorzien van metagegevens

Gebruikers zijn niet altijd in staat gegevens te vinden, te raadplegen, te interpreteren of te bepalen of het aansluit bij het beoogde gebruik. Een belangrijke oorzaak daarvoor is het ontbreken van relevante metagegevens, zoals over wat de gegevens betekenen of wat de precieze herkomst is van gegevens. Er is in organisaties onvoldoende tijd, geld, aandacht en competentie om metagegevens structureel vast te leggen.

Kwaliteit van gegevens onduidelijk of onvoldoende

Er is vaak geen inzicht in de kwaliteit van beschikbare gegevens waardoor onduidelijk is of de kwaliteit voldoende is voor een specifiek gebruik. Metagegevens hierover ontbreken in veel gevallen. Daarnaast wordt er in veel gevallen onvoldoende tijd- en energie besteedt aan het borgen en verbeteren van de kwaliteit van gegevens. Gegevens worden ook vaak

gekopieerd, waardoor ze minder actueel of inconsistent zijn. Gebruikers zijn zich hier vaak onvoldoende bewust van en trekken dan conclusies die eigenlijk niet getrokken kunnen worden uit de beschikbare gegevens.

Betekenis is contextueel

Begrippen en gegevens die daar invulling aan geven hebben een specifieke betekenis in de context waarin ze ingewonnen zijn. Het vastleggen van deze betekenis krijgt niet altijd voldoende aandacht, waardoor er verwarring en misinterpretatie kan ontstaan. Daarnaast is hergebruik in andere contexten lastig, doordat hier andere begrippen en betekenissen bestaan. Het vraagt allerlei afstemming om gegevens te vertalen van de ene context naar de andere, waarbij er ook een reëel risico is dat een deel van de betekenis verloren gaat. Anders gezegd: semantische interoperabiliteit is in de praktijk een uitdaging.

Integraal beeld ontbreekt

Er ontbreekt veelal in organisaties een integraal beeld van de gegevens die bestaan, de precieze betekenis waarmee ze zijn vastgelegd, de plaatsen waar ze zijn opgeslagen en de koppelvlakken waarin ze worden uitgewisseld. Hierdoor kost het inschatten van de impact van veranderingen relatief veel tijd, geld en inspanning.

Gegevens opgesloten in systemen

Gegevens zitten vaak nog te veel opgesloten in (oude) systemen en kunnen daardoor niet makkelijk gedeeld of uitgewisseld worden. En ook bij het bouwen van nieuwe systemen zijn de gegevens soms nog niet goed los van de applicaties beschikbaar. De kennis van oude systemen is ook niet meer altijd aanwezig. Van standaard applicaties is ook niet altijd voldoende documentatie beschikbaar over het gehanteerde gegevensmodel, waardoor ook niet duidelijk is welke gegevens precies beschikbaar zijn.

Onnodige complexiteit

Bij veel organisaties zijn in de loop der jaren veel administraties en koppelvlakken toegevoegd zonder dat daarbij voldoende gelet is op de mogelijke overlap met reeds aanwezige gegevens en koppelvlakken. Daarnaast is vaak ook een grote variatie aan technologieën geïmplementeerd. Door dit alles is de complexiteit van de informatievoorziening en de bijbehorende onderhoudslast onnodig hoog, zijn wijzigingen lastig door te voeren en gegevens lastig uit te wisselen.

3.5 Capability's

Capability's beschrijven dat wat organisaties zouden moeten kunnen. Het zijn vermogens waar organisaties over moeten beschikken. Om invulling te geven aan een capability zijn mensen, processen en middelen nodig. In deze architectuur zijn de capability's een abstracte beschrijving van wat belangrijk is voor organisaties om invulling te geven aan gegevensuitwisseling.

Gegevensuitwisseling organiseren

Het maken van afspraken tussen bronhouders, afnemers, intermediairs en dienstverleners om gegevens optimaal en verantwoord binnen en tussen domeinen te kunnen laten stromen, alsook het inrichten van relevante processen voor gegevensuitwisseling.

Begrippen en gegevens modelleren

Het definiëren en verbinden van semantische, conceptuele, logische en implementatiemodellen om de betekenis en structuur van gegevens te beschrijven.

Gegevens metadateren	Gegevens voorzien van rijke metagegevens, conform standaarden voor metagegevens, om hun vindbaarheid, toegankelijkheid, interoperabiliteit en hergebruik te borgen.
Gegevens aanbieden	Het pro-actief aanbieden van gegevens voor hergebruik door anderen, in machineleesbare vorm, via open en algemeen implementeerbare protocollen.
Gegevens bruikbaar maken	Het bieden van gegevens- en informatieproducten die qua inhoud, vorm en kwaliteit aansluiten bij de behoeften en het gebruik van afnemers.

4 Gewenste situatie

Dit hoofdstuk beschrijft de architectuur van de gewenste situatie met betrekking tot gegevensuitwisseling. Het start met een architectuurvisie die een overkoepelende beschrijving geeft van de gewenste situatie en de architectuurprincipes die deze meer concreet maken. Op basis hiervan worden veranderinitiatieven voorgesteld, die aangeven welke nieuwe afspraken, standaarden of voorzieningen of wijzigingen daarin wenselijk zijn.

4.1 Architectuurvisie

Deze architectuurvisie geeft een overzicht van de belangrijkste ideeën in de domeinarchitectuur. Het kan voor een belangrijk deel worden gezien als het overkoepelende verhaal en een samenvatting en verbinding van de architectuurprincipes. Het bevat dan ook verwijzingen naar deze architectuurprincipes, waar meer over hun rationale en implicaties kan worden gelezen.

4.1.1 Inleiding

Gegevensuitwisseling zorgt ervoor dat partijen beschikken over de gegevens die ze nodig hebben om hun werk op een goede manier uit te voeren. Het is essentieel om publieke dienstverlening in ketens mogelijk te maken, zonder dat burgers en ondernemers steeds opnieuw hun gegevens moeten aanleveren. Het stroomlijnt processen en maakt het mogelijk om tot nieuwe inzichten te komen. Het is echter geen doel op zich. Het ondersteunt doelstellingen en moet altijd in de context van deze doelstellingen worden beschouwd en afgewogen. Een professionele en kwalitatief hoogwaardige uitwisseling van gegevens kan op gespannen voet staan met het bereiken van een specifiek (maatschappelijk) doel, bijvoorbeeld als daar onvoldoende middelen voor beschikbaar zijn. Daarnaast moet gegevensuitwisseling waardegedreven zijn en rekening houden met algemene ethische principes zoals transparantie, verantwoordelijkheid, privacy en autonomie. De menselijke maat zou de basis moeten zijn. Zo moet bijvoorbeeld duidelijk zijn welke gegevens worden uitgewisseld en voor welk doel, moeten de betrokken partijen erop aangesproken kunnen worden, moeten persoonsgegevens goed worden beschermd en willen mensen regie kunnen voeren op hun eigen gegevens.

Het uitwisselen van gegevens is niet iets nieuws. Het blijft echter in de praktijk voor veel organisaties een uitdaging, met name doordat wet- en regelgeving en het maken van afspraken veel aandacht vragen. Daarnaast lag de nadruk in het verleden ook te vaak op het operationeel inrichten van de uitwisseling tussen twee partijen. Deze nadruk zorgt ervoor dat alhoewel de uitwisseling zelf werkt deze in de praktijk toch vaak onvoldoende toekomstvast bleek. Op het moment dat ook andere partijen geïnteresseerd waren in de gegevens werd al snel een nieuwe gegevensuitwisseling ingericht, omdat het hergebruiken van de bestaande meer moeite kostte dan verwacht. Dat had bijvoorbeeld ook te maken met het feit dat veel partijen een geheel ander perspectief op de werkelijkheid hebben en daarmee interesse hebben in net wat andere gegevens en daarbij vaak ook een eigen taal hanteren. Het vertalen van gegevens kost in de praktijk veel inspanning. In dit hoofdstuk beschrijven we een nieuw beeld van hoe gegevensuitwisseling zou moeten werken. Daarbij spelen met name de Europese datastrategie en Europese wet- en regelgeving een belangrijke rol.

De [Europese datastrategie](#) legt de nadruk op het wegnemen van juridische en technische drempels voor het uitwisselen van gegevens door de juiste combinatie van instrumenten en infrastructuur en het scheppen van vertrouwen, bijvoorbeeld door middel van gemeenschappelijke regels. Er moet een Europese gegevensruimte komen, een interne markt voor gegevens, waar zowel overheidsorganisaties als bedrijven gebruik van kunnen maken. De interne markt is een belangrijke pijler onder de Europese Economische Ruimte (EER). Door de drempels in deze markt

weg te nemen, kunnen personen in de EER uiteindelijk de procedures voor het werken, wonen, studeren, leven en ondernemen in een andere lidstaat net zo makkelijk doorlopen als in de eigen lidstaat. Binnen de Europese gegevensruimte ziet de Europese Commissie gemeenschappelijke gegevensruimtes ontstaan voor specifieke sectoren. De precieze inrichting van veel van deze gegevensruimtes is nog onduidelijk. De aandacht voor gegevensuitwisseling vanuit Europa biedt individuele lidstaten in ieder geval kansen om de politieke en beleidsmatige doelstellingen te realiseren. Dat geldt zeker voor Nederland dat al jaren investeert in het uitwisselen en benutten van gegevens.

Binnen programma FDS wordt gewerkt aan een federatief datastelsel dat kan worden gezien als gegevensruimte voor Nederlandse bronregistraties, als uitbreiding op de (gegevensruimte voor de) basisregistraties. Er zijn inmiddels allerlei referentie-architecturen voor gegevensruimtes beschikbaar van bijvoorbeeld [OpenDEI](#), de [International Data Spaces Association](#), en het [Data Spaces Support Center](#). Veel van de ideeën in deze referentie-architecturen kunnen we breder omarmen. Ze zijn voor een belangrijk deel niet nieuw, maar door ze meer consequent en in samenhang toe te passen kan gegevensuitwisseling wel worden gestroomlijnd. Zo kunnen we ons meer bewust zijn van, en sturen op het domeinspecifieke karakter van veel gegevensuitwisselingen. Domeinen hebben zelf de inhoudelijke kennis van hun gegevens en het is dan ook logisch om het beheer ervan bij de domeinen zelf te laten liggen. Binnen domeinen zijn er ook specifieke ketenprocessen, wordt een specifieke taal gehanteerd en gelden specifieke eisen. Het is daarom belangrijk om binnen domeinen afsprakenstelsels te hanteren die ervoor zorgen dat gegevens binnen domeinen optimaal stromen. Tegelijkertijd is het ook nodig dat over domeinen heen gegevens uitwisselbaar zijn.

4.1.2 Heldere rolverdeling

Om gegevensuitwisseling goed te laten werken is het belangrijk dat rollen, taken en verantwoordelijkheden helder zijn (zie ook Tabel 1). Bronhouders zijn ervoor verantwoordelijk dat de [kwaliteit van de gegevens in de bronnen aansluiten bij het gebruik](#). Onderdeel daarvan is dat ze afstemmen met afnemers over de gewenste kwaliteit en dat ze terugmeldingen van gebruikers afhandelen en onderzoeken. Ze moeten de [historie](#) van gegevens vastleggen, zodat hier naar verwezen kan worden als het nodig is. Het is ook belangrijk dat ze [relevante context](#) van gegevens vastleggen als metagegevens, zodat er geen twijfel kan zijn over de herkomst en betekenis van gegevens.

Aanbieders moeten ervoor zorgen dat gegevens beschikbaar zijn conform de [FAIR-principes](#), zodat ze vindbaar, toegankelijk, interoperabel en herbruikbaar zijn. Het gebruik van [open standaarden](#) is daarvoor een belangrijke basis. Daarnaast zullen ze metagegevens beschikbaar moeten stellen, en zorgen dat deze bekend zijn in relevante (data)catalogi. Ze moeten expliciete aandacht hebben voor belangrijke [gegevens- of informatiebehoeften](#) die bij meerdere afnemers spelen. De gegevensdiensten die ze aanbieden moeten [herbruikbaar](#) zijn, zodat ze breed voor allerlei afnemers beschikbaar zijn. Ze zullen in de toekomst gegevens over partijen ook beschikbaar moeten stellen in de vorm van verifieerbare verklaringen, zodat deze gebruikt kunnen worden in EDI wallets. Aanbieders moeten afnemers notificeren over relevante gebeurtenissen die zijn optreden bij bronhouders, zodat overheidsorganisaties snel kunnen acteren. Aanbieders zijn het loket richting afnemers en moeten terugmeldingen routeren naar de verantwoordelijke bronhouder. Gegevens moeten zowel binnen domeinen, als tussen domeinen kunnen worden uitgewisseld. Dat betekent dat landelijke afspraken en [standaarden](#) gebruikt moeten worden voor het beschikbaar stellen van gegevens die landelijk waardevol zijn.

Een partij die bronhouder is kan zelf ook de rol van aanbieder invullen. Het is afhankelijk van de context of dit logisch is. Een scheiding van de rollen bronhouder en aanbieder heeft als voordeel

dat het leidt tot een duidelijker verdeling van taken en verantwoordelijkheden. Het vastleggen van feiten vraagt nu eenmaal een andere focus dan het toegankelijk ontsluiten van gegevens.

Afnemers behandelen de [bronnen die worden beheerd door bronhouders als leidend](#), zodat er geen discussie nodig is over de authenticiteit en actualiteit van de gegevens. Zij laten gegevens zoveel mogelijk bij de bron. Afnemers hebben een verantwoordelijkheid om het gebruik van gegevens te kennen en te ondersteunen. Zij moeten zicht hebben op de kwaliteitseisen van gebruikers, zodat ze deze kunnen inbrengen bij bronhouders. Als zij twijfel hebben over de juistheid van gegevens dan melden ze deze bij de aanbieder. Zij zijn verantwoordelijk voor het rechtmatig gebruik van gegevens. Dat betekent dat ze expliciet moeten maken wat de wettelijke grondslag en doelbinding is van het gebruik van de gegevens en dat op een later moment ook kunnen aantonen, bijvoorbeeld in een audit. Daaraan gerelateerd moeten zij zorgen dat het gebruik van persoonsgegevens is getoetst op privacy en ethiek. Afnemers die gegevens ontvangen zullen deze zelf moeten [valideren](#). Als afnemers verifieerbare verklaringen ontvangen dan zullen ze zelf de authenticiteit, integriteit en geldigheid van deze verklaringen moeten controleren.

Bronhouder	Aanbieder	Afnemer
<ul style="list-style-type: none"> Inwinnen gegevens Vastleggen historie Vastleggen context van gegevens (metagegevens) Beheren gegevens Verbeteren gegevenskwaliteit Opstellen gebruiksvoorwaarden Genereren trigger voor relevante gebeurtenissen Onderzoeken en verwerken terugmeldingen Opstellen en vastleggen afspraken met aanbieders 	<ul style="list-style-type: none"> Ontwikkelen en beheren gegevensdiensten Opstellen en vastleggen afspraken met afnemers Beschikbaar stellen actuele en historische gegevens Beschikbaar stellen metagegevens Beschikbaar stellen verifieerbare verklaringen Notificeren over gebeurtenissen Ontvangen terugmeldingen Verlenen toegang Loggen verzendingen 	<ul style="list-style-type: none"> Definiëren kwaliteitseisen vanuit gebruik Expliciet en aantoonbaar maken grondslag en doelbinding van gebruik Toetsen op privacy en ethiek Ontvangen gegevens Valideren gegevens Valideren en verifiëren verklaringen Afhandelen notificaties over gebeurtenissen Terugmelden gereede twijfel over de juistheid van een gegeven Loggen ontvangsten (en gebruik)

Tabel 1: Basisrollen en verantwoordelijkheden

Binnen een domein maken bronhouders, aanbieders en afnemers [onderlinge afspraken](#) om ervoor te zorgen dat gegevens optimaal kunnen worden uitgewisseld. De voorwaarden voor het gebruik van gegevens worden [expliciet gemaakt](#), zodat daar geen verwarring over kan bestaan. Dat kunnen rechten, plichten en beperkingen zijn. De eindverantwoordelijkheid voor deze gebruiksvoorwaarden ligt bij de bronhouder, maar ook de aanbieder kan bepaalde voorwaarden toevoegen. Als specifieke afspraken nodig zijn tussen partijen, bijvoorbeeld omdat persoonsgegevens worden uitgewisseld, dan worden deze ook [vastgelegd](#). Bronhouders stellen overeenkomsten op met aanbieders en aanbieders stellen overeenkomsten op met afnemers. Bij het verlenen van toegang tot de gegevens door de aanbieder, wordt een deel van de afspraken gecontroleerd. Als er discussie ontstaat over of (gevoelige) gegevens zijn uitgewisseld dan kan teruggevallen worden op [logs](#) die aanbieders en afnemers hebben vastgelegd en waarmee de onweerlegbaarheid van uitwisselingen kan worden geborgd.

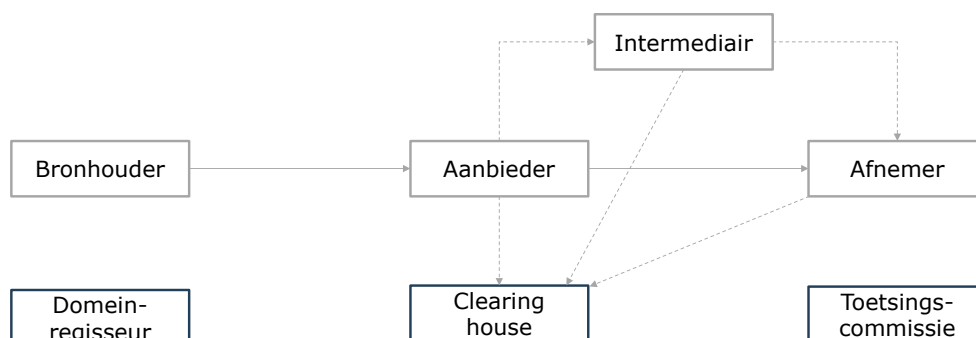
Een belangrijke categorie van het maken van afspraken is het definiëren van begrippen en het opstellen van informatie- en gegevensmodellen. Het is afhankelijk van de context of een

bronhouder daarbij eindverantwoordelijk is voor deze modellen of dat deze verantwoordelijkheid in een samenwerkingsverband of bij een derde partij ligt (zoals een ministerie). Het beleggen van deze verantwoordelijkheid bij de bronhouder is vooral logisch als deze de enige partij is die de betreffende soort gegevens beheert. In alle gevallen zijn de begrippen zoals aanwezig in wet- en regelgeving leidend.

Er kan voor gegevensuitwisseling gebruik worden gemaakt van intermediairs. Deze kunnen allerlei taken en verantwoordelijkheden hebben en kunnen deze ook als diensten beschikbaar stellen. Er is een onderscheid tussen intermediairs die alleen een technische rol vervullen en intermediairs die ook inhoudelijke bewerkingen op gegevens uitvoeren. Intermediairs moeten er voor zorgen dat de gegevens die ze beschikbaar stellen [herleidbaar zijn tot het informatie-object in de bron](#). Daarmee kunnen aanvullende (actuele of historische) gegevens bij de bron opgevraagd worden. Intermediairs die inhoudelijke bewerkingen uitvoeren creëren een nieuwe (afgeleide) bron, omdat zij feitelijk nieuwe gegevens creëren. De verantwoordelijkheid voor deze nieuwe bron moet expliciet worden belegd. Deze intermediairs moeten er ook voor zorgen dat de betekenis van de originele gegevens wordt gerespecteerd bij de nieuwe gegevens die ze creëren.

We zien nieuwe rollen ontstaan in de context van de Europese gegevensruimtes, die breder toepasbaar zijn. Zo benoemt bijvoorbeeld de International Data Spaces Association de rol Dataspace Authority die verantwoordelijk is voor het definiëren van het afsprakenstelsel voor een gegevensruimte. Een dergelijke domeinregisseur is essentieel om gegevensuitwisseling in een domein goed te laten werken. Ze benoemen verder de rol van Clearing House, dat verantwoordelijk is voor [het vastleggen van de gegevensuitwisselingen](#), zodat er geen discussie kan zijn over de gegevensuitwisselingen die hebben plaatsgevonden. Een clearing house houdt logfiles bij op basis van gegevens van aanbieders en afnemers. Deze informatie kan ook worden gebruikt om de gegevensuitwisseling financieel te verrekenen tussen partijen.

In de context van privacy en ethiek zien we de rol ontstaan van toetsingscommissies, die afwegen of gegevensuitwisselingen passen binnen de AVG en morele waarden. In de basis ligt de verantwoordelijkheid voor dit soort toetsingen bij de afnemer, die een hiervoor een dergelijke commissie kan inrichten. Domeinen kunnen besluiten om zelf organisatie-overstijgende commissies in te richten. Voorafgaand aan toetsing is nodig dat van gegevensuitwisselingen de juridische grondslag duidelijk gemaakt wordt, in ieder geval als persoonsgegevens uitgewisseld worden. De volgende figuur geeft een overzicht van de aanvullende rollen zoals hiervoor beschreven. Deze zijn een aanvulling op de landelijke organisatorische stelselfuncties zoals geschetst in het kader van het federatief datastelsel, zoals de marktmeester en de poortwachter.



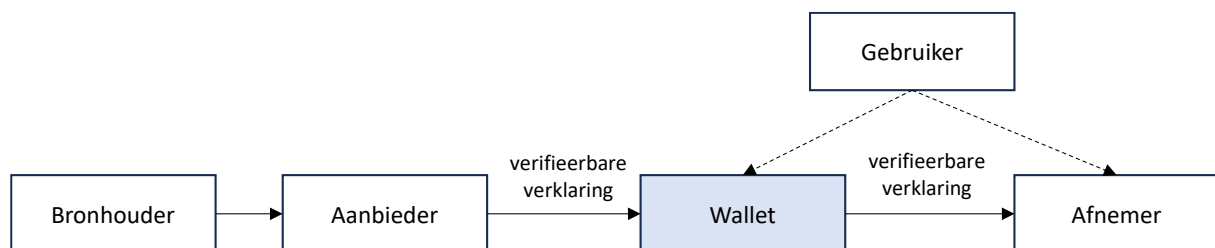
Figuur 3: Aanvullende rollen

4.1.3 Nieuwe uitwisselpatronen

Er ontstaan een aantal nieuwe uitwisselpatronen, onder andere gedreven vanuit de Europese wet- en regelgeving. De herziene [eIDAS verordening](#) verplicht de lidstaten om een European Digital

Identity Wallet (EDI-wallet) beschikbaar te stellen aan burgers en ondernemers. Zij krijgen met deze wallet meer [regie over hun eigen gegevens](#). Ze bepalen zelf welke gegevens ze in hun wallet laden en kunnen vervolgens kiezen om (delen van) de gegevens vrij te geven aan afnemers (dienstverleners). De gegevens worden door aanbieders beschikbaar gesteld in de vorm van verifieerbare verklaringen. Figuur 4 geeft een schets van het patroon dat hiermee ontstaat. Dit patroon is alleen relevant voor gegevensuitwisselingen waarvoor geen wettelijke grondslag bestaat. Voor de uitvoering van wettelijke taken zullen overheidsorganisaties direct gegevens blijven uitwisselen. Het gebruik van de wallet is verder op basis van vrijwilligheid. Het inzetgebied van de wallet is breder dan alleen gegevensuitwisseling. Het kan ook gebruikt worden als een identificatiemiddel, voor machtigen en vertegenwoordigen, en voor elektronisch ondertekenen. De wallet functioneert op het hoogste betrouwbaarheidsniveau (eIDAS hoog). Acceptatie van de wallet is verplicht voor publieke en optioneel voor private dienstverleners. Voor gebruikers Lidstaten moeten de wallet uiterlijk in 2026 geïmplementeerd hebben.

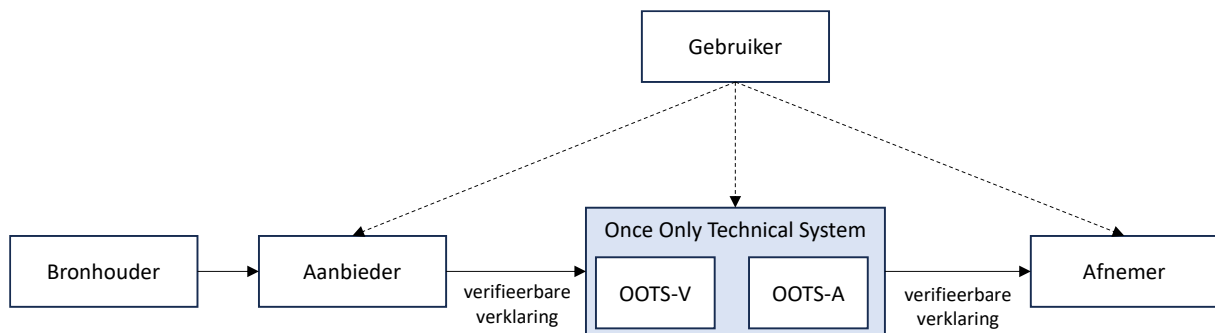
Met de herziene eIDAS verordening gaat de Europese commissie een stap verder dan in het verleden in het voorschrijven van standaarden, protocollen en voorzieningen voor gegevensuitwisseling. Aanbieders moeten de gegevens op de voorgeschreven manier leveren en afnemers moeten ze accepteren. Dat geldt niet alleen voor grensoverschrijdend gebruik van de wallet, maar ook nationaal. Hiermee neemt Europa een grote stap van het regelen van de onderlinge interoperabiliteit naar Europese integratie.



Figuur 4: De rol van de EDI wallet in gegevensuitwisseling

De [Single Digital Gateway verordening](#) zorgt ervoor dat iedereen in de EU op dezelfde manier toegang heeft tot een digitale overheidsdiensten waarvoor de verordening geldig is. Informatie en procedures moeten online worden aangeboden en toegankelijk zijn via het portaal Your Europe. Het Once Only Technical System (OOTS) zorgt ervoor dat gegevens maar één keer hoeven te worden verstrekt aan de overheid. Bevoegde instanties die de gedefinieerde diensten verlenen, moeten hun gebruikers de mogelijkheid geven om de benodigde gegevens direct bij de aanbieder in een andere lidstaat op te halen. Als de gebruiker hiervoor kiest, dan stuurt de dienstverlener de aanbieder een leveringsverzoek en stuurt de gebruiker naar een website van de aanbieder. Daar krijgt de gebruiker een voorinzagemogelijkheid. Na instemming van de gebruiker, stuurt de aanbieder de gegevens en de gebruiker terug naar de dienstverlener. Figuur 5 geeft een schets van het patroon dat hiermee ontstaat. Voor deze uitwisseling ontwikkelt de Europese Commissie samen met de lidstaten een gedecentraliseerd netwerk van eDelivery toegangspunten met ondersteunende voorzieningen. Eind 2023 is een eerste kleinschalige OOTS-implementatie gedaan voor het leveren van bedrijfsinformatie.

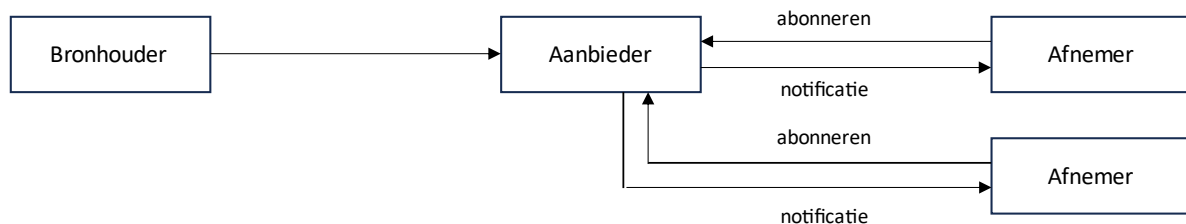
Het OOTS en de EUDI-wallet hebben elk een eigen toepassingsgebied. Daarom kunnen ze elkaar niet in alle gevallen vervangen. Verder is de verwachting dat er verschillende gebruikersvoorkeuren zijn voor die diensten waarvoor beide instrumenten ingezet mogen worden en daardoor een mix ontstaat in de toepassing van OOTS en de EDI-wallet.



Figuur 5: De rol van het Once Only Technical System in gegevensuitwisseling

Het uitwisselpatroon dat OOTS ondersteunt is eigenlijk een algemener patroon, dat ook los van de Europese context relevant is. Dit meer algemene patroon is dat een gebruiker eerst een voorinzage (preview) van gegevens krijgt en op basis daarvan expliciet moet instemmen met de uitwisseling van gegevens. De uitwisseling zelf vindt in dit patroon direct tussen de aanbieder en afnemer plaats. Dit patroon biedt gebruikers regie over hun eigen gegevens. Een voorbeeld waarin dit meer algemene patroon is toegepast is EMREX. Dit is een operationeel uitwisselingsnetwerk dat wordt gebruikt voor grensoverschrijdende uitwisselingen in het onderwijs van onder meer diploma's en vakresultaten. Het diplomaregister van DUO is breed toegankelijk in EMREX. De Europese Commissie en EMREX hebben samengewerkt aan een 'brug' die het mogelijk maakt dat bewijs uit EMREX in OOTS beschikbaar komt. Dit maakt het voor EMREX aanbieders makkelijk om aan hun OOTS-verplichting te voldoen. Inmiddels worden miljoenen Europese diploma's digitaal via EMREX beschikbaar gesteld.

Een inzicht is dat het standaard uitwisselpatroon dat hoort bij RESTful API's niet goed past op alle situaties. Er zijn andere vormen van gegevensuitwisseling die in bepaalde situaties de voorkeur hebben. Een voorbeeld hiervan is [gebeurtenisnotificatie](#), dat op zich niet nieuw is maar wel nieuwe relevantie krijgt. Het kernidee van deze vorm van gegevensuitwisseling is dat de afnemer niet om gegevens vraagt, maar zich alleen abonneert op bepaalde soorten gebeurtenissen die vervolgens door de aanbieder worden verspreid naar alle geabonneerde partijen. Dit patroon is belangrijk om afnemers te informeren over plaatsgevonden gebeurtenissen waarop zij mogelijk moeten acteren. Deze vorm van gegevensuitwisseling wordt belangrijker gegeven dat er meer aandacht ontstaat voor (levens)gebeurtenissen en pro-actieve dienstverlening. Het pro-actief leveren van diensten vraagt immers dat gereageerd wordt op relevante gebeurtenissen.



Figuur 6: Gebeurtenisnotificatie

Er ontstaan ook nieuwe interactiepatronen om op een andere manier met privacy om te gaan. Er zijn allerlei Privacy Enhancing Technologies (PET's) die hiervoor mechanismen bieden. Het [Nationaal innovatiecentrum voor PET's \(Nicpet\)](#) is een goede bron voor informatie en advies. Een voorbeeld van een PET is Multi Party Computation (MPC). Dit is een cryptografische techniek die partijen in staat stelt gezamenlijke berekeningen uit te voeren op gedeelde gegevens, zonder deze daadwerkelijk te onthullen. Het creëert een veilige omgeving waarin partijen gezamenlijke berekeningen kunnen uitvoeren zonder de onderliggende gegevens met elkaar te delen. De techniek versleutelt lokaal de gegevens van de partijen en deelt de versleutelde gegevens over

verschillende partijen. Berekeningen worden lokaal bij de partijen zelf uitgevoerd op deze versleutelde gegevens, en alleen het eindresultaat wordt met alle partijen gedeeld. Dit waarborgt zowel de privacy van de individuele partijen als de vertrouwelijkheid van de gegevens.

4.1.4 De rol van metagegevens in gegevensuitwisseling

Gegevensuitwisseling kan alleen werken als er ook metagegevens zijn die bepalen wat de gegevens betekenen, hoe met hun uitwisseling wordt omgegaan en wat daarvoor de wettelijke grondslag is. Metagegevens zijn een belangrijke basis onder [de FAIR-principes](#). Door datasets en gegevensdiensten te publiceren in relevante catalogi zijn ze vindbaar. Door in de metagegevens te verwijzen naar [begrippen](#), informatie- en gegevensmodellen worden gegevens meer interoperabel. Door het opnemen van metagegevens over de beperkingen, rechten en plichten die van toepassing zijn worden de gegevens ook beter herbruikbaar. Belangrijk is dat metagegevens [begrijpelijk zijn verwoord zodat ze eenvoudig kunnen worden begrepen](#). Ook in de uitwisseling zelf spelen metagegevens een belangrijke rol. Ze kunnen aangeven waar gegevens vandaan komen, hoe ze zijn ontstaan en wanneer ze zijn uitgewisseld. Hierdoor zorgen metagegevens ook voor herleidbaarheid en geloofwaardigheid van gegevens.

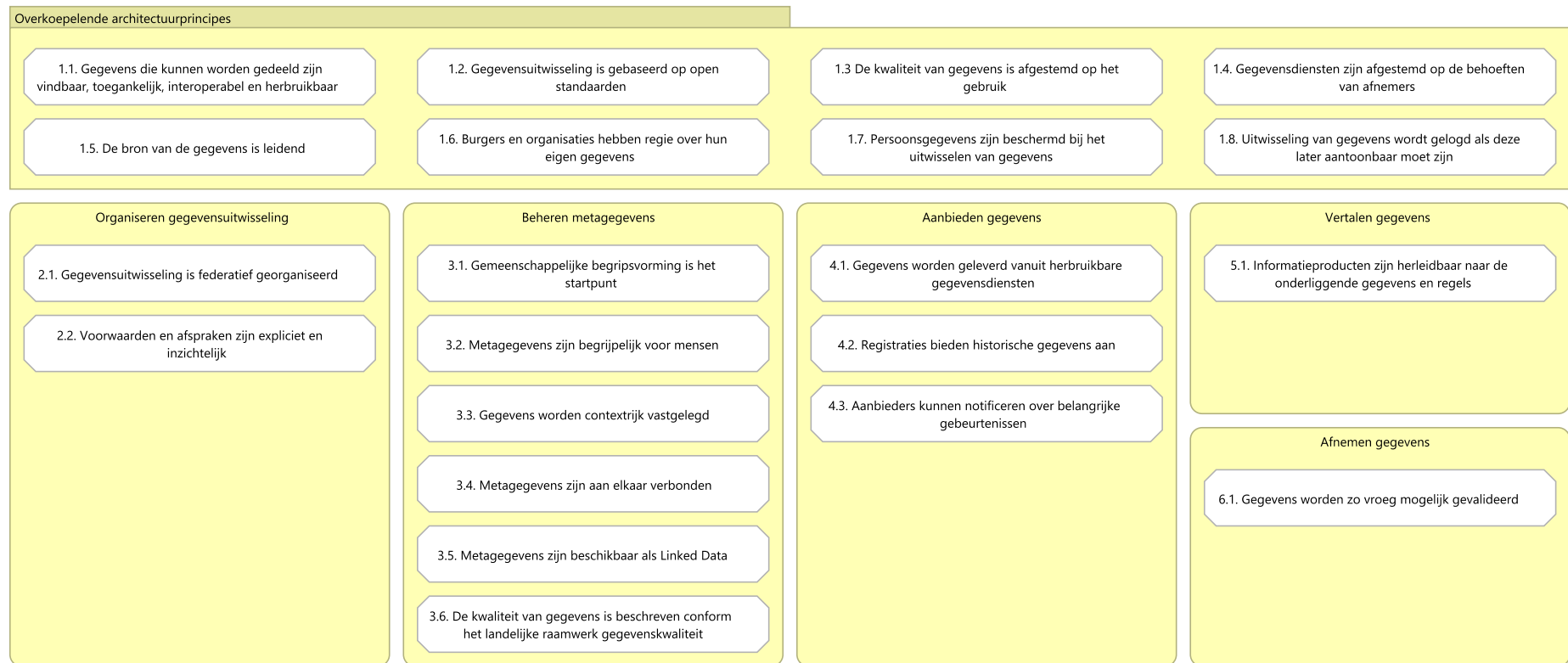
Begrippen, informatie- en gegevensmodellen zijn zelf ook een vorm van metagegevens. Ze beschrijven de betekenis en structuur van de gegevens. Begrippen zijn daarbij het [startpunt voor gemeenschappelijke begripsvorming](#). Zij zijn deels expliciet of impliciet aanwezig in wet- en regelgeving, waardoor ze een formele status hebben. Door informatie- en gegevensmodellen te [verbinden](#) aan deze begrippen wordt hun betekenis duidelijker. Als ook verbindingen worden gelegd vanuit gegevensmodellen naar schema's en uiteindelijk ook naar de individuele gegevens zelf is deze betekenis in de gehele keten geborgd. Het wordt dan ook mogelijk voor een eindgebruiker om de betekenis van een individueel gegeven op zijn scherm, in een rapportage of dashboard op te vragen. Als er daarnaast ook metagegevens over de herkomst van gegevens beschikbaar zijn, dan kan een eindgebruiker ook direct zien hoe de gegevens tot stand zijn gekomen: op basis van welke bronnen en welke regels.

Er zijn een aantal landelijke catalogi beschikbaar voor het publiceren van metagegevens. Zo kunnen begrippen en gegevensmodellen worden ontsloten via de stelselcatalogus. Metagegevens over datasets en gegevensdiensten zijn vindbaar via catalogi zoals [data.overheid.nl](#), [developer.overheid.nl](#) en het Nationaal Geo Register. Deze catalogi zullen in de toekomst [meer worden geïntegreerd](#) waardoor er meer integraal zicht is op alle vormen van metagegevens. Daarnaast is er een beweging naar een meer federatieve opzet van catalogi, waarbij ze op allerlei niveaus kunnen bestaan, naar elkaar kunnen verwijzen of elkaar kunnen harvesten. Datasets die alleen binnen een organisatie of domein relevant zijn hoeven daarbij ook niet breder vindbaar of toegankelijk te zijn. Domeinen kunnen ook zelf metagegevens catalogi bieden, voor gegevens die specifiek binnen een domein relevant zijn.

4.2 Architectuurprincipes

Architectuurprincipes zijn richtinggevende uitspraken die vooral uiting geven aan een streven. Ze bestaan uit een stelling die uiting geeft aan de overtuiging die eraan ten grondslag ligt, een rationale die meer informatie geeft over de drijfveren en implicaties die de consequenties beschrijven. Architectuurprincipes moeten als argument worden meegenomen in het maken van keuzes. De architectuurprincipes zijn in de domeinarchitectuur waar mogelijk gekoppeld aan de relevante wet- en regelgeving waar ze invulling aan geven en aan de functies die ingericht moeten zijn om ze te implementeren. Er is in de bijlagen ook een mapping opgenomen van deze architectuurprincipes op de uitgangspunten in de Architectuur Digitale Overheid 2030 en de principes en implicaties in NORA. Deze geeft een verdere onderbouwing en verdieping van de architectuurprincipes.

Figuur 7 geeft een overzicht van de architectuurprincipes en hun relatie met de belangrijkste functies voor gegevensuitwisseling. Een aantal principes hebben een brede impact en zijn als overkoepelend weergegeven.



Figuur 7: Overzicht van architectuurprincipes en relatie met functies

Principe 1.1. Gegevens die kunnen worden gedeeld zijn vindbaar, toegankelijk, interoperabel en herbruikbaar

Rationale Het beschikbaar stellen van gegevens voor hergebruik leidt tot meer transparantie, efficiëntie en innovatie. De wet open overheid onderstreept het belang van openbaarheid van publieke informatie voor de democratische samenleving. Voor het kunnen hergebruiken van gegevens zijn hun vindbaarheid, toegankelijkheid, interoperabiliteit en herbruikbaarheid zoals bedoeld met de [FAIR-principes](#) essentieel. Zij zorgen ervoor dat anderen in staat zijn om te begrijpen wat eigenschappen van de gegevens zijn, wat ze betekenen en of ze bruikbaar zijn voor hun eigen doeleinden. Ze zorgen er ook voor dat de gegevens eenvoudig verkregen kunnen worden.

- Implicaties*
1. Gegevens zijn voorzien van metagegevens, en zijn gepubliceerd in relevante catalogi; gegevens die landelijk waardevol zijn, zijn landelijk vindbaar (vindbaar).
 2. Gegevens en hun metagegevens zijn voorzien van wereldwijd unieke en stabiele identificaties (vindbaar).
 3. Metagegevens zijn rijk en bevatten ook informatie over de context, het oorspronkelijke gebruiksdoel, kwaliteit en karakteristieken van gegevens (vindbaar).
 4. Gegevens kunnen worden benaderd via standaard, open en algemeen implementeerbare protocollen (toegankelijk).
 5. Gegevens zijn beschreven in een gegevensmodel waarin hun syntax en betekenis zijn gedefinieerd en dat beschikbaar is een gestandaardiseerd open formaat zoals MIM (interoperabel).
 6. Metagegevens beschrijven gebruiksbeperkingen, -rechten en -plichten en de herkomst van de gegevens (herbruikbaar).

Principe 1.2. Gegevensuitwisseling is gebaseerd op open standaarden

Rationale Het tot stand brengen van uitwisseling van gegevens kost vaak veel inspanning, doordat gegevens ontworpen zijn in een eigen context en er allerlei vertalingen nodig zijn om ze bruikbaar te maken in een andere context. Door gebruik te maken van uitwisselstandaarden wordt de variatie beperkt en zijn er minder vertalingen nodig. Open standaarden zorgen er ook voor dat leveranciersafhankelijkheden zoveel mogelijk worden voorkomen. In Nederland is het sturen op standaarden geformaliseerd in Forum Standaardisatie, die veel energie stopt in het bepalen en aanwijzen van standaarden die breed zouden moeten worden ingezet. In de Wet digitale overheid is beschreven dat in algemene maatregelen van bestuur bepaalde standaarden ook wettelijk verplicht kunnen worden gesteld.

- Implicaties*
1. De standaarden op de "pas toe of leg uit" lijst van Forum Standaardisatie worden als eis meegegeven bij de selectie of ontwikkeling van systemen en gegevensuitwisselingen (of er wordt expliciet uitgelegd waarom ze niet van toepassing zijn).
 2. De standaarden op de lijst van aanbevolen standaarden worden serieus overwogen en de overweging tot al dan niet gebruik van de aanbevolen standaarden wordt vastgelegd.
 3. De standaarden zoals beschreven in de streefbeeldafspraken worden per direct doorgevoerd op alle ICT-systemen en -diensten.

4. Als er in een specifieke context geen toepasbare standaarden op de lijsten van Forum Standaardisatie staan, dan wordt gebruik gemaakt van internationale standaarden, of anders nationale standaarden en wordt overwogen deze aan te melden bij Forum Standaardisatie.
5. Nederlandse standaarden zijn voorbereid op gebruik in andere landen en er wordt onderzocht of deze kunnen worden ingebracht in internationale standaardisatie-organisaties.
6. Als er nog geen standaard bestaat voor een specifiek gebied, dan wordt onderzocht of er zelf een standaard kan worden ontwikkeld.

Principe 1.3 De kwaliteit van gegevens is afgestemd op het gebruik

Rationale Het is belangrijk dat gebruikers beschikken over gegevens die optimaal aansluiten bij hun eigen behoeften en gebruik. Daarbij is de kunst om een balans te vinden tussen kwaliteit en kosten. Een hele hoge kwaliteit leidt al snel tot onacceptabele kosten. De vraag is dus wat nodig is in een specifieke context. Dit vraagt vooral bewuste afwegingen. Als slechts een klein deel van de gebruikersgroep hoge eisen stelt, dan is de vraag of dat hogere kosten voor alle gebruikers rechtvaardigt. Daarnaast zijn er ook eisen waar bronhouders gewoonweg niet aan kunnen voldoen. Het terugmelden van mogelijke fouten is een belangrijke maatregel voor het verhogen van de gegevenskwaliteit. In meer algemene zin is afstemming tussen bronhouders en afnemers essentieel.

- Implicaties*
1. De eisen die gebruikers stellen aan de kwaliteit van gegevens worden door de (afnemer)organisatie gebundeld en expliciet gemaakt in elke gebruikscontext.
 2. Als afnemers specifieke kwaliteitseisen stellen en overeenkomen met de bronhouder dan worden deze vastgelegd in een overeenkomst met de aanbieder.
 3. De huidige kwaliteit van gegevens wordt expliciet gemeten en inzichtelijk gemaakt in de metagegevens, op een voor gebruikers begrijpelijke wijze.
 4. Aanbieders bieden de mogelijkheid om vermoedelijke fouten in registraties terug te melden (ook aan burgers en bedrijven) en routeren meldingen naar de verantwoordelijke bronhouder.
 5. Als er een verschil is tussen de eisen die worden gesteld vanuit gebruik en de huidige kwaliteit dan vindt hierover afstemming tussen bronhouder en afnemers plaats en wordt een afweging tussen kosten en baten van mogelijke maatregelen gemaakt.
 6. Er is periodieke afstemming tussen bronhouders en afnemers over de mate waarin gegevens (blijven) voldoen aan de gestelde kwaliteitseisen.

Principe 1.4. Gegevensdiensten zijn afgestemd op de behoeften van afnemers

Rationale Afnemers willen worden ondersteund in hun specifieke informatie- of gegevensbehoefte. Ze willen deze bij voorkeur met een zo klein mogelijke inspanning ontvangen en gegevens liever ook niet zelf combineren en vertalen, als andere partijen dat voor ze kunnen doen tegen dezelfde of lagere kosten. Ze ontvangen gegevens bij voorkeur ook in hun eigen taal en in een formaat dat ze zelf direct kunnen gebruiken. Ze willen ook niet geconfronteerd worden met gegevens die ze niet nodig hebben. Dat sluit ook niet aan bij het principe van dataminimalisatie zoals beschreven in de AVG en levert alleen maar extra complexiteit en afhankelijkheden. Tegelijkertijd is ook de herbruikbaarheid van gegevensdiensten belangrijk en zal er dus een balans moeten worden gevonden tussen generiek en specifiek. Als slechts

een klein deel van de afnemers specifieke eisen stelt dan is het de vraag of dat hogere kosten voor alle afnemers rechtvaardigt.

- Implicaties*
1. De inhoud, omvang, taal, formaat en protocol van gegevensdiensten zijn afgestemd op de informatie- of gegevensbehoeften van groepen van afnemers.
 2. Als meerdere afnemers een soortgelijke informatie- of gegevensbehoefte hebben dan wordt onderzocht of hiervoor een gemeenschappelijke gegevensdienst kan worden ingericht.
 3. Als meerdere afnemers gegevens willen in een andere taal, formaat of protocol dan de aanbieder kan of wil leveren dan wordt onderzocht of een voorziening deze vertalingen kan verzorgen.

Principe 1.5. De bron van de gegevens is leidend

Rationale Het is belangrijk dat duidelijk is waar gegevens vandaan komen. Gegevens worden onderhouden in een bron. De bron is de plaats waar de kwaliteit van gegevens wordt bewaakt. Specifieke eisen m.b.t. performance of beschikbaarheid kunnen het lastig maken om gegevens technisch ook direct uit de bron op te halen. In een bepaalde gebruikscontext kan een gegevensdienst op een gecontroleerde kopie als verstrekkingpunt worden aangewezen (ervan uitgaande dat deze voldoet aan de gestelde kwaliteitseisen). De bron is wel de plaats waarnaar gerefereerd moet worden, omdat het de plaats is waar gegevens hun legitimiteit aan ontleen. Als een intermediair gegevens inhoudelijk bewerkt (op basis van afleidingsregels) dan ontstaan er feitelijk andere gegevens en dus een nieuwe (afgeleide) bron.

- Implicaties*
1. Er zijn bronnen aangewezen voor specifieke soorten gegevens.
 2. In gebruikscontexten kunnen verstrekkingpunten worden aangewezen voor specifieke gegevens, waarbij wettelijke bepalingen leidend zijn.
 3. Verstrekkingpunten zijn gecontroleerd, voldoen aan gestelde kwaliteitseisen en daar wordt periodiek op gemonitord.
 4. Gegevens worden opgehaald bij en/of ontvangen van de bron of een verstrekkingpunt.
 5. Als gegevens met een hoge actualiteit (of juist historische gegevens) nodig zijn dan worden deze direct bij de bron of een verstrekkingpunt geraadpleegd.
 6. Het verwijzen naar een bron heeft de voorkeur boven het maken van een kopie van gegevens uit die bron.
 7. Er wordt geen lokale kopie van gegevens gemaakt, tenzij er specifieke eisen zijn die daarom vragen.
 8. Raadplegen, zoeken en selecteren van gegevens bij een bron heeft de voorkeur boven het uitwisselen van gegevens.
 9. Het is voor gebruikers duidelijk op welke bronnen de gegevens die zij zien zijn gebaseerd.

Principe 1.6. Burgers en organisaties hebben regie over hun eigen gegevens

Rationale De Europese datastrategie stelt dat mensen meer invloed moeten krijgen over hun gegevens en dat zij daarom middelen en bevoegdheden nodig hebben om te beslissen wat er met hun gegevens gebeurt, als er geen wettelijke grondslag is voor hun verwerking. Voor burgers zijn rechten bij de verwerking van persoonsgegevens voor een deel al geborgd in de AVG. In de herziene eIDAS-verordening krijgen burgers en organisaties verdergaande de mogelijkheid om hun gegevens via eigen wallets te verstrekken aan partijen. Dat is met name relevant voor private dienstverleners, omdat overheidsorganisaties vanuit hun wettelijke taak gegevens direct mogen uitwisselen. Datasoevereiniteit is een belangrijk uitgangspunt bij gegevensruimtes en betekent dat organisaties zelf willen kunnen bepalen aan wie ze hun gegevens verstrekken.

- Implicaties*
1. Private afnemers bieden burgers of organisaties de keuzemogelijkheid om gegevens over henzelf via een wallet aan te leveren.
 2. Publieke afnemers die gegevens over burgers of organisaties nodig hebben, die nog niet bekend zijn bij de overheid bieden de keuzemogelijkheid om gegevens via een wallet aan te leveren.
 3. Aanbieders bieden burgers en organisaties de mogelijkheid om hun gegevens te downloaden inclusief een verifieerbare verklaring, zodat ze deze zelf kunnen delen met partijen of opnemen in hun wallet.
 4. Burgers (en liefst ook organisaties) kunnen hun gegevens inzien en hebben inzicht in wanneer, met wie en waarom gegevens over henzelf zijn uitgewisseld.
 5. Organisaties zorgen dat toegang tot gevoelige gegevens alleen mogelijk is nadat de daaraan gerelateerde autorisatieregels zijn gecontroleerd.

Principe 1.7. Persoonsgegevens zijn beschermd bij het uitwisselen van gegevens

Rationale De Europese datastrategie stelt dat het belang van de burger altijd op de eerste plaats moet komen, in overeenstemming met de Europese waarden, grondrechten en regels. Het is belangrijk om te voldoen aan eisen rondom privacy en informatiebeveiliging bij het uitwisselen van gegevens. Daarbij vragen met name persoonsgegevens aandacht omdat deze inherent privacygevoelig zijn en de uitwisseling alleen onder specifieke condities mogelijk is. Anderzijds wordt privacy vaak onterecht als blokkade gezien voor de uitwisseling van gegevens. Eisen aan de bescherming van persoonsgegevens (en daarmee privacy) zijn gesteld in de Algemene Verordening Gegevensbescherming.

- Implicaties*
1. De wettelijke grondslag en doelbinding van de gegevensuitwisseling zijn expliciet gemaakt door de afnemer, die deze op een later moment ook kan aantonen.
 2. Voorafgaand aan het uitwisselen van gegevens vindt expliciete toetsing op privacy (door afnemer) en informatiebeveiliging plaats.
 3. Gegevensdiensten die persoonsgegevens ontsluiten zijn alleen toegankelijk voor geauthenticeerde en geautoriseerde afnemers.
 4. Gegevens die worden uitgewisseld zijn geclassificeerd (in termen van beschikbaarheid, integriteit en vertrouwelijkheid) en op basis van deze classificatie zijn relevante maatregelen genomen.
 5. De persoonsgegevens die worden uitgewisseld zijn geanonimiseerd, gepseudonimiseerd of versleuteld (kan ook op transportniveau).

6. De persoonsgegevens die worden uitgewisseld zijn beperkt tot het hoogst noodzakelijke.
7. Waar mogelijk en waardevol wordt gebruik gemaakt van Privacy Enhancing Technologies om privacy te borgen.

Principe 1.8. Uitwisseling van gegevens wordt gelogd als deze later aantoonbaar moet zijn

Rationale Logging van gegevensuitwisselingen (verzendingen en ontvangsten) maakt het mogelijk om op een later moment aan te tonen dat gegevensuitwisselingen hebben plaatsgevonden (onweerlegbaarheid). Dat is met name relevant bij de uitwisseling van persoonsgegevens, maar bijvoorbeeld ook bij het aanleveren van gegevens aan een landelijke registratie. Het faciliteert verder foutanalyse, procesanalyse, misbruikdetectie, forensisch onderzoek en onderlinge verrekening van diensten. Auditlogging is in het algemeen een plicht vanuit het perspectief van informatiebeveiliging.

- Implicaties*
1. Bronhouders afspraken maken met aanbieders over onweerlegbaarheid en logging.
 2. Aanbieders loggen (metagegevens van) berichten die zijn verzonden, afnemers loggen (metagegevens van) berichten die zijn ontvangen als de uitwisseling later aantoonbaar moet zijn.
 3. De logs van verzonden en ontvangen berichten zijn aan elkaar te relateren op basis van een gemeenschappelijke identificatie, zodat berichten die volgen uit één trigger aan elkaar gerelateerd kunnen worden.
 4. Als hoge eisen aan onweerlegbaarheid worden gesteld dan worden aanvullende maatregelen overwogen, zoals het ondertekenen van berichten of het delegeren van logging naar een derde partij (clearing house).
 5. De bewaartermijn van logs wordt expliciet bewaakt en gerespecteerd.

Principe 2.1. Gegevensuitwisseling is federatief georganiseerd

Rationale De Europese datastrategie beoogt gegevensuitwisseling tussen en binnen sectoren te stimuleren middels gegevensruimtes. Inherent ligt de kennis van specifieke gegevens bij partijen in specifieke domeinen. Het is daarom het meest logisch om domeinen zelf verantwoordelijkheid te geven voor hun eigen gegevens. Binnen domeinen gelden ook specifieke eisen en zijn specifieke afspraken nodig. Tegelijkertijd zouden bepaalde gegevens ook buiten domeinen beschikbaar moeten zijn voor hergebruik. Samenwerkingen in domeinen kunnen starten tussen twee partijen, maar hebben vaak de potentie om te groeien. Voor het creëren van duurzame samenwerkingen is het afstemmen met andere mogelijke partijen belangrijk. Als wordt samengewerkt dan kunnen kosten en baten op een eerlijke manier worden gedeeld en kan worden geprofiteerd van schaalvoordeel. Hierdoor kunnen de drempels tot verdere samenwerking worden verlaagd voor nieuwe spelers.

- Implicaties*
1. Gegevens worden decentraal, in domeinen, beheerd door partijen met de inhoudelijke domeinkennis.
 2. Domeinen zijn er zelf voor verantwoordelijk om hun gegevens aan te bieden, conform landelijke afspraken en standaarden voor breder hergebruik.
 3. Binnen domeinen wordt expliciete samenwerking gezocht tussen partijen die behoefte hebben aan dezelfde soorten gegevens.

4. Er is een domeinregisseur die de leiding neemt in het organiseren van de samenwerking en het maken, monitoren, evalueren en bijstellen van afspraken.
5. Er wordt breed afgestemd met partijen in het domein om te komen tot samenwerkingsafspraken, zodat deze duurzaam zijn.
6. Er wordt onderzocht of er binnen de context van specifieke samenwerkingsverbanden specifieke voorzieningen wenselijk zijn die gegevensuitwisseling kunnen vereenvoudigen.
7. Er zijn binnen specifieke domeinen duidelijke en eerlijke afspraken over wie waarvoor betaalt, zodat bepaalde partijen niet met onevenredig hoge kosten worden geconfronteerd.

Principe 2.2. Voorwaarden en afspraken zijn expliciet en inzichtelijk

Rationale Bronhouders willen hun gegevens beschermen. Vanuit de AVG is belangrijk dat een verwerkingsverantwoordelijke duidelijke afspraken maakt met verwerkers in verwerkingsovereenkomsten. In meer algemene zin is belangrijk dat rechten, plichten en aansprakelijkheden goed zijn geborgd. Als bepaalde afspraken generiek kunnen worden gemaakt, landelijk of in de context van een domein, dan heeft dat de voorkeur omdat het de noodzaak tot bilaterale afspraken minimaliseert. Inzicht in overeengekomen gegevensuitwisselingen (gegevensdeelrelaties) is wenselijk om transparantie te bieden over (her)gebruik van gegevens aan partijen binnen en buiten de overheid. Als voorwaarden en afspraken in machineleesbare vorm beschikbaar zijn dan kunnen ze geautomatiseerd worden getoetst.

- Implicaties*
1. Bronhouders maken hun voorwaarden (rechten, plichten en beperkingen) expliciet en leggen relevante aspecten ervan vast als metagegevens.
 2. Afspraken worden bij voorkeur generiek gemaakt, landelijk of binnen een domein.
 3. Voorwaarden en aansprakelijkheden zijn in wetten, formele afspraken en/of overeenkomsten geborgd.
 4. Bronhouders en/of aanbieders maken waar nodig specifieke afspraken met afnemers, zoals over specifieke kwaliteitseisen.
 5. Overeengekomen gegevensuitwisselingen worden vastgelegd en publiek inzichtelijk gemaakt (tenzij daar specifieke beperkingen voor gelden).
 6. Waar mogelijk en waardevol worden relevante voorwaarden in machineleesbare vorm omgezet en geautomatiseerd getoetst bij de uitwisseling.
 7. Afspraken worden periodiek door aanbieder en afnemers getoetst aan de realisatie, geëvalueerd en bijgesteld.

Principe 3.1. Gemeenschappelijke begripsvorming is het startpunt

Rationale Taal is een belangrijke basis voor het creëren van wederzijds begrip. Het is tevens een essentiële basis voor gegevens, die een concrete invulling geven aan taal. Als we dus niet dezelfde begrippen hanteren of niet weten hoe bepaalde begrippen zich tot elkaar verhouden, dan zullen de gegevens ook niet uitwisselbaar zijn. Afstemming over begrippen zou zo vroeg mogelijk moeten starten, nog voordat wet- en regelgeving wordt opgesteld. Dat wat in de wet- en regelgeving is opgenomen is nu eenmaal de formele basis voor gegevens en informatievoorziening en kan niet eenvoudig van afgeweken worden. Standaardisatie van begrippen is niet altijd haalbaar, omdat ze vaak een specifieke contextuele betekenis hebben.

- Implicaties*
1. In alle domeinen worden de daarin gehanteerde begrippen expliciet gemaakt, inclusief de wet- en regelgeving waar zij op gebaseerd zijn.
 2. Begrippen worden gedeeld zodat deze vindbaar en toegankelijk zijn voor anderen.
 3. Begrippen worden gestandaardiseerd waar mogelijk zodat ze alleen van elkaar verschillen als er inherent andere betekenissen bij horen.
 4. Bij de ontwikkeling van wet- en regelgeving wordt multidisciplinair gewerkt aan gemeenschappelijke begripsvorming.
 5. In alle relevante documentatie, ontwerp en modellen in het domein wordt verwezen naar de begrippen, zodat ze beter vindbaar zijn en "by design" met elkaar samenhangen.
 6. Het eigenaarschap van begrippen wordt duidelijk belegd, zodat het beheer ervan geborgd is.

Principe 3.2. Metagegevens zijn begrijpelijk voor mensen

Rationale Gebruikers willen op basis van metagegevens bepalen wat gegevens betekenen voor hun eigen gebruik en moeten deze daarvoor kunnen begrijpen. In de praktijk worden gebruikers te vaak te snel doorverwezen naar technische specificaties en ontbreekt een begrijpelijke functionele uitleg. Specialisten hebben daarnaast ook een verantwoordelijkheid voor het onderhouden van metagegevens, en moeten deze metagegevens dus ook kunnen begrijpen om ze te kunnen aanpassen. Bepaalde metagegevens worden gegenereerd uit andere (hoger liggende) metagegevens en zijn daarmee automatisch op een hoger niveau gedocumenteerd. Denk bijvoorbeeld aan schema's, die worden gegenereerd op basis van een gegevensmodel.

- Implicaties*
1. Metagegevens op alle niveaus zijn voorzien van een definitie of omschrijving en als dat niet voldoende is, ook van een aanvullende toelichting en/of voorbeelden.
 2. Metagegevens zijn geformuleerd in begrijpelijke taal, passend bij de doelgroepen.
 3. Metagegevens zijn niet alleen beschikbaar in machineleesbare vorm, maar zijn ook voorzien van begrijpelijke documentatie.
 4. Metagegevens zijn vastgelegd volgens open standaarden, zodat ze een breed herkenbare structuur en betekenis hebben.
 5. Fysieke schema's verwijzen naar gegevensmodellen waarin hun betekenis is gedefinieerd.
 6. Omschrijvingen en toelichtingen in metadata zijn digitaal toegankelijk.

Principe 3.3. Gegevens worden contextrijk vastgelegd

Rationale Het is belangrijk om de context en daarmee de herkomst van gegevens te kennen om hun betekenis goed te begrijpen. Dat is in het algemeen het doel van metagegevens. Metagegevens worden echter vaak niet goed vastgelegd omdat gebruikers het nut ervan niet goed begrijpen of omdat het te veel inspanning kost om ze vast te leggen. Door context expliciet en geautomatiseerd vast te leggen in metagegevens wordt de afhankelijkheid van mensen voor het vastleggen van metagegevens beperkt. Het belang van het expliciet maken van context door deze vast te leggen in metagegevens is groter als de afstand tussen inwinning en gebruik groter is.

- Implicaties*
1. Er wordt per gebruikscontext expliciet nagedacht welke metagegevens belangrijk zijn en vastgelegd moeten worden.

2. Metagegevens worden zoveel mogelijk gedurende een bedrijfsproces geautomatiseerd afgeleid uit de context en opgeslagen bij gegevens.
3. Het vastleggen van metagegevens is geïntegreerd in de reguliere applicaties waar gebruikers mee werken.
4. Waar mogelijk en waardevol worden metagegevens gegenereerd op basis van kunstmatige intelligentie, bijvoorbeeld om relevante trefwoorden, samenvattingen of toelichtingen te genereren.
5. Metagegevens die niet automatisch kunnen worden afgeleid, worden expliciet door gebruikers aan de gecreëerde gegevens toegevoegd zoals omschrijvingen.
6. Er worden in de metagegevens relevante contextgegevens beschikbaar gesteld zoals de organisatie of persoon die de gegevens gecreëerd heeft en welke gebeurtenis en/of activiteit ten grondslag lag aan het vastleggen van de gegevens.
7. In alle schakels in de keten van bronhouder tot gebruiker wordt relevante context toegevoegd, zoals over de bewerkingen die hebben plaatsgevonden en door wie.

Principe 3.4. Metagegevens zijn aan elkaar verbonden

Rationale Gegevens hebben metagegevens nodig om betekenis te krijgen en bruikbaar te zijn. Er zijn allerlei soorten metagegevens die verschillende aspecten van gegevens modelleren, zoals metagegevens die de betekenis beschrijven, metagegevens die de structuur beschrijven en metagegevens die beschrijven welke datasets beschikbaar zijn. Dit soort metagegevens moeten in relatie tot elkaar geïnterpreteerd worden, om echt waardevol te zijn.

- Implicaties*
1. Modelelementen in informatie- en gegevensmodellen zoals objecttypes en attribuutsoorten refereren expliciet naar de gedefinieerde begrippen die ze representeren.
 2. In informatie- en gegevensmodellen wordt ook gerefereerd naar de beperkingsregels en afleidingsregels die van toepassing zijn.
 3. Bij metagegevens over datasets zijn ook metagegevens beschikbaar over de objecttypen en attribuutsoorten van de in de dataset aanwezige gegevens.
 4. Informatieobjecten zoals documenten en datasets zijn voorzien van begrippen zodat ze beter vindbaar zijn.
 5. Bij gegevens die worden uitgewisseld is een verwijzing aanwezig naar het gebruikte schema.
 6. Data-elementen in schema's verwijzen expliciet naar de objecttypen en attribuutsoorten die ze representeren.
 7. Er is bij de documentatie van diensten of operaties in gegevensdiensten beschreven welke beperkingsregels en afleidingsregels worden toegepast.

Principe 3.5. Metagegevens zijn beschikbaar als Linked Data

Rationale Het is belangrijk dat metagegevens aan elkaar verbonden zijn om maximaal context te geven aan gegevens en ze echt waardevol te maken. Praktisch is het daarvoor nodig om verbindingen te leggen tussen verschillende vormen van metagegevens. Linked Data standaarden zijn specifiek gericht op het verbinden van gegevens en zijn geoptimaliseerd om gegevens betekenisvol te publiceren op het web. Er zijn allerlei Linked Data standaarden die ook specifiek gericht zijn op metagegevens.

- Implicaties*
1. Metagegevens zijn beschikbaar in de wereldwijd veelgebruikte Linked Data vocabulaires voor metagegevens.
 2. Nederlandse standaarden voor metagegevens bieden (ook) een Linked Data vocabulaire.
 3. Voor wereldwijde standaarden voor metagegevens waarvoor geen Linked Data vocabulaires aanwezig zijn wordt een standaard vocabulaire ontwikkeld.
 4. Op de raakvlakken tussen de standaarden wordt middels webadressen (IRI's) verwezen naar gerelateerde metadatastandaarden.
 5. Metagegevens zijn vindbaar in landelijke catalogi zoals data.overheid.nl, developer.overheid.nl en de stelselcatalogus, die deze (ook) als Linked Data ontsluiten.

Principe 3.6. De kwaliteit van gegevens is beschreven conform het landelijke raamwerk gegevenskwaliteit

Rationale Het is belangrijk dat gebruikers eenvoudig inzicht kunnen krijgen in de kwaliteit van gegevens, zodat zij begrijpen of deze aansluiten bij hun eigen gebruik. Door de naamgeving en inhoud van dimensies voor gegevenskwaliteit te standaardiseren, zijn deze beter begrijpelijk voor afnemers. Het [NORA raamwerk gegevenskwaliteit](#) is gebaseerd op wereldwijde ISO standaarden, breed afgestemd binnen de Nederlandse overheid en is ook de basis voor het federatief datastelsel.

- Implicaties*
1. In de metagegevens van datasets zijn beschrijvingen van de kwaliteitseisen(normen) en gerealiseerde kwaliteit beschreven conform de structuur van het NORA raamwerk gegevenskwaliteit.
 2. Er is liefst ook een machineleesbare versie van de kwaliteit van de gegevens beschikbaar conform de DQV standaard.

Principe 4.1. Gegevens worden geleverd vanuit herbruikbare gegevensdiensten

Rationale Door vanuit hergebruik naar de clustering van functionaliteit en gegevens te kijken wordt voorkomen dat specifieke afnemers eigen specifieke gegevens en gegevensdiensten vragen. Hergebruik van gegevensdiensten is efficiënter en meer beheersbaar dan het gebruik van point-to-point koppelingen omdat het tot minder koppelingen leidt. Tegelijkertijd vraagt dataminimalisatie aandacht, waardoor hergebruik lastiger kan zijn.

- Implicaties*
1. Gegevensdiensten leveren een clustering van functionaliteit en gegevens die past bij de behoeften van een grote hoeveelheid afnemers.
 2. Gegevensdiensten worden kenbaar gemaakt in developer.overheid.nl, data.overheid.nl en als het geografische gegevens betreft ook in het Nationaal Geo Register.
 3. Aanbieders van gegevensdiensten bieden afnemers testfaciliteiten zoals een testomgeving, testdata en/of testscripts, met name als de gegevensdienst meer behelst dan het ontsluiten van open data.
 4. Gegevensdiensten die zijn gerealiseerd als RESTful API voldoen aan de Nederlandse API-strategie en de REST API Design Rules.
 5. Er zijn beschrijvingen van de serviceniveaus die gelden voor de gegevensdienst beschikbaar en deze serviceniveaus worden gemonitord door de aanbieder.

Principe 4.2. Registraties bieden historische gegevens aan

Rationale Registraties zijn de formele bron voor de gegevens die ze beheren. Formele registraties zoals sector- en basisregistraties zijn een belangrijke basis voor de Nederlandse overheid en er zal op allerlei manieren naar ze worden gerefereerd. Het is belangrijk dat er geen discussie kan ontstaan over welke gegevens er op een bepaald moment onderdeel waren van een registratie, ook in juridische zin.

- Implicaties*
1. Nieuwe formele overheidsregistraties die worden ontwikkeld leggen de formele historie van gegevens vast.
 2. Er wordt expliciet bepaald of er in een gebruikcontext behoefte is aan materiële historie.
 3. Er wordt bij het ontwikkelen van informatie- en gegevensmodellen expliciet rekening gehouden met historie.
 4. Registraties bieden de mogelijkheid om historische gegevens op te vragen.
 5. Gegevens worden niet fysiek verwijderd; als ze niet meer geldig zijn dan wordt alleen vastgelegd dat ze niet meer geldig zijn (tenzij ze om juridische redenen vernietigd moeten worden).
 6. De historische integriteit van gegevens is geborgd; oude gegevens worden niet overschreven.
 7. Gegevens en hun historie kunnen worden overgebracht naar een archief om hun duurzame toegankelijkheid te kunnen garanderen.

Principe 4.3. Aanbieders kunnen notificeren over belangrijke gebeurtenissen

Rationale Overheidsorganisaties willen worden geïnformeerd over gebeurtenissen waarop zij moeten acteren. De werkagenda waardegedreven digitaliseren stelt dat overheidsdienstverlening proactief zou moeten zijn en georganiseerd vanuit het perspectief van burgers en ondernemers o.a. aan de hand van levensgebeurtenissen. Dit betekent dat het belangrijk is om informatie over levensgebeurtenissen te delen.

- Implicaties*
1. Organisaties definiëren expliciet welke (levens)gebeurtenissen zij op willen acteren en welke gegevensuitwisselingen met andere organisaties hiervoor nodig zijn.
 2. Aanbieders verstrekken notificaties als belangrijke gebeurtenissen plaatsvinden.
 3. Er zijn mechanismen die borgen dat de notificaties daadwerkelijk worden ontvangen door afnemers.

Principe 5.1. Informatieproducten zijn herleidbaar naar de onderliggende gegevens en regels

Rationale Het is belangrijk dat afnemers van informatieproducten weten hoe deze tot stand zijn gekomen. Ze willen weten welke onderliggende brongegevens zijn gebruikt en welke afleidingsregels daarop zijn toegepast. Hierdoor kunnen ze beter inschatten of de resulterende gegevens aansluiten bij hun informatiebehoefte en of ze voldoende betrouwbaar zijn. Het geeft ze vertrouwen in de mate waarin het informatieproduct aansluit bij hun eigen gebruik. De kwaliteit van de onderliggende brongegevens bepalen de kwaliteit van het informatieproduct.

- Implicaties*
1. De afleidingsregels (en hun documentatie) die zijn gebruikt voor het creëren van het informatieproduct (vanaf de bron) zijn toegankelijk voor de afnemer.

2. In metagegevens van informatieproducten is expliciet gemaakt welke administraties zijn gebruikt.
3. Liefst zijn ook de specifieke onderliggende brongegevens die zijn gebruikt bij de afleiding toegankelijk voor de afnemer (daarbij rekening houdende met privacy).
4. Afleidingsregels zijn onder versiebeheer zodat ook historisch inzicht kan worden gegeven in hun werking (en de wet- en regelgeving waarop ze gebaseerd zijn).

Principe 6.1. Gegevens worden zo vroeg mogelijk gevalideerd

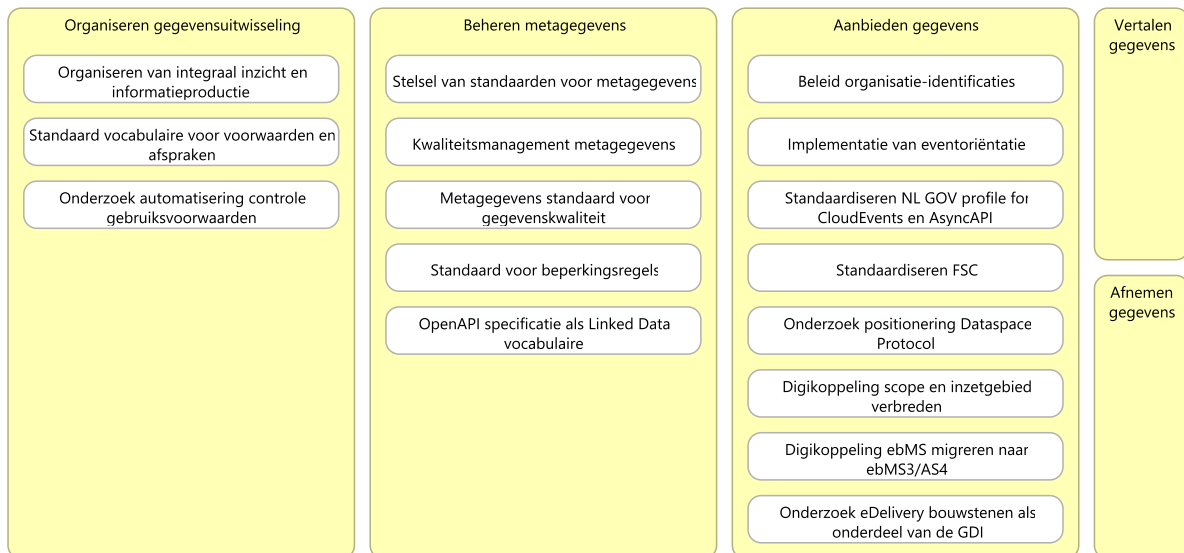
Rationale Het valideren van gegevens borgt dat gegevens valide en consistent zijn en is daarmee een belangrijke maatregel voor het borgen van de kwaliteit van gegevens. Dit is met name relevant als gegevens vervolgens worden doorgeleverd aan anderen zodat een mate van kwaliteit is geborgd in de keten. Bepaalde aspecten van kwaliteit zijn zo belangrijk dat gegevens die daar niet aan voldoen zouden moeten worden afgewezen. Dat gaat in ieder geval over de validiteit (structuur en vorm) en consistentie (samenhangend en vrij van tegenspraak) van gegevens, maar kan bijvoorbeeld ook over actualiteit gaan. Zo is bij het controleren van verifieerbare verklaringen belangrijk om te bepalen of ze nog geldig zijn. Door zo vroeg mogelijk te valideren kan snel een terugkoppeling worden gegeven over fouten en is fouterstel het meest eenvoudig en minder kostbaar dan het herstellen van de fout verderop in de keten.

Implicaties

1. Bronhouders en aanbieders controleren van gegevens die bij hen worden aangeleverd minimaal de validiteit, consistentie en andere aspecten van kwaliteit die tot afwijzing kunnen leiden, voordat ze worden geaccepteerd.
2. Validatiediensten worden ook als losse dienst aangeboden zodat partijen zelf kunnen controleren of gegevens voldoen, zonder ze direct ter verwerking aan te bieden.

4.3 Veranderinitiatieven

De domeinarchitectuur beschrijft veranderinitiatieven die worden voorgesteld omdat ze nodig zijn om ervoor te zorgen dat de digitale overheid kan voldoen aan de beschreven architectuur. Het zijn in eerste instantie alleen voorstellen en ze zijn ook nog niet voorzien van informatie over kosten en baten. Ze zijn vooral input voor nog op te stellen vernieuwingsvoorstellen, in het kader waarvan kosten en baten kunnen worden uitgewerkt. Er is ook bewust voor gekozen om initiatieven die al deel uitmaken van lopende programma's of projecten niet te benoemen, omdat dat weinig meerwaarde heeft. Figuur 8 plot de voorgestelde veranderinitiatieven op het functiemodel.



Figuur 8: Veranderinitiatieven geplot op functiemodel

Organiseren van integraal inzicht en informatieproductie

In een federatief datastelsel blijven gegevens in domeinen, maar is er wel behoefte aan integrale inzichten en informatieproducten. Technisch is dat te realiseren, maar de vraag is vooral hoe dit binnen de overheid structureel te organiseren. Welke (soort) overheidsorganisaties hebben hierin welke verantwoordelijkheden? Er is nader onderzoek nodig, dat zou moeten resulteren in voorstellen voor afspraken en liefst een concrete governancestructuur.

Standaard vocabulaire voor voorwaarden en afspraken

Aanbieders en afnemers zouden gegevens moeten uitwisselen op basis van expliciet vastgelegde voorwaarden en afspraken. Er is nu geen algemene overheidsbrede standaard die beschrijft hoe deze voorwaarden en afspraken kunnen worden vastgelegd. Het standaardiseren hiervan heeft veel meerwaarde. Het zorgt ervoor dat er meer duidelijkheid ontstaat tussen partijen over de voorwaarden en afspraken die gelden. Het maakt het ook mogelijk om dit soort informatie eenvoudiger publiek inzichtelijk te maken en om uitwisseling verder te automatiseren.

Onderzoek automatisering controle gebruiksvoorwaarden

Er bestaan mogelijkheden om gebruiksvoorwaarden om te zetten in autorisatieregels die geautomatiseerd gecontroleerd kunnen worden. Hiermee is verdergaande automatisering van uitwisseling tussen aanbieders en afnemers mogelijk. Er is onderzoek nodig om te bepalen in hoeverre dit een bredere behoefte is bij overheidsorganisaties, hoe ver dit soort controles zouden moeten gaan en hoe dit technisch kan worden ingericht. Zo is het bijvoorbeeld mogelijk om ook aan de kant van de

	<p>afnemer en gebruiker dergelijke controles uit te voeren. Verder zijn er verschillende standaarden die kunnen worden gebruikt zoals de XACML standaard, de ODRL standaard, de Rego taal van de Open Policy Agent (OPA), MYDATA of de Usage Contract Language van de International Data Spaces Association.</p>
Stelsel van standaarden voor metagegevens	<p>Er zou expliciete aandacht en sturing moeten zijn op landelijk niveau op het borgen dat landelijk vastgestelde standaarden voor metagegevens consistent zijn en goed met elkaar te integreren. Het ministerie van BZK heeft aangegeven eigenaar te willen zijn. Er moet een beheerder worden aangewezen en die dit stelsel inricht en beheert.</p>
Kwaliteitsmanagement metagegevens	<p>Goede metagegevens zijn randvoorwaardelijk voor gegevensuitwisseling. Het is daarom essentieel dat kwaliteitsmanagement van metagegevens expliciete aandacht krijgt, zowel landelijk als binnen individuele overheidsorganisaties. Voor landelijke catalogi dient onderzocht te worden hoe hier invulling aan wordt gegeven en of het bijvoorbeeld waardevol is om kwaliteitsdashboards in te richten, vergelijkbaar met hoe dat in het verleden ook voor het Nationaal Geo Register is gedaan. Individuele overheidsorganisaties zouden minimaal een analyse moeten doen van compleetheid van hun metagegevens. Het is belangrijk dat alle gegevens die landelijk gedeeld kunnen worden vindbaar zijn in landelijke catalogi.</p>
Metagegevens standaard voor gegevenskwaliteit	<p>Het is wenselijk om een standaard te bepalen waarmee op een consistentie manier over gegevenskwaliteit in metagegevens kan worden gecommuniceerd. Hierdoor kunnen afnemers eenvoudiger begrijpen in hoeverre gegevens passen bij hun eigen gebruik. Het NORA raamwerk gegevenskwaliteit zou hiertoe moeten worden vertaald naar de DQV standaard.</p>
Standaard voor beperkingsregels	<p>Er is nu geen eenvoudige technologie-onafhankelijke standaard voor het uitdrukken van beperkingsregels, waardoor moet worden gekozen tussen natuurlijke taal, een zelfbedachte taal, een leveranciersspecifieke taal of modelleertaalspecifieke talen zoals OCL of SHACL. Hierdoor is het niet goed mogelijk om deze op een standaard en begrijpelijke manier te beschrijven in een informatie- of gegevensmodel of om kwaliteitsregels mee uit te drukken. Er zou onderzoek moeten plaatsvinden of er in de markt wel talen of standaarden beschikbaar zijn die kunnen worden omarmd, of dat een nieuwe taal moet worden ontwikkeld.</p>
OpenAPI specificatie als Linked Data vocabulaire	<p>Het is wenselijk om een Linked Data vocabulaire te ontwikkelen voor de OpenAPI specificatie. Dit maakt het mogelijk om metagegevens over API's (API specificaties) te integreren met andere vormen van metagegevens, zoals gegevensmodellen. Specifieke aandacht is gewenst voor het op gestandaardiseerde wijze kunnen verbinden van data-elementen in API specificaties (en daarmee in JSON schema's) aan objecttypes en attributen in gegevensmodellen. Dit creëert een verticale data lineage waardoor gebruikers van API's beter inzicht krijgen in de precieze betekenis van gegevens in API's.</p>
Beleid organisatie-identificaties	<p>Er zijn verschillende manieren om organisaties te identificeren, zoals het gebruik van KvK-nummer, OIN, CBS-code, de codes in het Register van Overheidsorganisaties en TOOI. Het is onduidelijk welke identificaties in welke situaties moeten worden gebruikt. Doordat er in de praktijk verschillende keuzes worden gemaakt is het integreren van gegevens over organisaties ook lastig. Er is beleid nodig dat duidelijkheid geeft om tot</p>

	meer consistentie te komen. Daarbij moeten ook de consequenties voor organisaties en systemen worden meegenomen.
Implementatie van eventoriëntatie	Er is aandacht nodig voor eventoriëntatie en het belang ervan en kennis hierover moet worden verspreid. Het is gewenst dat aanbieders notificaties gaan verstrekken over plaatsgevonden gebeurtenissen die relevant zijn voor andere (overheids)organisaties. Daarnaast is het gewenst dat organisaties hun processen en applicaties aanpassen zodat zij effectief gebruik kunnen maken van notificaties. Er is ook een behoefte aan catalogi waarin gebeurtenissen kunnen worden beschreven. Mogelijk kan developer.overheid.nl hiervoor gebruikt worden.
Standaardiseren NL GOV profile for CloudEvents en AsyncAPI	De standaarden "NL GOV profile for CloudEvents" en AsyncAPI zijn een belangrijke basis voor gebeurtenisgedreven gegevensuitwisseling, maar hebben op dit moment geen formele status binnen de overheid. Het sturen op het gebruik hiervan is wenselijk om te komen tot meer standaardisatie. De standaarden zouden aangeboden moeten worden aan Forum Standaardisatie zodat deze overheidsbreed aanbevolen of verplicht worden.
Standaardiseren FSC	De Federated Service Connectivity (FSC) standaard biedt standaard mogelijkheden voor veelvoorkomende uitdagingen bij het veilig en betrouwbaar delen van gegevens tussen organisaties. Het is daarmee een belangrijke basis voor gegevensuitwisseling. Het zou als voorstel moeten worden ingediend bij Forum Standaardisatie zodat deze overheidsbreed aanbevolen of verplicht wordt.
Onderzoek positionering Dataspace Protocol	Het door IDSA beschreven Dataspace Protocol is een belangrijke basis onder de referentie-architectuur van IDS en naar verwachting tot gegevensruimtes in algemene zin. Er is duidelijkheid nodig over hoe het zich verhoudt tot standaarden die worden gebruikt bij de Nederlandse overheidsorganisaties. Zo zijn er overeenkomsten met de FSC en Digikoppeling standaarden alsook met het Nederlands profiel op DCAT. Daarnaast is er overlap met standaarden in het domein toegang.
Digikoppeling scope en inzetgebied verbreden	Er is herbezinning nodig op de scope en het inzetgebied van Digikoppeling. Er zijn andere standaarden voor gegevensuitwisseling zoals GraphQL en SPARQL die veel gebruikt worden. Er moet worden bepaald of Digikoppeling dit soort standaarden expliciet kan ondersteunen. Daarnaast is het verbreden van het inzetgebied van Digikoppeling naar gegevensuitwisseling met bedrijven en mogelijk zelfs naar open data wenselijk, omdat dat bijdraagt aan maximale standaardisatie. Er is daarbij wel expliciet aandacht nodig voor drempels die het verplicht gebruik van certificaten mogelijk opwerpen. Verder is de vraag of de naam van de standaard de lading nog voldoende dekt.
Digikoppeling ebMS migreren naar ebMS3/AS4	De ebMS3/AS4 standaard is de opvolger van de ebMS2 standaard. De ebMS2 standaard is technisch verouderd, en in de markt is er meer kennis en ondersteuning beschikbaar voor ebMS3/AS4. Migratie naar de ebMS3/AS4 standaard is daarom aanbevolen. Daarnaast is het ook onderdeel van de Europese e-Delivery standaard. Er moet een implementatie- en migratieplan worden opgesteld.
Onderzoek eDelivery bouwstenen als onderdeel van de GDI	Als onderdeel van de Europese e-Delivery standaard zijn een aantal (software)bouwstenen beschikbaar. Het zou waardevol kunnen zijn om deze formeel onderdeel te laten zijn van de GDI en breed beschikbaar te

stellen aan overheidsorganisaties. Daarbij hoort ook beleid over hoe deze bouwstenen generieker ingezet kunnen worden. Het vraagt nader onderzoek om te bepalen of dit meerwaarde heeft.

5 Verdieping

Dit hoofdstuk beschrijft een verdieping op de architectuurvisie en de architectuurprincipes op de onderwerpen gegevensruimtes, metagegevens, communicatieprotocollen, historie en eventoriëntatie. Het is vooral bedoeld als een uitleg op deze onderwerpen.

5.1 Verdieping: gegevensruimtes

Gegevensuitwisseling staat ook in Europa hoog op de agenda. Deze domeinarchitectuur noemt de Europese ontwikkelingen, waaronder wetgeving en de komst van gegevensruimtes (data spaces). Dit verdiepende hoofdstuk biedt meer diepgang en is tevens een zelfstandig leesbare introductie op het onderwerp. Het is voor een belangrijk deel gebaseerd op input, documentatie en afstemming met Geonovum, inclusief de eerder opgestelde [verkenning dataspaces](#).

5.1.1 Inleiding

De EU wil de maatschappelijke baten van het gebruik van gegevens vergroten. Dat vergt dat er meer gegevens beschikbaar komen en dat er uniforme regels komen over hoe je verantwoord met gegevens om kunt gaan. De Europese datastrategie neemt het maximaliseren van de waarde van het gegevensgebruik als startpunt. Net als het vrije verkeer van personen en goederen creëert de Europese Commissie daarvoor ook een eenheidsmarkt voor gegevens waarin:

- binnen de EU en tussen sectoren ongehinderd gegevensverkeer mogelijk is;
- de Europese regels en waarden, met name die ter bescherming van persoonsgegevens, consumenten en mededinging, volledig in acht genomen worden;
- de regels voor de toegang tot en het gebruik van gegevens eerlijk, praktisch en duidelijk zijn.

om zo het mondiale concurrentievermogen en de soevereiniteit van Europa op het gebied van gegevens te waarborgen.

De Europese Commissie werkt aan de datastrategie middels verschillende wetgevingstrajecten en investeringen. Dit zal onder andere leiden tot de totstandbrenging van gemeenschappelijke sectorale gegevensruimtes die samen een EU-brede gegevensruimte (eenheidsmarkt) zullen gaan vormen. Deze EU-brede gegevensruimte is een omgeving voor het uitwisselen, aanbieden en gebruiken van gegevens, binnen de randvoorwaarden en afspraken die voor die marktomgeving gelden. De sectorale gegevensruimtes zullen hiertoe onderling operabel zijn. Hiermee wordt het bestaande vrije verkeer van personen, goederen en kapitaal aangevuld met het vrije verkeer van gegevens. Het maakt het mogelijk maken om gegevens uit de hele EU, zowel uit de publieke sector als uit het bedrijfsleven, op betrouwbare wijze en tegen lagere kosten uit te wisselen, waardoor de ontwikkeling van nieuwe data-gedreven producten en diensten wordt gestimuleerd.

De Europese Commissie definieert 14 sectorale gegevensruimtes (Common European Data Spaces) zoals benoemd in Tabel 2. Per gegevensruimte bestaan meerdere programma's (met financiering van de Europese Commissie) waarin bijvoorbeeld onderzoek wordt verricht of waarin bouwstenen worden opgeleverd ten behoeve van de EU-brede gegevensruimte (Common European Dataspace). Een voorbeeld is het GREAT project dat bijdragen heeft geleverd voor de Green Deal dataspace. Verder is het name de Health gegevensruimte al ver uitgewerkt in specifieke wet- en regelgeving. In de meeste gevallen zijn de gegevensruimtes gestart met inventariserende acties, zoals het inventariseren van bestaande platformen. Het speelveld is nog flink in ontwikkeling.

Agriculture	Green deal	Media	Skills
Cultural Heritage	Health	Mobility	Tourism
Energy	Language	Public administration	
Finance	Manufacturing	Research and Innovation	

Tabel 2: Common European Data Spaces

Naast gemeenschappelijke gegevensruimtes wordt ook gesproken over persoonlijke gegevensruimtes. Deze maken het mogelijk om als individu of organisatie gegevens voor een specifiek gebruiksgeval (tijdelijk) in te brengen. Een voorbeeld zou kunnen zijn, dat je je eigen mobiliteitsgegevens meeneemt naar een discussie over een nieuwe busroute of rondweg in je wijk. Hiermee kan het in de Data Governance Act (DGA) genoemde "data-altruïsme" worden vormgegeven. Data-altruïsme is het beschikbaar stellen van gegevens voor algemeen nut aan een behorende erkende organisatie die toeziet op het juiste gebruik van die gegevens.

Gegevensruimtes zijn in meer algemene zin gericht op het verhogen van interoperabiliteit. Dat is het vermogen van organisaties (en hun processen en systemen) om effectief en efficiënt informatie te delen met hun omgeving. Dit vraagt het maken van afspraken op allerlei niveaus: grondslagen, organisatie, informatie, applicatie en netwerk. Het betekent dat gegevensruimtes op elkaar aan moeten sluiten en daartoe zoveel mogelijk gestoeld moet zijn op overeenkomende afspraken en standaarden. Het borgen van deze interoperabiliteit ziet de Europese Commissie als belangrijke uitdaging om daadwerkelijk tot een eenheidsmarkt te komen. Andere specifieke aandachtspunten van de Commissie zijn garanderen van de betrokkenheid van deelnemers, het bevorderen van het gebruik van gegevensruimtes en het aanmoedigen van startup's en het midden- en kleinbedrijf om deel te nemen aangezien zij gezien worden als sleutelspelers in de data-economie.

5.1.2 Definitie

Wat een gegevensruimte precies is, is nog niet geheel duidelijk. Het wordt geconcretiseerd in een geleidelijk ontstaansproces, waarbij bestaande en nieuwe elementen worden gefedereerd en verbonden. Een gegevensruimte zal in ieder geval bestaan uit een technische infrastructuur, gereedschappen, afspraken, standaarden en gebruiksvoorwaarden voor het delen en gebruiken van gegevens. Daarnaast geldt dat inmiddels veel organisaties bezig zijn met gegevensruimtes. De Europese Commissie stelt dat stakeholders de drijvende kracht zijn achter de ontwikkeling van gegevensruimtes. Elke gegevensruimte kan daardoor unieke eigenschappen hebben.

Het Data Spaces Support Centre (DSSC) hanteert de volgende definitie: "A data space is a distributed system defined by a governance framework. It facilitates secure and trustworthy data transactions between participants, emphasising trust and data sovereignty. A data space supports one or more use cases." Het DSSC is in 2022 opgericht, gefinancierd door de Europese Commissie.

Centraal in de diverse definities staat steeds het ecosysteem van aanbieders en afnemers die met elkaar afspraken maken om gegevens op een vertrouwde en soevereine manier te delen ten behoeve van concrete use cases. Hiertoe wordt in een gegevensruimte een governance ingericht, gefaciliteerd door een zogenaamde "Data Space Authority".

Naast gegevensruimtes zijn er ook vormen van gegevensuitwisseling die niet onder de noemer van gegevensruimtes vallen, zoals open data portalen of bilaterale gegevensuitwisseling. Open dataportalen zijn niet gericht op concrete use cases en bij bilaterale gegevensuitwisseling is geen ecosysteem van partijen betrokken. Deze andere vormen van gegevensuitwisseling kunnen wel geraakt worden door ontwikkelingen op het gebied van gegevensruimtes. Zo kunnen bijvoorbeeld standaarden voor gegevensruimtes ook breder ingezet worden. Daarnaast zijn partijen typisch betrokken in verschillende vormen van gegevensuitwisseling.

5.1.3 Organisaties en initiatieven

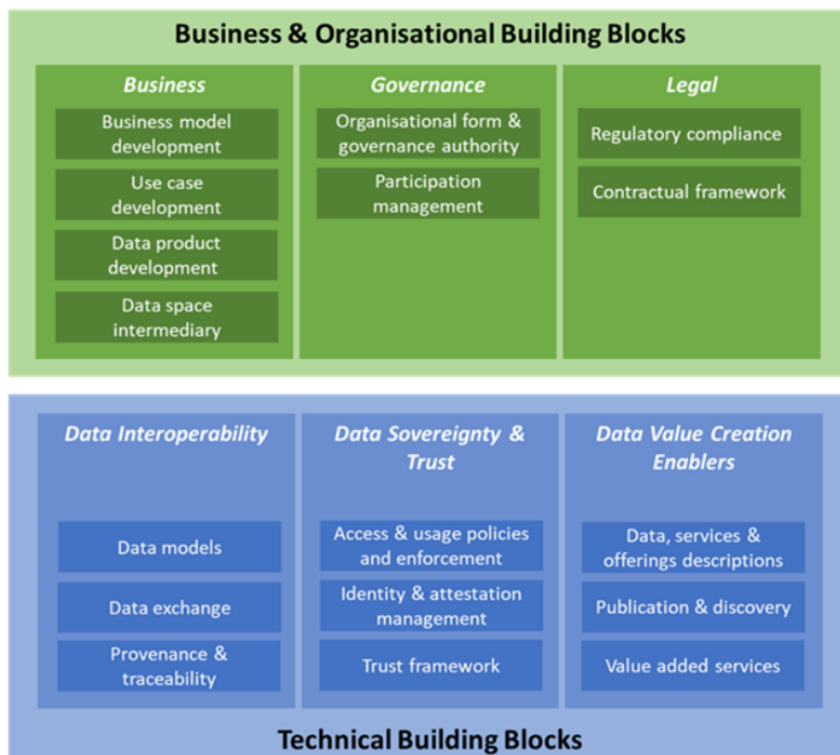
Er zijn allerlei organisaties en initiatieven die gestart of ge(her)positioneerd zijn rondom gegevensruimtes. In deze paragraaf benoemen we een aantal van deze organisaties en initiatieven, inclusief een aantal referentie-architecturen en infrastructuren.

Alhoewel de Europese datastrategie een belangrijke drijfveer is voor gegevensruimtes, zijn niet alle initiatieven direct gerelateerd aan de Europese Commissie of diens initiatieven. De International Data Spaces Association (IDSA) IDSA heeft het initiatief genomen om een [radar](#) te ontwikkelen waarop initiatieven geïnterpreteerd worden. Er wordt onderscheid gemaakt tussen "Communities of Practice", "Use Cases" en "Data Spaces" en per initiatief wordt het ontwikkelingsstadium aangegeven. In de versie van maart 2024 zijn bijna 150 initiatieven uit 18 sectoren opgenomen. Naast de 14 eerder genoemde Common European Data Spaces staan ook Logistics, Automotive, Smart City en 'Other' als sectoren opgenomen. Van de 54 Data Space initiatieven zitten er twee in het eerste ontwikkelingsstadium (scaling phase): het Once Only Technical System uit de Common European Dataspace Public Administrations (ter implementatie van de Single Digital Gateway Regulation) en de dataspace GDSO uit de Automotive industrie (dit gaat over de waardeketen van data over banden).

Data Spaces Support Center

Het Data Spaces Support Centre (DSSC), gefinancierd door de Europese Commissie onder het Digital Europe Programme, coördineert die streven naar gemeenschappelijke Europese gegevensruimtes. Het streeft ernaar om samenwerking, innovatie en groei binnen het dataruimte-ecosysteem te bevorderen door ondersteunende diensten aan te bieden, waaronder technische expertise, projectmanagementassistentie en toegang tot relevante netwerken en bronnen. Het DSSC onderzoekt de behoeften van initiatieven, definieert gemeenschappelijke eisen en stelt best-practices vast om de vorming van soevereine gegevensruimtes te versnellen als een cruciaal element van digitale transformatie op alle gebieden.

Om te helpen eenheid te creëren heeft het Data Space Support Centre een [Blueprint](#) opgesteld. De blueprint bevat richtlijnen ter ondersteuning van de ontwikkelingscyclus van gegevensruimtes. Het omvat het conceptuele model van een gegevensruimte, bouwstenen voor gegevensruimtes en aanbevolen standaarden en specificaties. De blueprint onderscheidt 12 bouwblokken waarmee een gegevensruimte wordt opgebouwd (zie Figuur 9). Deze zijn onderverdeeld in "bedrijfs- en organisatorische" en "technische" bouwblokken. Per bouwblok wordt beschreven wat nodig is om te regelen in een gegevensruimte en worden aanbevolen standaarden en specificaties genoemd.



Figuur 9: Bouwblokken voor gegevensruimtes in de DSSC Blueprint

De technische bouwblokken uit de figuur beschrijven de capability's die nodig zijn in een gegevensruimte. Technisch gezien zullen deze bouwblokken niet één-op-één relateren aan technische componenten. In veel gevallen zal een technische component meerdere bouwblokken raken. Veel gegevensruimtes implementeren bijvoorbeeld een "Data Space Connector" waarin zowel "Data Exchange", "Identity Management" als "Access & Usage Policies" worden geïmplementeerd.

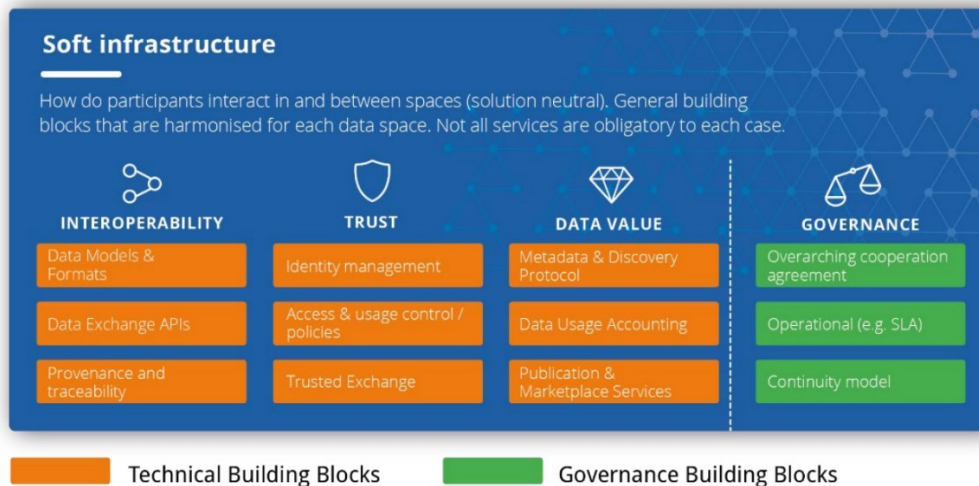
De Blueprint maakt een onderscheid tussen de "control plane" en de "data plane". De control plane reguleert het management van gegevens en hoe gegevens worden gerouteerd en verwerkt. Het gaat dan bijvoorbeeld om de identificatie van gebruikers en de afhandeling van het toegangs- en gebruiksbeleid. De data plane zorgt voor de daadwerkelijke gegevensuitwisseling. De control plane kan van nature vergaand worden gestandaardiseerd, met behulp van gemeenschappelijke standaarden voor identificatie, authenticatie, etc. De data plane kan meer specifiek zijn voor een gegevensruimte. Sommige dataspace richten zich op het delen van grote datasets, andere op het uitwisselen van berichten en anderen kiezen voor een op gebeurtenissen gebaseerde aanpak. Er is geen one-size-fits-all, hoewel er wel enkele mechanismen zijn (vooral op het gebied van data-interoperabiliteit) die kunnen helpen ervoor te zorgen dat verschillende dataplans samenwerken.

OpenDEI

OpenDEI was een door de EU gefinancierd project dat heeft gelopen tot 2022. Het had als doel om lacunes op te sporen, synergiën aan te moedigen, regionale en nationale samenwerking te ondersteunen, en de communicatie tussen de EU-projecten ter uitvoering van de digitale strategie van de EU te verbeteren. OpenDEI heeft een zeer lezenwaardig [position paper "Design principles for data spaces"](#) opgeleverd in mei 2021. Aan het OpenDEI position paper hebben diverse andere gegevensruimte initiatieven en organisaties een bijdrage geleverd. Het bijbehorende model is ook de basis voor de architectuur van het federatief datastelsel.

Het position paper beschrijft de principes voor het maken van data spaces, en is eveneens een conceptueel model van de nodige afspraken en generieke (federatieve) technische bouwstenen

voor het maken van een gegevensruimte (zie Figuur 10). Het is te zien als een referentie-architectuur op hoofdlijnen. De blueprint zoals ontwikkeld door het DSSC is een doorontwikkeling van deze referentie-architectuur. Het paper verwijst naar toe te passen standaarden bij de invulling van bepaalde aspecten. Het geeft ook aandacht aan governance en het belang van een business model. Het onderstreept daarmee het belang van data spaces en het soeverein delen van data in de toekomstige EU data-economie.



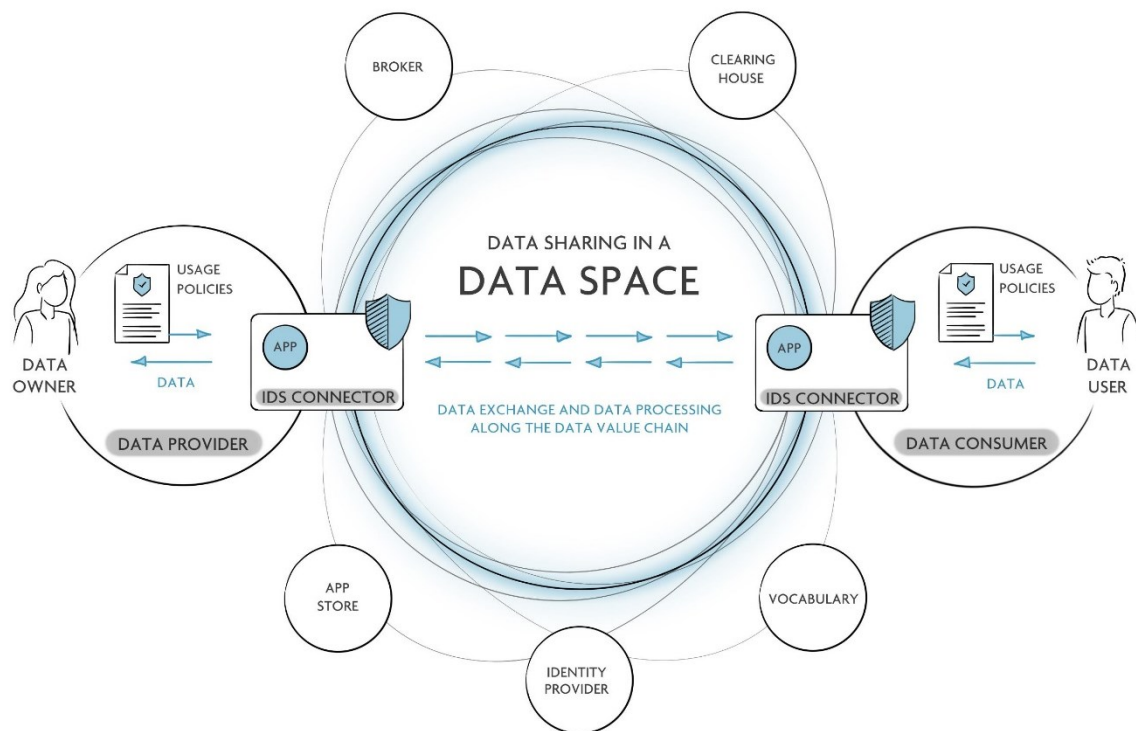
Figuur 10: OpenDEI bouwstenen

De OpenDEI referentie-architectuur beschrijft vier principes:

- **Datasoevereiniteit.** Het vermogen van een natuurlijke persoon of organisatie tot exclusieve zelfbeschikking met betrekking tot haar economische data goederen. Dit is het innovatieve en transformatieve concept dat ten grondslag ligt aan gegevensruimtes.
- **Gelijk speelveld op data.** Nieuwkomers ondervinden geen onoverkomelijke toetredingsdrempels vanwege monopolistische situaties. Wanneer er sprake is van een gelijk speelveld, concurreren spelers op kwaliteit van de dienstverlening en niet op de hoeveelheid data die ze beheren. Een gelijk speelveld voor data is een cruciale voorwaarde om een eerlijke economie voor het delen van data te creëren.
- **Gedecentraliseerde 'zachte infrastructuur'.** De infrastructuur voor het delen van gegevens is geen monolithische gecentraliseerde IT-infrastructuur. Het is een verzameling van interoperabele implementaties van gegevensruimtes die voldoen aan een set afspraken.
- **Publiek-private governance.** Voor het ontwerp, de creatie en het onderhoud van het gelijke speelveld voor data is een goede governance essentieel. Alle belanghebbenden moeten zich vertegenwoordigd en betrokken voelen: gebruikers, leveranciers van gegevensdiensten, evenals hun technologiepartners en professionals.

International Data Spaces Association

De International Data Spaces Association (IDSA) is een non-profit organisatie gericht op het creëren van standaarden voor gegevensruimtes. Het is een organisatie waar veel andere internationale organisaties in participeren als deelnemer. Het is in 2015 ontstaan uit het International Data Spaces (IDS) project, geïnitieerd vanuit de Fraunhofer Society en gefinancierd door het Duitse federale ministerie van Onderwijs en Onderzoek. IDSA was ook verantwoordelijk voor de coördinatie van het OpenDEI project. IDSA biedt een aantal producten zoals een referentie-architectuur en een regelboek, waarbij datasoevereiniteit centraal staat. De [International Data Spaces Reference Architecture Model](#) (IDS DAM) beschrijft op business, functioneel, informatie, proces en systeemniveau hoe gegevensruimtes worden vormgegeven. Figuur 11 geeft een overzicht van het IDS RAM op hoofdlijnen.



Figuur 11: IDS Reference Architecture Model op hoofdlijnen

Data providers (aanbieders) en data consumers (afnemers) zijn in de IDS RAM van elkaar ontkoppeld door connectoren. Hierdoor ontstaat een four-corner model, waarbij er geen centraal middelpunt bestaat in de communicatie. Een IDS connector is een softwarecomponent voor veilige en vertrouwde data-uitwisseling. Er is inmiddels een [grote verzameling standaard connectoren beschikbaar](#), voor verschillende platformen en technologieën. Een connector verzendt de gegevens rechtstreeks naar de ontvanger, waarbij de aanbieder de controle over de gegevens behoudt en de voorwaarden voor het gebruik ervan bepaalt. Partijen kunnen in een connector hun gebruiksvoorwaarden (usage policies) aan hun gegevens koppelen en afdwingen. De IDS connector fungeert verder als gateway voor gegevens en diensten en als vertrouwde omgeving voor apps en software. Apps worden ingelezen vanuit de App Store in de vertrouwde omgeving van de IDS connector. Apps voeren taken uit zoals transacties, aggregaties of analyse van gegevens. IDS-connectors kunnen de beschrijving van hun gegevens publiceren bij een IDS makelaar of "broker", waardoor ze vindbaar zijn voor afnemers. Aanbieders van vocabulaires leveren een taal (begrippenkader of informatiemodel) om gegevens mee te beschrijven, gebaseerd op het gemeenschappelijke IDS-informatiemodel. Een clearing house kan onweerlegbaarheid en traceerbaarheid van gegevensuitwisselingen bieden. App stores bieden data-apps aan. Dit zijn toepassingen die kunnen worden geïmplementeerd in IDS Connectors om taken zoals transformatie, aggregatie of analyse van de data uit te voeren. Identiteitsproviders bieden diensten voor het maken, onderhouden, beheren en valideren van identiteitsinformatie van en voor alle IDS deelnemers en componenten.

Om de interacties tussen de verschillende componenten in de control plane te standaardiseren wordt door IDSA het Dataspace Protocol ontwikkeld. Hierin worden de schema's en protocollen voor het publiceren van data, het onderhandelen over contracten en toegang tot gegevens in een gefedereerd systeem beschreven. Het protocol beschrijft dus niet de daadwerkelijke uitwisseling van gegevens (data plane). Het beschrijft ook niet de uitwisseling van gegevens tussen verschillende gegevensruimtes en biedt ook geen specifieke ondersteuning op het gebied van semantische interoperabiliteit. Het protocol is gebaseerd op bestaande standaarden en zal zelf ook richting een ISO standaard doorontwikkeld worden. Het protocol beschrijft voor een belangrijk deel

hoe voor uitwisseling relevante metagegevens er uitzien. Het gaat ervan uit dat datasets worden gepubliceerd in DCAT-gebaseerde catalogi en dat regels voor toegang worden uitgedrukt in ODRL-gebaseerde policies. Het beschrijft hoe voorwaarden en afspraken over datagebruik moeten worden beschreven en hoe hierover elektronisch moeten worden onderhandeld. Het beschrijft ook hoe toegang kan worden verkregen tot datasets. De interactie tussen partijen wordt uitgevoerd door connectoren, die het Dataspace Protocol implementeren. Het protocol biedt een overkoepelend raamwerk.

GAIA-X

[Gaia-X](#) is een Europees initiatief, dat een softwareraamwerk van controle en governance ontwikkelt en een gemeenschappelijke reeks beleidsregels en regels implementeert. Deze kunnen worden toegepast op elke bestaande cloud / edge-technologiestack om transparantie, controleerbaarheid, portabiliteit en interoperabiliteit tussen gegevens en diensten te verkrijgen. Het raamwerk is bedoeld om te worden geïmplementeerd bovenop bestaande cloudplatforms die zich houden aan de Gaia-X-standaard. Gaia-X is geen marktexploitant en zal ook geen van de door het kader vereiste diensten rechtstreeks of uitsluitend exploiteren. Gaia-X-diensten zullen worden gecreëerd, geëxploiteerd en geadopteerd door de markt.

Gaia-X heeft tot doel om datasoevereiniteit, databeschikbaarheid en innovatie te ondersteunen. Europese bedrijven en organisaties moeten altijd de keuze hebben waar en bij wie ze data opslaan en verwerken en waar ze digitale diensten afnemen. Gaia-X wil monopolies en daarmee een eenzijdige afhankelijkheid van Europa van grote niet-Europese platformaanbieders voorkomen. Europese bedrijven, overheden, instellingen en burgers hebben ook garanties nodig om gegevens op een betrouwbare, veilige en transparante manier uit te wisselen. Gaia-X is bedoeld om innovatie in Europa te bevorderen en de digitale economie te versterken. De cloud en edge services die onder Gaia-X zijn verzameld, ondersteunen de digitale bedrijfsmodellen van het Europese bedrijfsleven en geeft deze de mogelijkheid om op basis van deze infrastructuur wereldwijd te groeien.

De Gaia-X Federatieve Diensten zijn diensten, die nodig zijn voor de operationele implementatie van een Gaia-X Data Ecosysteem mogelijk te maken. Gaia-X onderscheidt vier groepen diensten: Identity and Trust, Federated Catalogue, Sovereign Data Exchange en Compliance. Binnen het Gaia-X federation diensten ontwikkelt de Gaia-X gemeenschap ook open-source softwarecomponenten. Op basis van technische specificaties worden de federatieve diensten op basis van open-source code ontwikkeld. Dit staat ook bekend als de GXFS Toolbox. Gaia-X biedt geen meta-model voor het definiëren van gegevens of API's. Gaia-X heeft een governance model, waarin de Gaia-X Association een belangrijke rol speelt. Daarnaast is Community building is een belangrijke organisatorische pilaar van Gaia-X. Gaia-X is minder ver ontwikkeld dan de IDS RAM, maar volgt dezelfde visie om datasoevereiniteit te verspreiden en een ecosysteem van vertrouwen te creëren voor het delen van gegevens.

Data sharing coalition

De [Data Sharing Coalition](#) wil voortbouwen op bestaande initiatieven voor het delen van gegevens om ze te versterken bij het ontsluiten van de waarde van het delen van data in en over hun domein. De coalitie heeft tot doel het cross-domein delen van gegevens onder controle van de rechthebbende partij te stimuleren, door interoperabiliteit tussen domeinen mogelijk te maken. De Data Sharing Coalition is een internationaal initiatief waarin een grote verscheidenheid aan organisaties samenwerkt om het delen van gegevens tussen bestaande gegevensruimtes mogelijk te maken. Hierdoor kunnen partijen uit verschillende sectoren en domeinen eenvoudig data met elkaar delen, waardoor aanzienlijke economische en maatschappelijke waarde wordt ontsloten. De Data Sharing Coalition realiseert daarvoor verschillende cross-domein use cases. In deze use cases definiëren en realiseren organisaties uit verschillende domeinen samen een use case die nieuwe waarde realiseert dankzij (cross-sectoraal) data delen.

De coalitie is in januari 2020 gestart met steun van het Ministerie van Economische Zaken en Klimaat in Nederland. De verwachte levensduur van de projectfase van de coalitie is tot 2025. Tegen 2025 zal de Data Sharing Coalition naar verwachting haar resultaten en activiteiten hebben overgedragen aan een entiteit, die een Trust Framework exploiteert en beheert dat cross-domein data delen faciliteert. De eerste fase van de Data Sharing Coalition was een onderzoek naar het harmonisatiepotentieel om domeinoverstijgend delen van gegevens mogelijk te maken. Dat is uiteengezet in de Data Sharing Canvas, waarin de onderdelen van het cross-domein data delen zijn benoemd. Het heeft niet tot doel uitputtend te zijn of in detail invulling te geven aan deze onderwerpen. Het vormt ook de globale leidraad voor toekomstige werkzaamheden van de Data Sharing Coalition. Het beschrijft een Proxy model, waarbij proxies vergelijkbaar zijn met connectoren. In de toekomst zal het Data Sharing Canvas verder worden onderbouwd met inzichten, die zijn afgeleid van praktische use cases voor het delen van gegevens die de Data Sharing Coalition heeft gerealiseerd.

iShare

iShare is een Nederlands initiatief dat werkt aan een vertrouwenskader voor gegevensruimtes. Het vertrouwenskader is een uniforme set van afspraken voor Identificatie, Authenticatie en Autorisatie (IAA), inclusief tooling die benodigd is om het afsprakenstelsel te implementeren. Door gebruik te maken van het vertrouwenskader van iSHARE hebben aanbieders de zekerheid, dat organisaties die toegang hebben tot gegevensdiensten wettelijk onder de geheimhoudingsovereenkomst vallen en in de licentie blijven die met de gegevens is afgegeven. Daarnaast heeft de aanbieder de zekerheid dat gegevens alleen wordt gedeeld met geautoriseerde afnemers. iSHARE is een volledig gefedereerde structuur en juridisch kader, die vertrouwen, databescherming en datasoevereiniteit binnen gegevensruimtes mogelijk maakt.

iSHARE is ontstaan in de logistieke sector vanuit de vraag waarom organisaties weinig tot geen data met elkaar delen. Vanuit de eerste fase in 2016 is iSHARE opgebouwd met hulp van vele co-creatie-partners. De co-creatie-partners hebben verschillende achtergronden: uit de private en publieke sector, organisaties van verschillende grootte, verschillende modaliteiten, zowel aanbieders als ontvangers van data, enz. Deze verscheidenheid aan organisaties zorgt ervoor dat het iSHARE vertrouwenskader breed toepasbaar is geworden. De besturing van iSHARE is geregeld in een Nederlandse stichting, opgericht in 2018.

Het iSHARE kader beschrijft een actormodel met zes rollen die, afhankelijk van de situatie, met elkaar interacteren op basis van de iSHARE 'schemaovereenkomsten'. De zes rollen zijn: Service Consumer, Service Provider, Entitled Party, Identity Provider, Identity Broker en Authorization Registry. De iSHARE Satelliet vormt de kern van het iSHARE-vertrouwensnetwerk, als coördinator en governancekern in een data space. De iSHARE Satelliet heeft de rol van 'schemabeheerder' en zorgt voor toelating, terugtrekking, waarschuwingen, opschorting, uitsluiting, wijzigingen en updates.

Geo Informatie Infrastructuur

Geo Informatie Infrastructuur is een internationaal concept, dat in de loop van de jaren invulling heeft gekregen in Nederland via wetgeving, afspraken en governance, standaardisatie en implementatie van voorzieningen in vooral publieke organisaties. De Geo Informatie Infrastructuur geeft reeds invulling aan een groot deel van de noodzakelijke bouwstenen van gegevensruimtes en kun je daarmee beschouwen als een infrastructuur voor het creëren van geografische gegevensruimtes.

Het ministerie van Binnenlandse zaken, verantwoordelijk voor de Nationale Geo-Informatie Infrastructuur (NGII), ziet het als een datafundament onder de maatschappelijke opgaven, en sectoren die er gebruik van maken. Het bestaat uit gegevensverzamelingen, voorzieningen,

werkprocessen, afspraken, standaarden, governance, financiering en wet- en regelgeving. De NGII omvat de geo-basisregistraties alsook voorzieningen zoals PDOK en het Nationaal Geo Register.

Voor de NGII is de Europese INSPIRE wet richtinggevend geweest, met voorschriften voor het gestandaardiseerd ontsluiten van allerlei geo-informatie voor milieutoepassingen. (data, netwerkdiensten en metadata). Dat heeft er mede toe geleid, dat in 2007 het Nationaal Geo Register is opgezet, waarin inmiddels meer dan 8000 datasets zijn geregistreerd om de toegang tot publieke geo-informatie te verbeteren. De NGII is daarmee onderdeel van de Europese geo-informatie infrastructuur en biedt voor INSPIRE het Nederlandse ingangspunt voor het EU geoportaal. Dat is voor INSPIRE de centrale catalogus waar alle lidstaten hun dataproducten (datasets en gegevensdiensten) kenbaar maken.

5.2 Verdieping: metagegevens

In dit deel van de architectuur wordt een verdieping gegeven aan het thema metagegevens. Het start met een korte inleiding van het onderwerp en een overzicht van de belangrijkste objecten en de standaarden die daarbij van toepassing zijn. Vervolgens gaat het dieper in op specifieke vormen van metagegevens die extra aandacht vragen in de context van gegevensuitwisseling: modellen, metagegevens over gegevenskwaliteit, voorwaarden, overeenkomsten en de herkomst van gegevens.

5.2.1 Inleiding

Metagegevens zijn gegevens over gegevens en helpen je om bepaalde aspecten van de gegevens beter te begrijpen. Praktisch gezien kun je metagegevens zien als bijsluiter bij gegevens. Het onderscheid tussen gegevens en metagegevens is niet altijd zwart-wit; het is afhankelijk van de context en de rol die de gegevens spelen. Zo kunnen bijvoorbeeld gegevens over een persoon gebruikt worden om aan te geven wie de auteur is van een informatie-object en daarmee worden ze metagegevens. Er zijn allerlei vormen van metagegevens. De DAMA Data Management Body of Knowledge (DMBoK) maakt onderscheid tussen business metagegevens, technische metagegevens en operationele metagegevens. Business metagegevens zijn bijvoorbeeld begrippen, bedrijfsregels, informatie- en gegevensmodellen, kwaliteitsregels, datasetdefinities en gegevens over de herkomst van gegevens. Technische metagegevens zijn bijvoorbeeld technische gegevensmodellen, gegevens over databases, bestandsformaten en ETL scripts. Operationele metagegevens zijn bijvoorbeeld audit- en errorlogs, omvang- en gebruiksgegevens en uitwisselafspraken. Dit onderscheid wordt vooral gebruikt in de context van gestructureerde gegevens. In de context van archivering wordt ook wel het onderscheid gemaakt tussen beschrijvende metagegevens, structurele metagegevens en administratieve metagegevens. Er is eerder door een NORA werkgroep een [visie op metagegevens](#) opgesteld waarin meer algemene informatie over het onderwerp te lezen is. Onderdeel daarvan is ook een volwassenheidsmodel voor het omgaan met metagegevens.

In de context van gegevensuitwisseling is vooral interessant welke metagegevens worden uitgewisseld met andere organisaties. Daarbij spelen standaarden een cruciale rol. Ze zorgen ervoor dat afnemers eenvoudiger kunnen begrijpen welke gegevens het betreft. Er is een grote diversiteit aan standaarden die iets zeggen over metagegevens. Figuur 12 geeft een overzicht van gangbare standaarden, geplot op het [bedrijfsobjectenmodel](#). Het geeft aan welke standaarden, voor het beschrijven van welke soort metagegevens relevant zijn. Per standaard is met een kleur aangegeven of deze door Forum Standaardisatie verplicht of aanbevolen is, of dat deze in deze architectuur wordt aanbevolen. De figuur maakt direct het belang van metagegevens in de context van gegevensuitwisseling duidelijk. Er is een grote diversiteit aan soorten metagegevens en standaarden belangrijk om ervoor te zorgen dat gegevensuitwisseling op een goede manier kan verlopen. Om dit goed te laten werken zijn ook de relaties tussen deze standaarden belangrijk. Op het eerste gezicht lijkt het alsof er wel erg veel standaarden zijn, maar veel van deze standaarden zijn complementair of hebben een duidelijk eigen bestaansrecht en toepassingsgebied. Op hoofdlijnen is het bedrijfsobjectenmodel een metadatamodel en het kan door organisaties ook als startpunt voor een eigen metadatamodel dienen. Een dergelijk model is belangrijk bij het inrichten van het beheer van metagegevens.

5.2.2 Begrippen, informatie- en gegevensmodellen

Als het gaat over de uitwisseling van gestructureerde gegevens, dan is het belangrijk om met modellen duidelijk te maken wat de betekenis en structuur van deze gegevens is. Er zijn allerlei modellen die daarbij relevant zijn (zie Tabel 3). Er is een onderscheid tussen modellen die het (probleem)domein beschrijven en modellen die het oplossingsdomein beschrijven. De modellen voor het probleemdomein zijn primair analysemodellen. Ze zijn een representatie van het domein zelf, zonder dat de modelleur hier een ontwerpkeuze bij maakt. Ze hebben tot doel om het domein goed te begrijpen zodat misinterpretaties worden voorkomen. Door het opstellen van dit soort modellen wordt kennis over het domein vastgelegd, wat een belangrijke basis is voor automatisering. Modellen voor de oplossingsruimte zijn primair bedoeld als ontwerp. Ze zijn bijvoorbeeld nodig om te specificeren welke gegevens gegevensdiensten moeten leveren.

Een begrippenkader beschrijft de betekenis van termen en is de basis om ervoor te zorgen dat mensen elkaar begrijpen. Een conceptueel model is een formele beschrijving van een (probleem)domein, los van hoe dat in gegevens wordt vastgelegd. Logische modellen leggen de nadruk op het gebruik van gegevens in informatiesystemen door het structureren van gegevens. Fysieke (technische) modellen leggen de nadruk op de vertaling naar implementatie. De Nederlandse Standaard voor het Beschrijven van Begrippen (NL-SBB) biedt een standaard taal, structuur en set aan metagegevens voor begrippenkaders, gebaseerd op de SKOS standaard. Het Metamodel Informatie Modelleren (MIM) biedt een standaard taal, structuur en set aan metagegevens voor informatie- en logische gegevensmodellen. Hierdoor zijn ze meer gestandaardiseerd en kunnen ze eenvoudiger worden begrepen en uitgewisseld. Het beschrijft ook hoe ze in UML, XML en als Linked Data gerepresenteerd kunnen worden. Het is ook mogelijk om informatie- en logische gegevensmodellen direct conform Linked Data standaarden zoals RDFS, OWL en SHACL vast te leggen.

Door de community die hoort bij de MIM standaard is gewerkt aan een [manifest](#) dat het belang van kennisrepresentatie onder de aandacht brengt. Onderdeel daarvan is ook een uitwerking van de soorten modellen die daarbij relevant zijn en die in dit document is weergegeven in Tabel 3. De overtuiging die ten grondslag ligt aan het manifest is dat de kunde van kennisrepresentatie een noodzakelijke voorwaarde is om te komen tot goede informatiediensten. Het beschrijft onder meer het belang van een expliciet begrip van het domein en de daarin gebruikte taal en geeft aan dat een gezamenlijk begrip alleen tot stand kan komen via een gestructureerde dialoog. Het manifest is bedoeld om richting te geven aan de doorontwikkeling van de MIM standaard, omdat de huidige versie van de standaard het onderscheid tussen het conceptuele en logische niveau niet duidelijk uitwerkt. Merk op dat de werkgroep en het resultaat geen formele status hebben en de informatie slechts ter inspiratie in dit document is opgenomen.

Het opstellen van dit soort modellen is essentieel om op een professionele manier met gegevens om te gaan en is daarmee ook een basis voor gegevensuitwisseling. Het zorgt ervoor dat expliciet wordt geredeneerd vanuit begrippen. Deze begrippen worden deels beschreven in wet- en regelgeving, en vormen de basis voor de inrichting van informatievoorziening. Middels [wetsanalyse](#) kunnen de juridische kwalificaties van formuleringen in wet- en regelgeving geannoteerd worden. Dezelfde aanpak kan ook worden gebruikt voor het analyseren van beleidsteksten, procesdocumenten en instructies. Dit is de basis voor het definiëren van begrippen en bedrijfsregels, die niet in de teksten zelf expliciet zijn gedocumenteerd. Dit maakt vooral kennis expliciet en verkleint de kans op interpretatieverschillen. Een verdere uitwerking daarvan in meer formele conceptuele modellen zorgt ervoor dat er duidelijkheid is over de dingen en eigenschappen die onderdeel zijn van het domein. Een conceptueel model zegt strikt genomen nog niets over hoe gegevens eruit zien, beschrijft alleen het (probleem)domein.

Op het moment dat de informatievoorziening wordt ingericht, moet worden nagedacht over de structuren die nodig zijn bij het opslaan, uitwisselen en gebruiken van gegevens. Er moet ook worden nagedacht over de eenheden waarin gegevens worden verwerkt (de groeperingen van gegevens die als geheel worden uitgewisseld). Als de eenheden te groot of te klein zijn dan ontstaan er mogelijk performanceproblemen bij het gebruik van een informatiesysteem of gegevensdiensten. Als de eenheden verkeerd worden gekozen dan wordt mogelijk onvoldoende invulling gegeven aan de informatiebehoefte van gebruikers, of sluiten ze mogelijk onvoldoende aan bij mogelijke wijzigingen in de toekomst. Bij deze structuur horen ook regels die aangeven welke beperkingen worden gesteld aan de gegevens en regels die aangeven hoe bepaalde soorten gegevens kunnen worden afgeleid van andere gegevens. Deze aspecten worden beschreven in logische modellen, waarvan er meerdere soorten bestaan. Zo zal er een logisch model nodig zijn voor het inrichten van de database waarin de gegevens worden opgeslagen, van de berichten of bestanden die worden uitgewisseld en van de informatieproducten die aan gebruikers worden verstrekt.

Uiteindelijk moeten deze modellen vertaald worden naar technische gegevensmodellen of schema's die bepalen hoe de gegevens in een bepaalde technologie worden gerepresenteerd. Dat gaat bijvoorbeeld over het formaat van de gegevens, over de precieze datatypes die gebruikt worden en over de technische implementatie van de regels. Schema's worden bijvoorbeeld gebruikt om een validatie uit te voeren, zodat gegevens een bepaalde basiskwaliteit bezitten.

In deze hele keten van modellen is het streven om te zorgen voor traceerbaarheid. Dat zorgt ervoor dat van individuele gegevens duidelijk is aan welk schema ze voldoen, welke structuur wordt gehanteerd, wat de gegevens precies betekenen en hoe dat zich verhoudt tot de woorden die worden gebruikt. Dit heet ook wel "verticale data lineage". Het vraagt dat elementen in modellen verwijzen naar elementen in modellen eerder in de keten. Het zorgt ervoor dat snel inzicht kan worden gegeven in de impact van wijzigingen in wet- en regelgeving, omdat alles daar (direct of indirect) aan verbonden is.

Naast genoemde modellen zou er ook aandacht moeten zijn voor het expliciet maken en waar mogelijk hergebruiken van waardelijsten. Denk bijvoorbeeld aan lijsten van landen of talen. De Europese Unie heeft een [lijst van waardelijsten](#) beschikbaar die binnen Europa relevant zijn. In Nederland is bijvoorbeeld de standaard [Thesauri en Ontologieën voor Overheidsinformatie](#) (TOOI) een interessante bron voor waardelijsten rondom overheidsorganisaties en publicaties.

	Beschouwingsniveau I	Beschouwingsniveau II	Beschouwingsniveau III	beschouwingsniveau IV
<i>Naam</i>	Semantisch	Conceptueel	Logisch	Implementatie
<i>Doel</i>	Analyseren	Analyseren	Ontwerpen	Ontwerpen
<i>Functie</i>	Elkaar begrijpen	Begrip van het domein expliciteren	Gegevensgebruik specificeren	Gegevensgebruik realiseren
<i>Voorbeeld- termen</i>	Begrippenmodel, Begrippenkader, Conceptmodel, Thesaurus, Taxonomie, Business glossary	Conceptueel informatiemodel, Ontologie, Kennismodel, Bedrijfsobjectenmodel, Domeinmodel	Logisch gegevensmodel, Logisch informatiemodel, Logisch datamodel	Technisch gegevensmodel, Technisch datamodel, Fysiek datamodel, Schema
<i>Doelgroep</i>	Iedereen	Expertgebruikers van informatiediensten	Ontwerpers van informatiediensten	Ontwikkelaars van informatiediensten
<i>Modelleer- talen</i>	SKOS, SBVR	OWL, RDFS, UML (OO), OntoUML, ORM, CogNIAM, FCO-IM, ERD (conceptueel), ArchiMate	SHACL, UML (OO), ERD (logisch)	SQL DDL, JSON Schema, XML Schema, ER (fysiek/implementatie), programmeertaal
<i>Inhoud</i>	<ul style="list-style-type: none"> Begrippen die worden gebruikt en herkenbaar zijn in het domein Definities en toelichtingen van de termen die worden gebruikt voor de begrippen Synoniemen/homoniemen en alternatieve schrijfwijzen van de begrippen zoals afkortingen Relatie naar wet- en regelgeving en beleid Hiërarchische en associatieve relaties tussen de begrippen Classificaties van de begrippen Regels over het domein in natuurlijke taal in termen van de begrippen (bedrijfsregels) 	<ul style="list-style-type: none"> Een formalisatie van dingen die bestaan in het domein Feiten en uitspraken over de dingen in het domein Eigenschappen van de dingen in het domein Eigenschappen die (mogelijk in combinatie) dingen uniek identificeren Naamgeving gericht op exactheid Formele definities van de dingen en hun eigenschappen Mogelijke waarden van eigenschappen Exacte relaties tussen de dingen Regels over de dingen en hun eigenschappen in een formele taal Verbalisaties over eigenschappen van dingen 	<ul style="list-style-type: none"> Een representatie van dingen in het domein als gegevens Clusters van gegevens die relevant zijn vanuit logistiek perspectief Individuele data-elementen binnen de gegevensclusters Identificaties van gegevensclusters, die geen identificatie op conceptueel niveau kennen Naamgeving gericht op gebruik in ontwerpen (bijv. CamelCase) Datatypes van de gegevens Relaties tussen de gegevens Regels over de gegevens en hun onderlinge relatie, mede op basis van kennis over hoe ze tot stand komen en worden gebruikt Vastlegging van historie van gegevens Vastlegging van gegevens t.b.v. herleidbaarheid en auditlogging 	<ul style="list-style-type: none"> Technologie-specifieke representatie van gegevens als data Technologie-specifieke datatypes Technologie-specifieke naamgeving van gegevens Technologie-specifieke representatie van identificaties (bijv. als URI's)

Tabel 3: Beschouwingsniveaus van modellen voor begrippen, informatie en gegevens

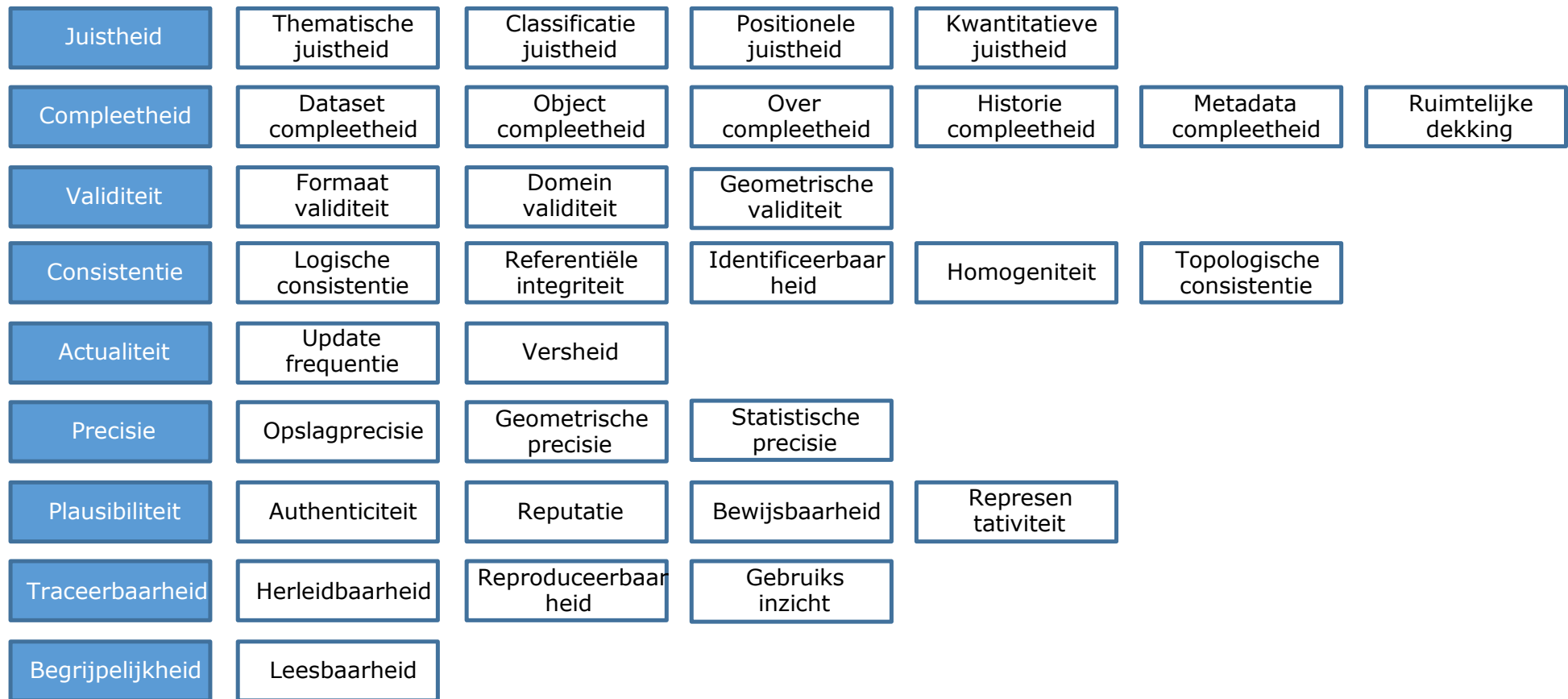
5.2.3 Gegevenskwaliteit

Het is belangrijk dat in de metagegevens ook informatie aanwezig is over de kwaliteit van gegevens. Dit zorgt ervoor dat gebruikers kunnen bepalen in hoeverre de kwaliteit van de gegevens voldoende is voor hun specifieke gebruik. Dat is in eerste instantie met name relevant op het niveau van een dataset zoals een informatieproduct. Er zou op dataset niveau minimaal een vriendelijke beschrijving aanwezig moeten zijn waarin alle voor de gebruiker relevante aspecten van de kwaliteit. Dat is zowel een beschrijving van de eisen die worden gesteld aan de kwaliteit als de feitelijke kwaliteit zoals die is gebleken uit metingen. Die laatste is meer dynamisch van aard en zal daardoor in catalogi minder actueel zijn. Het resultaat van een meting op een specifiek moment in tijd geeft gebruikers al wel meer gevoel.

Er zijn allerlei raamwerken en standaarden die gebruikt kunnen worden om meer gestructureerd en gericht uitdrukking te geven aan de kwaliteit van gegevens. Het resultaat is echter dat er allerlei verschillende termen en indicatoren worden gebruikt om uitdrukking te geven aan kwaliteit. Dit maakt het voor gebruikers lastig om dit goed te begrijpen. Om te komen tot meer consistentie is het belangrijk om met elkaar tot een gemeenschappelijke taal te komen in de vorm van een standaard raamwerk voor gegevenskwaliteit. Er is inmiddels een dergelijk raamwerk beschikbaar: het [NORA raamwerk gegevenskwaliteit](#) (zie ook Figuur 13). Dit raamwerk is gebaseerd op een brede set van standaarden en op allerlei kennis en ervaringen van overheidsorganisaties. De basis ervan is ontstaan in de context van de Omgevingswet. Het raamwerk is inmiddels ook omarmd door het federatief datastelsel. Het streven is daarmee om alle registraties die daar deel van uit gaan maken conform dit raamwerk te beschrijven. Dit streven is ook overgenomen in deze domeinarchitectuur.

De praktische implicaties van het gebruik van het raamwerk zijn ook besproken in een werkgroep binnen het programma federatief datastelsel. Het blijkt dat de diversiteit aan soorten gegevens, soorten contexten en gebruik het lastig maakt om tot een volledig gestandaardiseerde beschrijving te komen. Het meest waardevol en realistisch is om de kwaliteitsdimensies en attributen in het raamwerk vooral als categorie-indeling te gebruiken, zodat op dat niveau er in ieder geval een gestandaardiseerde taal is. Daarbinnen is het streven om zoveel mogelijk standaard zinstructuren te gebruiken, zodat de beschrijvingen zelf ook meer gestandaardiseerd kunnen zijn. Hiervoor zijn inmiddels zinsjablonen beschreven en beschikbaar. Idealiter zijn metagegevens over de kwaliteit van gegevens ook beschikbaar in machineleesbare vorm. Daarvoor bestaat de [DQV standaard](#), die gebaseerd is op Linked Data standaarden. Het NORA raamwerk kan hierin als taal worden gehanteerd. Vooralsnog is dit waarschijnlijk voor veel organisaties te ver gegrepen.

Los van de beschrijving van de huidige of gewenste kwaliteit aan de hand van een kwaliteitsraamwerk zouden ook de kwaliteitsregels zelf beschikbaar moeten zijn via de metagegevens. Kwaliteitsregels zijn een specifieke vorm van beperkingsregels en drukken uit binnen welke grenzen gegevens zich zouden moeten begeven. Het kwaliteitsattribuut "logische consistentie" verwijst naar de mate waarin aan dit soort regels wordt voldaan en heeft dan ook alleen betekenis als de regels zelf beschikbaar zijn. Het kwaliteitsattribuut "waarschijnlijkheid" zegt iets over de mate waarin de gegevens waarschijnlijk zijn voor de situatie en verwijst naar de mate waarin signaalregels worden overschreden. Signaalregels zijn een specifieke vorm van kwaliteitsregels die aangeven dat gegevens mogelijk foute waarden bevatten. Ze leiden tot een waarschuwing. Er is op dit moment geen eenvoudige technologie-onafhankelijke standaard voor het beschrijven van beperkingsregels, waardoor moet worden gekozen tussen natuurlijke taal, een zelfbedachte taal, een leverancierspecifieke taal of modelleertaalspecifieke talen zoals OCL of SHACL.



Figuur 13: NORA raamwerk gegevenskwaliteit

5.2.4 Voorwaarden en afspraken

Een andere belangrijke categorie van metagegevens heeft betrekking op de voorwaarden die gelden bij het gebruik van de gegevens. Dat zijn rechten, plichten en beperkingen die bijvoorbeeld kunnen voortvloeien uit wet- en regelgeving of auteursrechten. Het expliciet maken hiervan zorgt ervoor dat afnemers en gebruikers weten binnen welke grenzen gebruik van de gegevens mogelijk is. Het daadwerkelijk gebruik van de gegevens kan daarmee beschouwd worden als het impliciet akkoord gaan met deze gegevens. Het is ook mogelijk om rechten, plichten en beperkingen als afspraken in een overeenkomst op te nemen. Tabel 4 beschrijft een aantal voorbeelden van metagegevens met betrekking tot voorwaarden en de standaarden waar ze uit afkomstig zijn. Dublin Core (ISO 15836) is een algemene standaard voor metagegevens, die initieel voor web content is ontworpen. DCAT is gericht op metagegevens voor datasets. NL ISO 19115 is het Nederlandse metadata profiel op de ISO 19115 standaard voor geografische datasets. ODRL is een standaard voor het beschrijven van rechten, plichten en beperkingen.

Naam	Omschrijving	Standaard
license	Een verwijzing naar een juridisch document dat toestemming geeft om iets te doen met de resource.	Dublin Core / DCAT
accessRights	Informatie over wie toegang heeft tot de resource of een indicatie van de beveiligingsstatus.	Dublin Core / DCAT
rights	Een uitspraak of verwijzing naar eigendomsrechten, voor zover deze niet beschreven worden door license of accessRights.	Dublin Core / DCAT
rightsHolder	Een persoon of organisatie die eigenaar is of de rechten beheert over de resource.	Dublin Core / DCAT
hasPolicy	Machineleesbare autorisatieregels die rechten, plichten en/of beperkingen uitdrukken die van toepassing zijn op de resource.	ODRL / DCAT
accessConstraints	Juridische toegangsbeperkingen zoals copyrights, patenten, patentaanvragen, handelsmerken, licenties, intellectuele eigendomsrechten, verboden op gebruik of overige beperkingen.	NL ISO 19115
otherConstraints	Een verwijzing en beschrijving van de creative commons beperkingen die van toepassing zijn.	NL ISO 19115
useLimitation	Een beschrijving van de toepassingen waarvoor de dataset niet geschikt is.	NL ISO 19115
classification	Een classificatie van het vertrouwelijkheidsniveau en een omschrijving van de beperkingen als informatie vertrouwelijk is.	NL ISO 19115

Tabel 4: Voorbeelden van metagegevens voor rechten, plichten en beperkingen

Voor het uitwisselen van gevoelige gegevens zoals persoonsgegevens is het niet voldoende om relevante metagegevens te publiceren. Er zullen aanvraagprocessen nodig zijn (toetsing op privacy en ethiek ligt bij de afnemer). Op het moment dat aanvragen worden goedgekeurd, dan zullen mogelijk specifieke overeenkomsten moeten worden opgesteld. Denk daarbij bijvoorbeeld aan verwerkersovereenkomsten, maar ook aan gegevensleveringsovereenkomsten waarin de specifieke afspraken over bijvoorbeeld verantwoordelijkheden, de betrokken gegevens en de specifieke eisen zijn beschreven. Generieke voorwaarden zouden al op een hoger niveau moeten zijn geborgd, zoals in de vorm van algemene voorwaarden en service level agreements.

In de huidige praktijk zijn er al allerlei aanvraagprocessen, maar kunnen deze best een lange doorlooptijd kennen en allerlei menselijke interpretatie en beoordeling vragen. Het streven is daarom om dit soort aanvraagprocessen te stroomlijnen en delen die zich daarvoor lenen te automatiseren. Dit vraagt dat bepaalde voorwaarden en afspraken ook worden vastgelegd in machineleesbare vorm, bijvoorbeeld conform de ODRL standaard. Onderdeel daarvan is ook dat controles die bij een aanvraag relevant zijn, alsook autorisatiescontroles die worden uitgevoerd bij

het daadwerkelijk gebruik van de gegevens in machineleesbare regels zijn beschreven. Dit wordt "Policy Based Access Control" genoemd en wordt in meer detail beschreven [in de domeinarchitectuur toegang](#). Het inrichten van de controleprocessen en bijbehorende systemen vraagt echter een behoorlijke inspanning en wordt dus liefst generiek ingericht. Er zijn hiervoor standaard afsprakenstelsels beschikbaar waarvan gebruik kan worden gemaakt, zoals iShare en de technologie van de International Data Spaces Association.

5.2.5 Herkomst van gegevens

Het is belangrijk om te kunnen begrijpen wat de herkomst is van gegevens. Het geeft een belangrijke indicatie van de kwaliteit van gegevens en bepaalt daarmee voor een belangrijk deel het vertrouwen dat gebruikers in de gegevens hebben. De herkomst van gegevens kan op allerlei niveaus in metagegevens zijn vastgelegd. De basis is dat in de metagegevens van een dataset duidelijk is welke organisatie de gegevens gecreëerd heeft. Voor individuele gegevens kan bijvoorbeeld relevante context zijn welke specifieke persoon ze heeft gecreëerd, op welk moment, naar aanleiding van welke gebeurtenis en als onderdeel van welke activiteit (zie ook Figuur 14).



Figuur 14: Gegevens in context

Voor informatieproducten geldt dat zij zijn afgeleid van brongegevens middels een transformatie. Gebruikers willen weten welke bronnen en afleidingsregels gebruikt zijn. De gebruikte bronnen moeten dan zijn beschreven in de metagegevens van het informatieproduct en de afleidingsregels moeten op te vragen zijn door gebruikers. Het liefst hebben gebruikers ook inzicht in de gebruikte brongegevens. Ze willen dat inzichtelijk hebben bij individuele gegevens in een rapport of dashboard waar ze naar kijken. In de door Kadaster en Geonovum ontwikkelde [IMX standaard](#) voor het samenstellen van gegevens is per individueel gegeven vastgelegd op basis van welke brongegevens en afleidingsregels deze tot stand is gekomen. Idealiter is de volledige keten inzichtelijk, van inwinning, via bewerkingen en transformaties tot op wat op een scherm zichtbaar is. Of dat ook echt noodzakelijk en haalbaar is zal in een individuele context moeten worden bepaald. Als niet de gehele keten inzichtelijk is bij een informatieproduct, dan zouden afleidingsregels in ieder geval in alle schakels van de keten moeten kunnen worden opgevraagd.

Tabel 5 laat zien hoe bepaalde soorten metagegevens zoals weergegeven in Figuur 14 zich verhouden tot een aantal standaarden voor metagegevens. De cellen geven de soorten metagegevens weer in de standaarden PROV, Dublin Core en MDTO geredeneerd vanuit de gegevens zelf. De PROV standaard is specifiek gericht op het beschrijven van herkomst (provenance). De eerder genoemde IMX standaard is ook gebaseerd op de PROV standaard. De MDTO standaard is gericht op metagegevens voor duurzame toegankelijkheid. Niet weergegeven in de tabel is bijvoorbeeld de DCAT standaard, aangezien deze vooral gebruik maakt van de Dublin Core en PROV standaarden. In het applicatieprofiel voor DCAT (DCAT-AP 3.0) is ook een metagegeven beschikbaar voor het beschrijven van de wettelijke grondslag voor een dataset (applicableLegislation). Genoemde standaarden kennen allemaal een Linked Data representatie. Als de gegevens zelf beschikbaar zijn als Linked Data, dan zijn deze ook direct verbonden aan de bijbehorende ontologie (informatie/gegevensmodel).

	PROV	Dublin Core	MDTO
<i>Gebeurtenis</i>	wasGeneratedBy.qualifiedStart		event
<i>Betrokkene</i>	wasAttributedTo	creator, contributor, publisher, rightsHolder	betrokkene, event.eventVerantwoordelijkActor
<i>Activiteit</i>	wasGeneratedBy		activiteit
<i>Locatie</i>	wasGeneratedBy.atLocation	coverage	dekkingInRuimte
<i>Gebeurtenismoment</i>	generatedAtTime	created, modified	event.eventTijd
<i>Object</i>	Entity	BibliographicResource	Informatieobject
<i>Registratiemoment</i>		issued	event.eventTijd
<i>Vermoedelijke fout</i>			event.eventResultaat
<i>Begrip</i>			classificatie
<i>Brongegevens</i>	wasDerivedFrom	source	gerelateerdInformatieobject
<i>Afleidingsregels</i>	qualifiedDerivation		

Tabel 5: Metagegevens voor herkomst in een aantal standaarden voor metagegevens

In de context van de hernieuwde eIDAS verordening zal er een European Digital Identity Wallet beschikbaar komen. Hierin kunnen gebruikers verifieerbare verklaringen plaatsen van allerlei partijen, die ze vervolgens kunnen verstrekken aan dienstverleners. Een verifieerbare verklaring is eigenlijk een bewijs dat gegevens afkomstig zijn van een bepaalde partij. Het zegt daarmee dus ook iets over de herkomst van gegevens. Ook in de context van de Single Digital Gateway zullen allerlei organisaties verifieerbare verklaringen moeten gaan leveren. Daarbij gaat het vooral over grensoverschrijdende procedures die ondersteund moeten worden, zoals het opvragen van een diploma van iemand. Bij elkaar zorgt dit ervoor dat het toenemend belangrijk wordt voor organisaties om verifieerbare verklaringen te kunnen leveren, om voorbereid te zijn op dit soort ontwikkelingen. Ook los van deze ontwikkelingen is het leveren van een meer formeel bewijs van de herkomst van gegevens mogelijk waardevol. Het geeft afnemers een bepaald vertrouwen in het gegeven en de herkomst. Op technisch niveau kan er ook gekozen worden voor het ondertekenen van een bericht om een vorm van onweerlegbaarheid te realiseren.

5.3 Verdieping: communicatieprotocollen

In dit deel van de architectuur wordt ingegaan op de verschillende vormen van gegevensuitwisseling. Er wordt specifiek ingegaan op de Digikoppeling standaard en de gewenste doorontwikkeling ervan. Daarna worden andere communicatieprotocollen en standaarden benoemd en wordt ook de nieuwe FSC standaard toegelicht.

5.3.1 Vormen van gegevensuitwisseling

Het is belangrijk om te onderkennen dat er heel veel verschillende vormen van gegevensuitwisseling bestaan, op allerlei abstractieniveaus, met allemaal hun eigen specifieke focus. Veel van deze vormen hebben een eigen bestaansrecht. Het is dan vooral ook de vraag wanneer je ze zou moeten toepassen. Het onderscheidende bij al deze vormen van uitwisseling is vooral dat wat centraal staat (de focus heeft). Dat kan zijn 1. de service, 2. de resource, 3. het event, 4. de gegevens, 5. het bericht of 6. de betekenis.

Service-oriëntatie: Bij service-oriëntatie (ook wel: Service Oriented Architecture - SOA) bieden applicaties hun functionaliteit aan in de vorm van services. Een applicatieservice is een logisch afgebakend stuk functionaliteit waarmee een bedrijfsfunctie ondersteund wordt. Het is te zien als een doorontwikkeling van wat eerder Remote Procedure Calls werden genoemd, in combinatie met ideeën uit componentgebaseerde software-ontwikkeling. Service-oriëntatie is min of meer synoniem geworden aan het gebruik van Web Services op basis van de SOAP standaard, alhoewel je het ook met andere communicatieprotocollen kunt realiseren.

Resource-oriëntatie: Tegenwoordig is er toenemende aandacht voor integratie op basis van RESTful API's, dat je kunt zien als onderdeel van resource-oriëntatie. Bij resource-oriëntatie ligt de nadruk niet op de service maar op de te benaderen resource (bijvoorbeeld een klantobject). Elke resource heeft daartoe een eigen adres (URL) en kent standaard operaties voor het creëren, lezen, wijzigen en verwijderen van gegevens. Bij RESTful API's staat de standaard HTTP centraal en wordt ervan uitgegaan dat de server geen toestand bijhoudt. Het is daardoor relatief goed schaalbaar.

Eventoriëntatie: Bij eventoriëntatie (ook wel: Event Driven Architecture - EDA) vormen gebeurtenissen de initiator voor uitwisseling van gegevens. Denk aan de geboorte van een kind, een huwelijk en een verhuizing. Bij event-oriëntatie wordt veel gewerkt met het publish-and-subscribe mechanisme, waarbij applicaties zich kunnen abonneren op bepaalde typen gebeurtenissen, die vervolgens worden genotificeerd bij het optreden van deze gebeurtenissen. Een combinatie tussen eventoriëntatie en berichtoriëntatie komt wel vaker voor. Message oriented middleware biedt dan functionaliteit voor publish-and-subscribe. Een specifieke vorm van eventoriëntatie is eventstreaming, waarbij events in een persistente stroom worden geplaatst en er ook zoekvragen aan de stroom zelf kunnen worden gesteld. Eventoriëntatie is vooral relevant als snel moet kunnen worden ingesprongen op gebeurtenissen.

Gegevensoriëntatie: Bij de uitwisseling van gegevens kunnen ook de gegevens zelf centraal staan. Je zou dit gegevensoriëntatie kunnen noemen. De functionaliteit en de rol van de gegevens in een proces zijn daarbij van ondergeschikt belang. Het belangrijkste is dat er een aanbieder is van gegevens en een afnemer van deze gegevens. De precieze vorm van de gegevens en de manier waarop de gegevens worden uitgewisseld kan sterk variëren. Het kan gaan om de uitwisseling van bestanden, het bevragen van gegevensbronnen of het synchroniseren van gegevensbronnen. Synchronisatie van gegevensbronnen maakt typisch gebruik van Change Data Capture technologie, waarbij elke wijziging zoals vastgelegd in de transactielog van een database wordt uitgewisseld. Hiermee kan een volledige replica (of subset ervan) van een gegevensbron worden gemaakt op een andere locatie. Gegevensoriëntatie leent zich in het algemeen goed voor periodieke (batch)processen.

Berichtoriëntatie: Bij berichtoriëntatie staat het bericht centraal, die typisch ook asynchroon wordt gecommuniceerd. Dat betekent dat de zender niet wacht op een antwoord. Vaak gaat het om verwerkingen die uitgesteld verwerkt kunnen worden, zoals periodieke batchprocessen. De nadruk ligt dan vooral op het asynchroon en betrouwbaar verzenden van berichten met Message Oriented Middleware, typisch op basis van queueing mechanismen. Door de ontkoppeling van de zender en de ontvanger met een queue is het eenvoudiger om het aantal gelijktijdige verwerkingen op te schalen.

Betekenisoriëntatie: Bij betekenisoriëntatie staat het betekenisvol publiceren van gegevens op het wereldwijde web centraal. Dat betekent dat het formeel beschrijven van de betekenis van de gegevens en het beschikbaar stellen van deze gegevens conform webstandaarden belangrijk is. Betekenisoriëntatie leent zich dan ook erg goed voor het publiceren van metagegevens. Gegevens krijgen ook meer betekenis door relaties te leggen naar andere begrippen en gegevens. Het op een efficiënte manier verwerken van de gegevens is daarbij minder belangrijk. In deze context wordt ook gesproken over het semantische web, waarbij gegevens betekenisvol beschikbaar zijn op het web en aan elkaar verbonden. Webstandaarden zoals HTTP staan daarbij centraal. Met het SPARQL protocol kunnen complexe zoekvragen worden gesteld, ook federatief over meerdere bronnen.

5.3.2 Digikoppeling

Het is belangrijk om gegevensuitwisseling te standaardiseren, waar mogelijk. Overheidsbreed is hiervoor de Digikoppeling standaard gedefinieerd. De Digikoppeling standaard maakt veilige gegevensuitwisseling tussen overheden mogelijk. De standaard beschrijft afspraken om gegevens juist te adresseren, leesbaar en uitwisselbaar te maken en veilig en betrouwbaar te verzenden. Het bevordert de interoperabiliteit tussen overheidsorganisaties. De standaard bestaat uit een viertal koppelvlakspecificaties voor gestructureerd gegevensuitwisseling met en tussen overheidsorganisaties:

- Digikoppeling Koppelvlakstandaard WUS - voor synchrone uitwisseling van gestructureerde berichten;
- Digikoppeling Koppelvlakstandaard ebMS2 - voor asynchrone uitwisseling voor betrouwbaar berichtenverkeer.
- Digikoppeling Koppelvlakstandaard REST-API - voor synchrone gegevensuitwisseling met resources;
- Digikoppeling Koppelvlakstandaard Grote Berichten - voor het uitwisselen van grote bestanden.

Zoals beschreven in de [architectuur Digikoppeling](#) is Digikoppeling gericht op de beveiligde uitwisseling van gestructureerde gegevens tussen systemen van Nederlandse overheidsorganisaties en instellingen uit de (semi-)publieke sector. Het zegt niets over de toepassing van de standaard buiten deze afbakening: met bedrijven, van open data of van ongestructureerde gegevens. Het is verplicht om te gebruiken bij gesloten diensten, de uitwisseling met GDI-voorzieningen en bij sector-overstijgende uitwisseling. Uitwisseling van geografische gegevens is uitgesloten van het functioneel toepassingsgebied.

Synchrone uitwisseling kan worden ingericht op basis van de Digikoppeling-koppelvlakstandaard WUS en het Digikoppeling REST API profiel. Digikoppeling Koppelvlakstandaard ebMS2 biedt specifieke ondersteuning voor asynchrone uitwisseling en betrouwbare aflevering. Digikoppeling Grote Berichten is gericht op de veilige bestandsoverdracht van berichten groter dan 20 MB, met name in de context van ebMS en WUS. Als er behoefte is aan signing en/of encryptie dan zijn alleen de WUS en ebMS koppelvlakstandaarden geschikt (er is wel een voorstel hierover voor de koppelvlakstandaard REST API). Dat is bijvoorbeeld relevant als zich tussen aanbieder en afnemer een niet vertrouwde intermediair bevindt. Er is in de huidige versie van de Digikoppeling

architectuur geen onderscheid meer tussen 'WUS voor bevestigingen' en 'ebMS voor meldingen'. In de praktijk bleek dit onderscheid niet altijd goed te werken.

Partijen bepalen in onderling overleg welke Digikoppeling profiel ze gebruiken. Aanbieders bepalen welke koppelvakstandaard gebruikt wordt voor een door hun geleverde dienst. Per dienst kunnen ook meerdere koppelvakstandaarden aangeboden worden.

5.3.3 Doorontwikkeling van Digikoppeling

In deze paragraaf schetsen we een aantal inzichten en ontwikkelingen die invloed hebben op de Digikoppeling standaard. Ons advies is om te onderzoeken of Digikoppeling als bredere standaard kan worden gepositioneerd, ook voor communicatie met bedrijven, binnen sectoren en mogelijk zelfs voor open data. Dat draagt bij aan maximale standaardisatie, hogere interoperabiliteit en maakt het uiteindelijk voor organisaties dus alleen maar eenvoudiger. Dit vraagt wel aandacht voor aansluitvoorwaarden en een stringenter vorm van lifecyclemanagement van de Digikoppeling standaard.

Digikoppeling is ontwikkeld voor toepassing op nationaal niveau. Voor gegevensuitwisseling op EU-niveau gelden EU-standaarden, waarvan e-Delivery op dit moment de dominante is. Voor gegevensuitwisseling met Europese overheden is gebruik van de e-Delivery standaard dus aanbevolen. Het zou goed zijn als de Digikoppeling-standaarden zoveel mogelijk afgestemd zijn op de e-Delivery standaard. Dat zou het eenvoudiger maken voor Nederlandse overheidsorganisaties om gegevens via Digikoppeling automatisch ook internationaal beschikbaar te kunnen stellen. Daarnaast zou de e-Delivery standaard zelf mogelijk ook als Digikoppeling koppelvakstandaard kunnen worden gedefinieerd. Het vraagt nader onderzoek om te bepalen of dit meerwaarde heeft.

Er is inmiddels een vervanger van de ebMS2 standaard zoals onderdeel van het koppelvakprofiel ebMS, namelijk de ebMS3 standaard. Wij adviseren om migratie naar deze ebMS3 standaard in te zetten, zeker ook gegeven dat deze standaard ook Europees wordt gebruikt als onderdeel van de e-Delivery standaard. Aandachtspunt is dat ebMS3 niet backwards compatible is met ebMS2. Het is dan ook belangrijk om een implementatie- en migratieplan op te stellen waarin deze aandachtspunten nader zijn uitgewerkt.

De Digikoppeling standaard is ontwikkeld voor gegevensuitwisseling tussen organisaties, maar het zou beter zijn als deze standaard ook voor uitwisseling met bedrijven ingezet kan worden. Gegevensuitwisseling met overheidsorganisaties is niet fundamenteel anders dan met bedrijven. De inzet voor bedrijven is al grotendeels mogelijk, maar een expliciete toets hierop en eventuele aanpassing van de standaard is wenselijk. Met name de kosten die verbonden zijn aan de beveiligingscertificaten zijn een mogelijke drempel.

Er is een voorgestelde uitbreiding van de koppelvakstandaard REST API met signing en encryptie, waardoor het beter geschikt is voor beveiligde uitwisseling van gegevens. Vanuit het Common Ground initiatief bij gemeenten is inmiddels de FSC-standaard ontwikkeld, die een aantal functies biedt die in meer algemene zin waardevol zijn bij het gebruik van (HTTP-gebaseerde) API's. Zo biedt het bijvoorbeeld mechanismen om partijen te machtigen voor het gebruik van API's van derden. We zien het als een logische stap, die ook inmiddels al is ingezet, om deze FSC standaard te combineren met de Digikoppeling API koppelvak standaard en om daarmee om te vormen tot een landelijke standaard.

De koppelvakstandaard REST API is nu specifiek gericht op RESTful API's. Tegelijkertijd zien we het belang van andere uitwisselprotocollen zoals GraphQL en SPARQL. Deze protocollen bieden meer specifieke mogelijkheden dan RESTful API's, bijvoorbeeld om mogelijke performanceproblemen die kunnen optreden bij het gebruik ervan te voorkomen. Het gebruik van

RESTful API's kan namelijk tot relatief veel kleine verzoeken leiden, wat tot performanceproblemen kan leiden. GraphQL is bijvoorbeeld mogelijk een beter bruikbaar protocol als er sprake is van complexe bevestigingen, mogelijk ook over meerdere endpoints. We denken dat Digikoppeling ook rekening zou moeten houden met het gebruik van dit soort protocollen.

5.3.4 Andere communicatieprotocollen en standaarden

Zoals beschreven heeft de Digikoppeling standaard een voorgeschreven functioneel toepassingsgebied. We denken dat het waardevol is om de Digikoppeling standaard ook buiten het huidige inzetgebied te gebruiken als dat meerwaarde heeft. Tegelijkertijd onderkennen we dat er ook andere communicatieprotocollen en standaarden zijn die mogelijk relevant zijn en een eigen logisch toepassingsgebied hebben. In de volgende tabel benoemen we een aantal relevante standaarden en het functionele toepassingsgebied. Voor een deel zijn dit soort standaarden ook opgenomen in de lijsten van Forum Standaardisatie. Voor die standaarden hebben we het functioneel toepassingsgebied overgenomen over de betreffende lijst en geven we aan welke status de standaard bij het Forum Standaardisatie heeft. Functioneel toepassingsgebieden die we zelf voorstellen geven we schuingedrukt weer.

Standaard	Functioneel toepassingsgebied	Status
Geo-standaarden	Geo-standaarden moeten worden toegepast op de uitwisseling van geografische informatie tussen organisaties, waarbij de ruimtelijke dimensie van significant belang is.	Verplicht
OData	OData kan worden toegepast voor het bouwen en gebruiken van REST APIs met als doel het gestructureerd ontsluiten van (statistische) open datasets.	Aanbevolen
GraphQL	<i>Het flexibel bevrogen van meerdere resources.</i>	geen
SPARQL	<i>Het bevrogen van Linked Data resources.</i>	geen
IIIF	<i>Het bevrogen van multimediale web resources.</i>	geen
AMQP	<i>Het realtime en/of betrouwbaar uitwisselen van berichten.</i>	geen

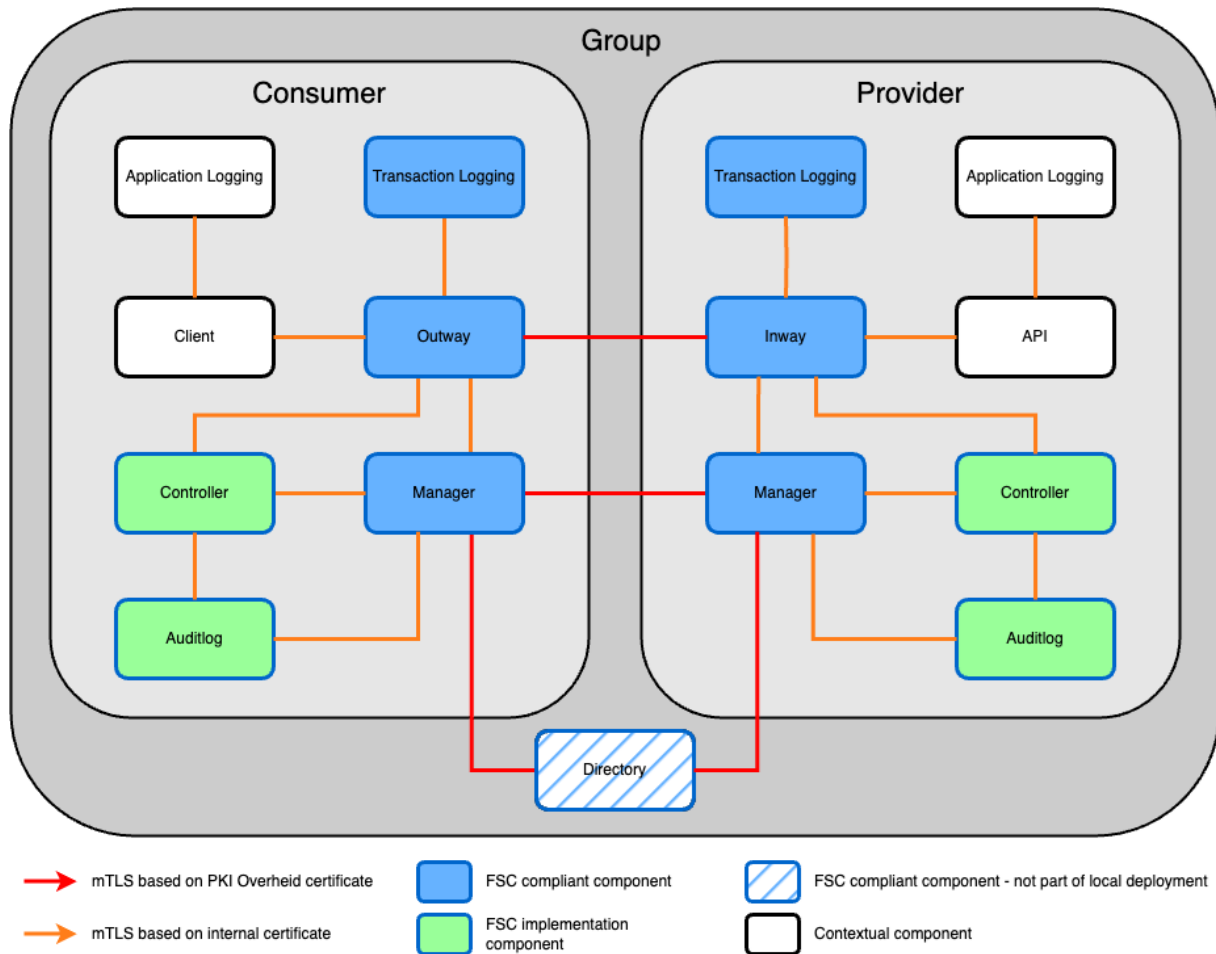
Tabel 6: Standaarden, functioneel toepassingsgebied en status bij Forum Standaardisatie

5.3.5 Federated Service Connectivity

De Federated Service Connectivity (FSC) standaard is ontwikkeld in de context van het Common Ground programma voor gemeenten. Het standaardiseert de werking van tussenliggende componenten die het gebruik van API's vereenvoudigen (zie ook Figuur 15). De standaard wordt inmiddels ondersteund door verschillende leveranciers en is gepositioneerd als een brede standaard die door alle overheidsorganisaties kan worden gebruikt. Het is voorgesteld als onderdeel van het Digikoppeling profiel voor REST API's, maar kan in bredere zin worden gebruikt voor gegevensuitwisseling tussen systemen over HTTP.

De kern van de FSC standaard is dat het een vertrouwensnetwerk kan creëren tussen systemen door het creëren van contracten tussen partijen. De API's die worden aangeboden en de bijbehorende contracten worden geregistreerd in een directory, waarvan er meerdere kunnen zijn. In een directory kunnen API's worden gezocht en op basis daarvan kunnen ze worden aangeroepen door systemen, waarbij het resulterende berichtenverkeer verloopt over tussenliggende FSC componenten. Er is een tussenliggend componenten bij het zendende systeem (outway) en een tussenliggend componenten bij het ontvangende systeem (inway). In deze componenten kan ook extra functionaliteit worden aangeroepen, zoals het loggen van de berichten. Hiervoor wordt een transactie-identificatie gegenereerd, die bij elkaar behorende berichten kan correleren. Daarnaast zijn er manager componenten die vooral verantwoordelijk zijn voor de contractafhandeling. Het is mogelijk om machtigingen tussen systemen toe te kennen. Hierdoor kan een systeem van een

derde partij (bijvoorbeeld een SaaS leverancier) een machtiging ontvangen om namens een overheidsorganisatie gebruik te maken van een ander systeem. Dit voorkomt dat er sleutels van certificaten aan deze derde partij moeten worden verstrekt, wat vanuit beveiligingsperspectief onwenselijk is.



Figuur 15: De architectuur van de Federated Service Connectivity standaard

5.4 Verdieping: historie

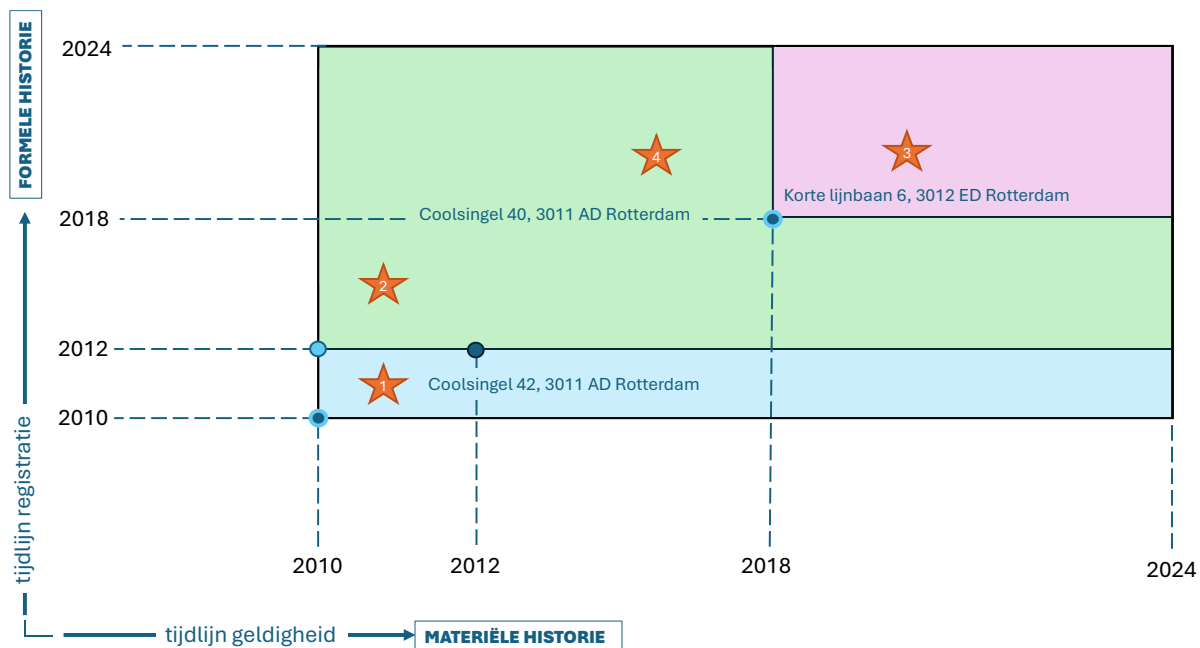
Gegevens zijn een belangrijke grondstof, die voor verschillende doelen bruikbaar zijn. Op het moment dat een registratie invulling geeft aan relevante functionele en niet functionele eisen dan kan deze als bronregistratie gebruikt worden. Aan bronregistraties moeten standaard eisen worden gesteld over het vastleggen en beschikbaar stellen van historie. Historie is een verantwoordelijkheid van een bronhouder, maar is ook zichtbaar en relevant voor afnemers. Daarmee is het ook een aspect om rekening mee te houden bij gegevensuitwisseling.

5.4.1 Vormen van historie

Voor veel afnemers is het van belang dat een bronregistratie actuele gegevens kan leveren. Er zijn ook allerlei processen waarin gegevens van een peildatum relevant zijn. Denk bijvoorbeeld aan een gemeentelijk WOZ-proces waarbij gegevens rondom een pand op de peildatum 1 januari van belang zijn. Het is dan nodig dat in de bronregistratie wordt vastgelegd op welk moment bepaalde wijzigingen zijn doorgevoerd. We noemen dit het bijhouden van de “formeel historie” van gegevens. Deze worden vastgelegd in de tijdlijn registratie, die de veranderingen van gegevens in de registratie bijhoudt. Je zou daarbinnen nog onderscheid kunnen maken tussen het moment waarop een gegeven is ontvangen en het moment waarop het beschikbaar is voor verdere verwerking. De laatste is vooral relevant, aangezien dat bepaalt wanneer gebruikers over de gegevens hebben kunnen beschikken. Formele historie is een basis die iedere bronregistratie moet ondersteunen.

Naast deze tijdlijn registratie is het vaak ook relevant om te weten wanneer het object waarnaar de gegevens verwijzen, in de werkelijkheid is gewijzigd. Neem als voorbeeld een persoon die verhuist. Tussen het moment van daadwerkelijk verhuizen en het doorgeven van de verhuizing aan de gemeente kan een aantal dagen passeren. In de tijd tussen daadwerkelijk verhuizen en het formeel vastleggen van die verhuizing door de gemeenten loopt hetgeen de gemeente formeel weet en dat wat in de werkelijkheid een feit is uit elkaar. De persoon woont immers een aantal dagen op een ander adres dan bij de gemeente is vastgelegd in de registratie. Het vastleggen van de veranderingen van een object in de werkelijkheid door een bronregistratie noemen we de “materiële historie”. Deze wordt bijhouden in de tijdlijn geldigheid.

Het vastleggen van materiële historie is niet voor alle bronregistraties relevant. De noodzaak voor het vastleggen van deze historie moet per bronregistratie specifiek worden onderzocht en bepaald op basis van eisen en wensen vanuit het gebruik. Voor registraties die een juridische werkelijkheid vastleggen is het vastleggen van materiële historie essentieel. Het is bij dit soort registraties voor afnemers belangrijk dat zij vast kunnen stellen wat iemand op een bepaald moment in de tijd kon weten over een situatie in de werkelijkheid. Als zowel de formele als de materiële historie van belang is spreken we ook wel van bi-temporaliteit, omdat er sprake is van de vastlegging van twee tijdlijnen. Bitemporale registraties zijn in staat vragen te beantwoorden over dat wat was geregistreerd en dat wat geldig was op een specifiek moment in het verleden. Figuur 16 illustreert dit.



Figuur 16: Voorbeeld van historie met twee tijdlijnen (bi-temporaliteit)

Figuur 16 geeft de twee tijdlijnen weer voor de wijzigingen van een adres. Op de horizontale as is de tijdlijn geldigheid weergegeven en op de verticale as de tijdlijn registratie. Weergegeven is de situatie waar initieel in 2010 een adres is geregistreerd (het blauwe vlak) en daarna tweemaal is gewijzigd. De eerste wijziging heeft plaatsgevonden in 2012 en betrof een correctie van het adres in verband met een onjuiste registratie van het huisnummer bij het adres. Vanaf 2012 staat in de registratie het correcte adres, dat geldig is vanaf 2010 (het groene vlak). Het foutieve adres dat vanaf 2010 in de registratie stond wordt beëindigd per 2012 (op de tijdlijn registratie). De tweede wijziging betreft de doorgifte van een adreswijziging in 2018. Door deze adreswijziging wordt het huidige adres (groen blok) beëindigd per 2018 en het nieuwe adres (groen blok) wordt geldig vanaf 2018.

Door het registreren van de tijdstippen van registratie en de tijdstippen van geldigheid is het mogelijk om te tijdreizen over de twee assen.

- Als in 2011 een afnemer het actuele adres opvraagt dan ontvangt de afnemer 'Breedstraat 1, 4006XX, Breda' als antwoord.
- Als in 2014 de vraag stelt wat het adres in 2011 was dan ontvangt de afnemer 'Breedstraat 3, 4006XX, Breda'. Dit doordat het adres in verband met een administratieve correctie met terugwerkende kracht gecorrigeerd is.
- Als in 2020 een afnemer het actuele adres opvraagt dan ontvangt de afnemer 'Kerkstraat 84, 2118 AD, Gouda' als antwoord.
- Als in 2020 een afnemer het in 2016 geregistreerde adres opvraagt dan ontvangt de afnemer 'Breedstraat 3, 4006XX, Breda' als antwoord.

Genoemde tijdslijnen moeten worden gerespecteerd bij het wijzigen, rectificeren en vergeten van gegevens. Uitgangspunt daarbij is dat gegevens nooit fysiek worden verwijderd of overschreven, tenzij daar een expliciete juridische reden voor is. Uiteraard is het wel belangrijk om na einde bewaartermijn de gegevens te vernietigen. Daarnaast zouden bronregistraties de vragen moeten kunnen beantwoorden over dat wat was geregistreerd en dat wat geldig was op een specifiek moment in het verleden.

5.4.2 Structureren van historie

Het is belangrijk om te beseffen dat het vastleggen en beschikbaar stellen van historie niet los gezien kan worden van de structuren waarin gegevens worden geregistreerd en uitgewisseld. In de huidige praktijk wordt vaak het resultaat van gebeurtenissen voor objecten (de stand van zaken) in een registratie opgeslagen. Het lastige van deze wijze van registratie is eigenlijk dat het onvoldoende recht doet aan dat wat eraan ten grondslag ligt. Gegevens zijn vooral een uitdrukking van een feit (gebeurtenis) in de werkelijkheid, in een specifieke context. Het is daarmee belangrijk om alle relevante context ook vast te leggen bij de gegevens. Daarnaast wijkt de inherent hiërarchische structuur van berichten die worden uitgewisseld na een gebeurtenis vaak af van de structuur waarin gegevens worden opgeslagen. Het is voor het kunnen werken met historie veel logischer als feiten zelf de eenheid van registratie zijn. Feiten kunnen dan gewoon als consistent geheel worden toevoegen aan een registratie en als geheel beschikbaar worden gesteld aan anderen. Wijzigingen in gegevens die bijvoorbeeld het gevolg van een administratieve correctie zijn, zouden ook expliciet als correctie vastgelegd moeten worden. In de uitwisseling van gegevens zou dit ook als metagegeven expliciet moeten zijn. Er ontstaat hierdoor een meer betrouwbare registratie.

Er is ook andere context die relevant is om toe te voegen aan feiten. Zo is het bijvoorbeeld mogelijk dat er terugmeldingen worden gedaan op bepaalde gegevens en dat deze in onderzoek worden geplaatst. Een dergelijke markering geeft belangrijke context aan een gegeven. Het kan ook zijn dat er kwaliteitscontroles op de gegevens hebben plaatsgevonden en dat een gegeven is gemarkeerd als niet plausibel (mogelijk foutief). Dat is ook relevante context voor het gegeven. Tenslotte kunnen gegevens ook zijn afgeleid van andere gegevens en kan het belangrijk zijn om bij het feit van afleiding te verwijzen naar de gebruikte afleidingsregels. Door een registratie dus te structureren en beschikbaar te stellen als een verzameling van feiten en de mogelijkheid te bieden om deze feiten te annoteren met relevante context ontstaat een veel rijkere registratie. De mate waarin een dergelijke registratie ook kan voldoen aan eisen van performance en schaalbaarheid vraagt wel aandacht.

5.5 Verdieping: notificeren

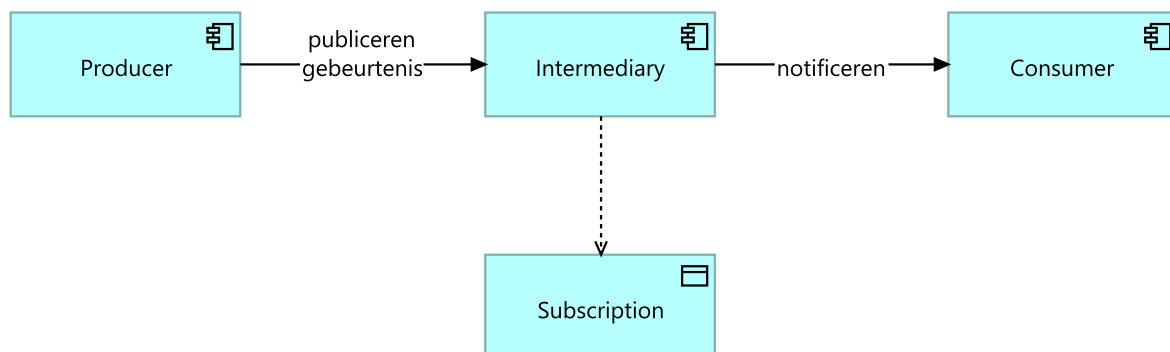
Dit deel van de architectuur beschrijft architectuuraspecten die van belang zijn bij het notificeren over gebeurtenissen. Het start met een uitleg van de terminologie die specifiek in dit hoofdstuk wordt gehanteerd. Deze terminologie is gebaseerd op de CloudEvents standaard en is te zien als een doorvertaling van de meer algemene begrippen in dit document, naar de invulling voor op applicatieniveau. Vervolgens gaat het hoofdstuk in op de applicatie-architectuur en de relevante standaarden.

5.5.1 Terminologie

Als we spreken over notificeren, refereren we in meer algemene zin naar een gebeurtenisgedreven werkwijze. Daarbij notificeren aanbieders afnemers en verstrekken ze daarbij gegevens over plaatsgevonden gebeurtenissen. Voorafgaand daaraan abonneren afnemers zich door aan te geven voor welke typen gebeurtenissen zij genotificeerd willen worden. De plaatsgevonden gebeurtenissen zijn de trigger om gegevens uit te wisselen. Het initiatief daarvoor ligt bij de aanbieder die gegevens verstrekt over binnen zijn domein plaatsgevonden gebeurtenissen ("don't call us, we'll call you"). Deze manier van gegevens uitwisselen is fundamenteel anders dan wanneer een aanbieder een service aanbiedt en afnemers zelf het initiatief nemen om gegevens op te gaan halen. Beide vormen van gegevensuitwisseling hebben bestaansrecht, maar kennen een specifiek toepassing en kunnen ook in combinatie worden gebruikt. Gebruikers van smartphones vinden het vanzelfsprekend dat zij kunnen aangeven voor welke type gebeurtenissen zij notificaties willen ontvangen.

Notificeren is een onderdeel van eventoriëntatie. Daarbij is het belangrijk om snel te kunnen reageren op gebeurtenissen in processen. Dat kunnen levensgebeurtenissen zijn; belangrijke gebeurtenissen in het leven van een burger. Notificeren kan ook op een meer technisch niveau relevant zijn, bijvoorbeeld om anderen te attenderen op wijzigingen in gegevens. Notificeren kan ook dataminimalisatie ondersteunen, door het notificeren over gegevenswijzigingen los te zien van het ophalen van de specifieke (persoons)gegevens die relevant zijn in een specifiek proces.

Een veelgebruikt patroon bij notificeren is "publish-and-subscribe". Daarbij produceren applicaties (producers) berichten over plaatsgevonden gebeurtenissen (events). Afnemende applicaties (consumers) nemen een abonnement (subscription) op bepaalde soorten berichten. Makelaars (intermediaries) kunnen bemiddelen tussen producers en consumers om gepubliceerde events aan de juiste consumers te verstrekken. Consumers ontvangen de soorten events waarop ze zijn geabonneerd. Onderstaande figuur geeft de beschreven rolverdeling weer.



Figuur 17: Terminologie van notificeren, gebaseerd op de CloudEvents standaard

Applicaties kunnen eigendom zijn van één of meerdere organisaties en kunnen (in verschillende samenstellingen) ook gecombineerd zijn. Bij een uitwisseling kunnen één of meerdere intermediairs een rol spelen. De afspraken tussen betrokken partijen over de gegevensuitwisseling zijn sterk vergelijkbaar met de algemeen geldende afspraken bij gegevensuitwisseling.

5.5.2 Applicatie-architectuur

De functionaliteit voor abonneren wordt op dit moment veelal geboden via interactieve schermen. Daarop kan een gebruiker aangeven welke soorten events hij wel en niet willen ontvangen. Het kan gaan om eenvoudige invulschermen of om schermen waarmee een gebruiker zelf complexe selectieregels kan definiëren. Soms wordt aanvullend de mogelijkheid geboden om periodiek geautomatiseerd bepaalde filtergegevens aan te leveren. Bijvoorbeeld in de vorm van een periodiek aangeleverd bestand of via een API waarmee een afnemer gegevens aanlevert die worden gebruikt om events te filteren. Een voorbeeld hiervan is een verzameling BSN's van personen waarvoor events moeten worden verstrekt.

Het is ook mogelijk om abonnementen geautomatiseerd via API's vast te leggen, te wijzigen of verwijderen. Dit biedt nieuwe mogelijkheden, zoals het afsluiten van (heel) veel kleine abonnementen waarin in detail is beschreven in welke events een afnemer is geïnteresseerd. Bijvoorbeeld door per persoon waarvoor genotificeerd moeten worden een eigen abonnement af te sluiten.

Abonneren krijgt in deze architectuur beperkt aandacht omdat de noodzaak van standaardisatie nu minder groot is en omdat gestandaardiseerd geautomatiseerd abonneren zeer complex is. De belangrijkste reden hiervoor is dat voor een standaard veel soorten metagegevens nodig zijn om in alle situaties bruikbaar te zijn, waardoor de standaard snel (te) complex wordt. Het zelf ontwikkelen van een abonneerstandaard is niet wenselijk, maar het is wel wenselijk om internationale ontwikkelingen op dit vlak te volgen en te zijner tijd daarop aan te sluiten.

Notificeren gaat over het verzenden van events. Een event is een data record dat een plaatsgevonden gebeurtenis beschrijft. Het bevat metagegevens over context voor bijvoorbeeld het kunnen routeren van het event van producers naar consumers en het bevat inhoudelijke informatie over de plaatsgevonden gebeurtenis of een verwijzing naar waar die is te vinden. Events worden getransporteerd via, gestructureerde of binaire, berichten. Voor een event wordt gebruik gemaakt van een bepaald formaat (bijv. JSON of XML) en transportprotocol (bijv. HTTP of AMQP). Bij notificeren gaat het in het algemeen over gebeurtenissen die hebben plaatsgevonden ('feiten'), niet over gebeurtenissen in de toekomst.

Voor notificeren zijn een aantal functionaliteiten relevant: routeren, filteren en verstrekken. Routeren is het fysiek transporteren van events zodat ze vanuit producers bij consumers terecht komen. Filteren is het binnen alle gepubliceerde events, per consumer selecteren van de juiste events. Verstrekken is het beschikbaar stellen van events aan consumers via een bezorg- of ophaalmechanisme.

Bij notificeren kan de communicatie tussen applicaties synchroon of asynchroon verlopen. Bij Asynchrone communicatie wacht de verzender niet op een antwoord van de ontvanger. Asynchrone communicatie biedt voordelen qua schaalbaarheid, flexibiliteit, foutbestendigheid en efficiëntie bij notificeren. Een notificatie die niet kan worden verstrekt omdat een consumer niet actief is kan dan bijvoorbeeld door een intermediair worden bewaard en op een later moment als de consumer actief is alsnog worden verstrekt. Bij gebeurtenisgedreven werken, inclusief notificeren, verdient asynchrone communicatie daarom de voorkeur.

5.5.3 Standaarden

Van 2021 tot 2023 is in opdracht van het Ministerie van Binnenlandse Zaken het [project 'Notificatieservices'](#) uitgevoerd. Een van de doelen daarvan was om een advies te geven over een standaard voor notificeren. Er is besloten om daarvoor voort te bouwen op de internationale standaard [CloudEvents](#). Deze standaard is gekozen omdat deze het beste aansluit bij de aanwezige behoeften en mogelijkheden van Nederlandse overheidsorganisaties. De [Linked Data Event Streams](#) standaard was nog in ontwikkeling en op dat moment (nog) te weinig toepasbaar. De standaard is wel in combinatie met de CloudEvents standaard te gebruiken. CloudEvents wordt vanaf 2018 ontwikkeld binnen de Cloud Native Computing Foundation (CNCF) via een community met onder andere Cloud leveranciers zoals Microsoft, Google en Amazon. Tijdens het project Notificatieservices is door onderzoeksbureau Gartner bevestigd dat de CloudEvents-standaard voldoende toekomst vast was om als basis te gebruiken.

[AsyncAPI](#) is de de facto standaard voor het definiëren van asynchroon werkende API's en wordt vaak vergeleken met OpenAPI specification. Met behulp van AsyncAPI zijn onder andere het formaat van berichten, de uit te voeren operaties en te gebruiken protocollen gestandaardiseerd te beschrijven. Dit bevordert de kwaliteit van documenteren, ontwerpen, testen en gebruiken van asynchroon werkende API's. AsyncAPI is onderdeel van de Linux Foundation en wordt actief onderhouden door een open-sourcegemeenschap. De standaard kent een groeiend ecosysteem van tools en bibliotheken die AsyncAPI-specificaties kunnen verwerken, zoals codegeneratoren, validatietools, integraties met API-gateways en meer. AsyncAPI is te combineren met CloudEvents. CloudEvents helpt bij het definiëren van het formaat van de gebeurtenissen en AsyncAPI helpt bij het definiëren van de gebeurtenisgestuurde API's. Dat zijn API's die zijn ontworpen om te reageren op notificaties van gebeurtenissen. AsyncAPI kan worden gebruikt om de API en het bijbehorende CloudEvent-formaat te documenteren.

Naarmate er meer eventgeoriënteerd wordt gewerkt wordt het steeds belangrijker om daarbij betrokken metagegevens gestandaardiseerd vast te leggen en raadplegen. Om events goed te kunnen verwerken moet bekend zijn om wat voor soort event het gaat en wat de precieze betekenis daarvan is. Hiervoor kan gebruik worden gemaakt van catalogi met de beschrijving van eventtypes en hun relaties. Het is wenselijk dat dit type documentatie wordt gestandaardiseerd omdat consumers met steeds meer producers en soorten events te maken krijgen.

5.5.4 De CloudEvents standaard in meer detail

Omdat er in een eerder onderzoek vooral is gekozen voor het gebruik van de CloudEvents standaard, wordt deze hier in meer detail uitgelegd. CloudEvents kent een compacte 'core specificatie' voor gestandaardiseerde beschrijving van events. Aanvullend zijn er specificaties voor gebruik van de core specificatie met specifieke gegevensformaten (bijvoorbeeld JSON en XML) en transportprotocollen (bijvoorbeeld HTTP en AMQP). Standaardisatie strekt zich daarmee uit tot en met implementatieaspecten. Er zijn door de community ondersteunende producten ontwikkeld, zoals System Development Kits (SDK) voor veelgebruikte programmeertalen.

Er is een Nederlands profiel op de CloudEvents standaard ontwikkeld: [NL GOV profile for CloudEvents](#). Het bevat een set afspraken over het gebruik van de internationale CloudEvents standaard binnen de Nederlandse overheid. Het beschrijft bijvoorbeeld welke (aanvullende) afspraken gelden met betrekking tot het gebruik van bepaalde attributen. Naast het profiel zelf is er een document [Guidelines for NL-GOV profile CloudEvents](#) dat gebruik van de standaard beschrijft bij gebruik van respectievelijk HTTP, JSON, webhooks. Het profiel en de handreiking zijn in beheer bij Logius. Het is de bedoeling dat het profiel op afzienbare termijn wordt opgenomen in de lijst van open standaarden van het Forum Standaardisatie.

Het centrale begrip in de CloudEvents standaard is 'event': een data record met metadata. Het bevat contextattributen om te kunnen notificeren en inhoudelijke gegevens over een plaatsgevonden gebeurtenis (of een verwijzing daarnaar). Een viertal metagegevens moeten volgens de CloudEvents specificatie, en het daarop gebaseerde NL GOV Profile for CloudEvents, altijd aanwezig zijn binnen een event:

- Een unieke identificatie voor het event ('id')
- De bron van het event ('source')
- De versie van de gebruikte CloudEvents-specificatie ('specversion')
- Het eventtype ('type')

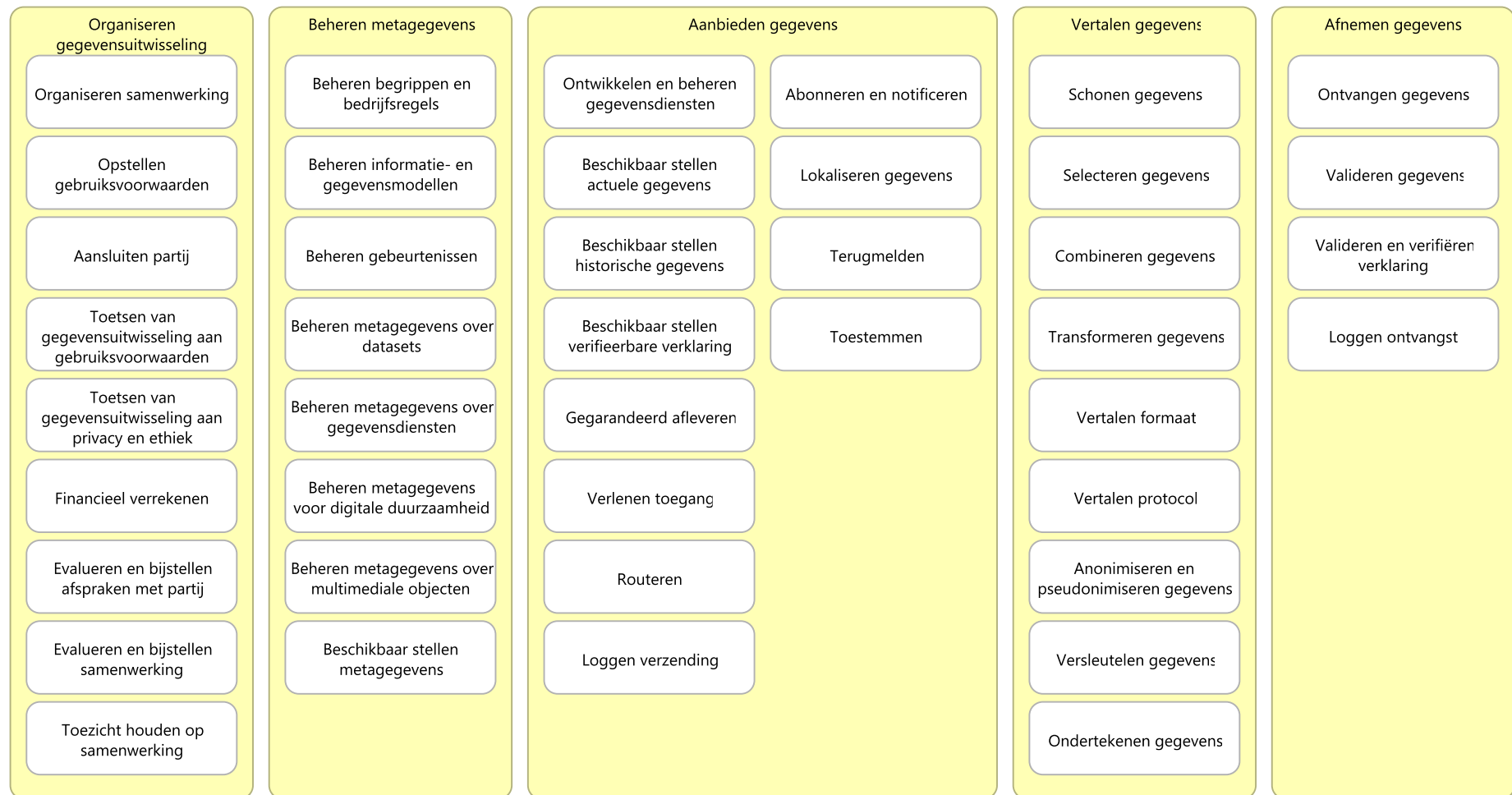
Het GOV NL profile for CloudEvents bevat afspraken over hoe deze attributen binnen de overheid moeten worden gebruikt. In een event kunnen ook aanvullende metagegevens worden opgenomen. CloudEvents heeft een aantal vaak voorkomende metagegevens gedefinieerd, maar ze zijn ook zelf te definiëren. Dit kan bijvoorbeeld op sector- of domeinniveau gebeuren.

Ook bij gebruik van het NL GOV Profile for CloudEvents is er ruimte voor betrokken organisaties om eigen keuzes te maken. Bijvoorbeeld wat betreft in events op te nemen metagegevens, het wel of niet opnemen van inhoudelijke data in berichten en gebruikte gegevensformaten, transportprotocollen en technische infrastructuur. Gegevens in een subscription kunnen zowel handmatig als geautomatiseerd worden bijgewerkt. Een samengestelde applicatie kan applicatiecomponenten combineren. Het initiatief voor verstrekking kan liggen bij intermediary of consumer.

6 Bijlagen

6.1 Functies

In deze domeinarchitectuur hebben we functies benoemd die in het algemeen relevant zijn voor gegevensuitwisseling (zie Figuur 18). De functies beschrijven vooral activiteiten op organisatieniveau (bedrijfsfuncties), maar ze zijn ook te zien als functies van informatiesystemen (applicatiefuncties). Het onderscheid is op dit niveau lastig te maken, mede doordat het afhankelijk is van de mate waarin activiteiten zijn geautomatiseerd. Organisaties zullen zelf moeten bepalen in hoeverre deze functies worden uitgevoerd door mensen en/of informatiesystemen. Daarbij kunnen ze ervoor kiezen om ze door andere organisaties te laten uitvoeren zoals aanbieders of andere soorten intermediairs of dienstverleners. Op landelijk niveau zijn er ook generieke voorzieningen beschikbaar die invulling geven aan een aantal van deze functies. De lijst van functies kan gebruikt worden om inzicht te geven in de huidige en gewenste inrichting van organisatie, processen en informatiesystemen. In de domeinarchitectuur zijn ze gekoppeld aan de capability's, architectuurprincipes, bedrijfsobjecten, rollen, voorzieningen en standaarden.



Figuur 18: Functiemodel voor gegevensuitwisseling

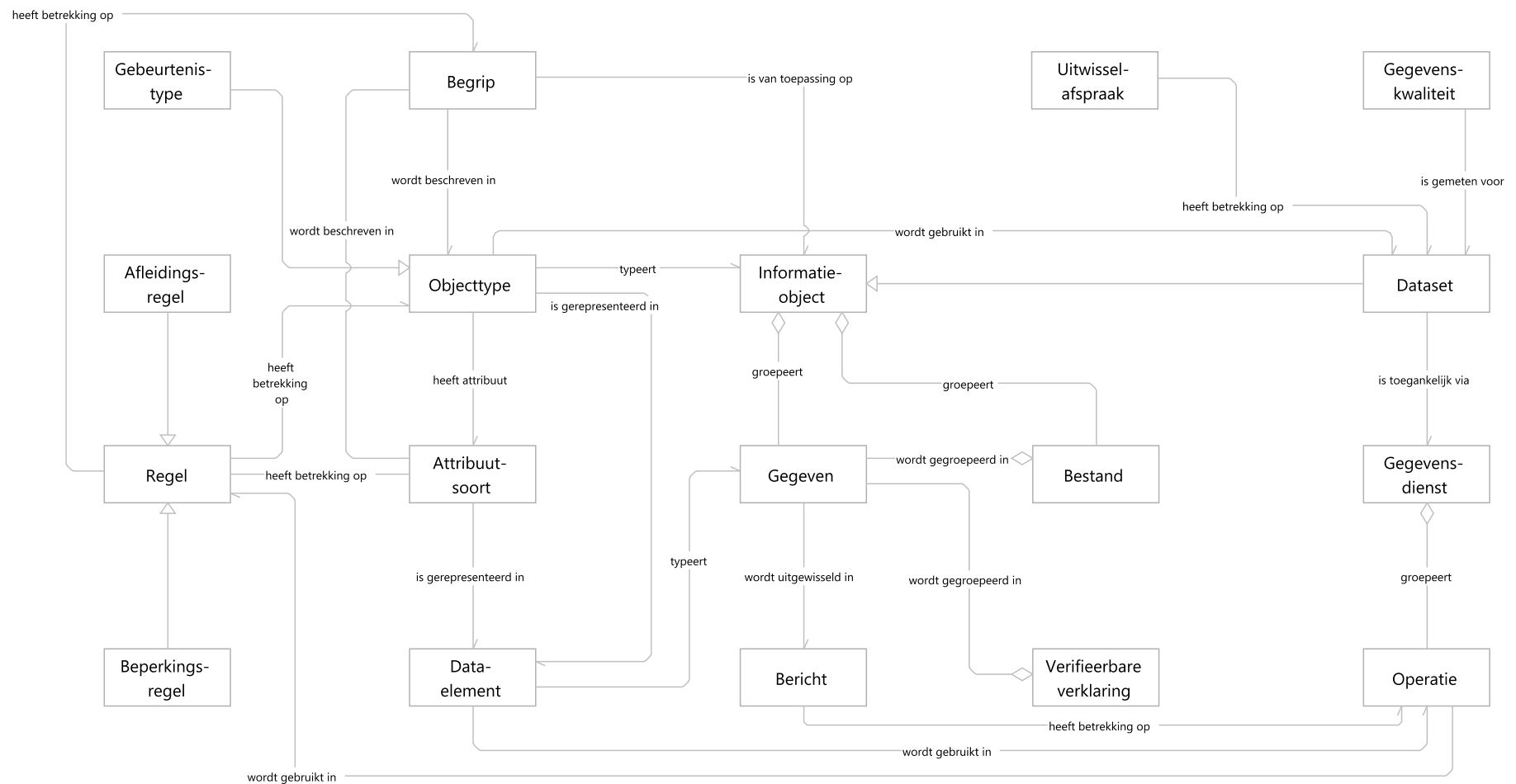
Aanbieden gegevens	Het beschikbaar stellen van gegevens.
Aansluiten partij	Het toelaten van een aanbieder, intermediair of afnemer tot de samenwerking en het toetsen of deze kan voldoen aan de bijbehorende samenwerkingsafspraken.
Abonneren en notificeren	Het bieden van de mogelijkheid voor afnemers om een abonnement te nemen op notificaties van gebeurtenissen en het creëren van een bericht over dat er een belangrijke gebeurtenis is opgetreden.
Afnemen gegevens	Het ervoor zorgen dat er gegevens afgenomen worden en daardoor beschikbaar zijn voor gebruik.
Anonimiseren en pseudonimiseren gegevens	Het verwijderen van persoonsgegevens of het vervangen van persoonsgegevens door een betekenisloos pseudoniem.
Beheren begrippen en bedrijfsregels	Het creëren, vastleggen, wijzigen en (logisch) verwijderen van begrippen en de bedrijfsregels die daar betrekking op hebben.
Beheren gebeurtenissen	Het creëren, vastleggen, wijzigen en (logisch) verwijderen van gegevens over gebeurtenissen.
Beheren informatie- en gegevensmodellen	Het creëren, vastleggen, wijzigen en (logisch) verwijderen van informatiemodellen en logische en fysieke gegevensmodellen.
Beheren metagegevens	Het creëren en beschikbaar stellen van gegevens over gegevens.
Beheren metagegevens over datasets	Het creëren, vastleggen, wijzigen en (logisch) verwijderen van metadata over datasets.
Beheren metagegevens over gegevensdiensten	Het creëren, vastleggen, wijzigen en (logisch) verwijderen van gegevens over gegevensdiensten.
Beheren metagegevens over multimediale objecten	Het creëren, vastleggen, wijzigen en (logisch) verwijderen van gegevens over multimediale bestanden zoals beelden en video's.
Beheren metagegevens voor digitale duurzaamheid	Het creëren, vastleggen, wijzigen en (logisch) verwijderen van gegevens over informatieobjecten ten behoeve van digitale duurzaamheid.
Beschikbaar stellen actuele gegevens	Het toegankelijk maken van gegevens die de actuele stand weergeven.
Beschikbaar stellen historische gegevens	Het toegankelijk maken van gegevens die een historische stand weergeven.
Beschikbaar stellen metagegevens	Het breed toegankelijk maken van allerlei vormen van metagegevens voor afnemers.
Beschikbaar stellen verifieerbare verklaring	Het toegankelijk maken van een bewering over iets of iemand op een manier die gecontroleerd kan worden of het intrekken van deze verklaring omdat deze niet meer geldig is.
Combineren gegevens	Het samenvoegen van gegevens uit verschillende datasets.

Evalueren en bijstellen afspraken	Het bepalen in welke mate partijen hebben voldaan aan de gemaakte afspraken en het aanpassen van afspraken aan nieuwe inzichten.
Evalueren en bijstellen samenwerking	Het bepalen in welke mate de samenwerking werkt en voldoende waarde oplevert voor de betrokken partijen en het aanpassen van samenwerkingsafspraken aan nieuwe inzichten.
Financieel verrekenen	Het bepalen welke bedragen partijen aan elkaar verschuldigd zijn gegeven de gegevensuitwisselingen die hebben plaatsgevonden.
Gegarandeerd afleveren	Het borgen dat bepaalde gegevens met zekerheid worden afgeleverd bij een afnemer.
Loggen ontvangst	Het vastleggen van metagegevens over de gegevens die zijn ontvangen van aanbieders.
Loggen verzending	Het vastleggen van metagegevens over de gegevens die zijn verzonden van aanbieders naar afnemers.
Lokaliseren gegevens	Het vastleggen bij welke gegevensdienst gegevens over een bepaald object of subject beschikbaar zijn en het ondersteunen van zoekvragen hierover.
Ondertekenen gegevens	Het creëren, verifiëren en valideren van een bewijs dat bepaalde gegevens afkomstig zijn van een specifieke partij en ongewijzigd zijn middels cryptografische technieken.
Ontvangen gegevens	Het ervoor zorgen dat gegevens die zijn aangeboden, beschikbaar zijn voor gebruik.
Ontwikkelen en beheren gegevensdiensten	Het creëren en wijzigen van processen en systemen die gegevensdiensten implementeren.
Opstellen gebruiksvoorwaarden	Het creëren en wijzigen van de gebruiksvoorwaarden die de beperkingen, rechten en plichten beschrijven die van toepassing zijn op datasets en gegevensdiensten.
Organiseren gegevensuitwisseling	Het organisatorisch inregelen van afspraken over hoe gegevens worden uitgewisseld.
Organiseren samenwerking	Het leggen van relaties en het creëren van samenwerkingsafspraken met partijen die een betrokkenheid hebben in de samenwerking waarbinnen gegevens worden uitgewisseld, inclusief afspraken over hoe kosten en baten worden verdeeld.
Routeren	Het sturen van berichten met daarin gegevens naar een afnemer, op basis van voorgedefinieerde criteria.
Schonen gegevens	Het verwijderen van gegevens die niet voldoen aan bepaalde kwaliteitseisen of -regels.
Selecteren gegevens	Het op basis van criteria selecteren van gegevens uit een dataset, zoals voor het ondersteunen van een zoekvraag.
Terugmelden	Het indienen, routeren, beoordelen, verwerken en terugkoppelen van een terugmelding over een gegeven.

Toestemmen	Het expliciet goedkeuren door iemand dat zijn of haar persoonsgegevens mogen worden verwerkt, of het intrekken van deze goedkeuring en het registreren en verstrekken van deze goedkeuring of intrekking.
Toetsen van gegevensuitwisseling aan gebruiksvoorwaarden	Het controleren of een gewenste gegevensuitwisseling voldoet aan de gebruiksvoorwaarden die de beperkingen, rechten en plichten beschrijven die van toepassing zijn op datasets en gegevensdiensten..
Toetsen van gegevensuitwisseling aan privacy en ethiek	Het controleren of een gewenste gegevensuitwisseling voldoet aan ethische en privacy waarden, normen en afspraken.
Toezicht houden op samenwerking	Het vanuit een onafhankelijke rol controleren of de samenwerking werkt en voldoende waarde oplevert.
Transformeren gegevens	Het omvormen van gegevens van een bepaald gegevensmodel naar een ander gegevensmodel, inclusief het verrijken van de gegevens om te voldoen aan het gegevensmodel van het doel.
Valideren gegevens	Het controleren of gegevens voldoen aan het gegevensmodel en alle van toepassing zijnde beperkingsregels.
Valideren en verifiëren verklaring	Het controleren van de authenticiteit, integriteit en geldigheid van een verifieerbare verklaring.
Verlenen toegang	Het authenticeren en autoriseren van afnemers voor toegang tot gegevensdiensten.
Versleutelen gegevens	Het inhoudelijk encrypten van gegevens zodat zij niet meer voor onbevoegden leesbaar zijn.
Vertalen formaat	Het beschikbaar stellen van gegevens in een formaat, anders dan het originele formaat.
Vertalen gegevens	Het uitvoeren van bewerkingen op gegevens.
Vertalen protocol	Het beschikbaar stellen van gegevens conform een protocol, anders dan het originele protocol.

6.2 Bedrijfsobjecten

Bedrijfsobjecten zijn dingen in de werkelijkheid waarover gegevens worden vastgelegd. Een model van bedrijfsobjecten is te zien als een hoog niveau gegevensmodel. Het geeft een overzicht van de belangrijkste begrippen die leiden tot gegevens die organisaties moeten vastleggen. Het is ook bruikbaar als checklist om verantwoordelijkheden van organisaties, mensen, processen en informatiesystemen toe te wijzen. In de domeinarchitectuur zijn ze gekoppeld aan de functies en standaarden. Het bedrijfsobjectenmodel voor gegevensuitwisseling is ook te beschouwen als een metadatamodel; het geeft een overzicht van de soorten gegevens waarover metagegevens zouden moeten worden vastgelegd. Figuur 19 geeft het bedrijfsobjectenmodel weer.



Figuur 19: Bedrijfsobjectenmodel voor gegevensuitwisseling

Afleidingsregel	Een regel die beschrijft hoe bepaalde soorten gegevens kunnen worden afgeleid uit andere soorten gegevens.
Attribuutsoort	De typering van gelijksoortige gegevens die voor een objecttype van toepassing is.. (bron: Metamodel Informatie Modellerling 1.2)
Begrip	Een eenheid van denken die wordt uitgedrukt door een woord of een groep woorden en verwijst naar de betekenis die daaraan wordt gegeven.
Beperkingsregel	Een conditie of een beperking, die van toepassing is op één of meerdere modelementen.
Bericht	Een verzameling gegevens die als geheel wordt verzonden.
Bestand	Geordende verzameling van gegevens in elektronische vorm, die door een elektronisch apparaat onder één naam kan worden behandeld en aangesproken. (bron: MDTO)
Data-element	Eenheid van gegevens die in een bepaalde context als ondeelbaar wordt beschouwd. (bron: ISO/IEC 11179-30:2023)
Dataset	Een verzameling gegevens die is gepubliceerd of samengesteld door één enkele partij. (bron: DCAT 2.0)
Gebeurtenistype	De typering van een groep gebeurtenissen die binnen een domein relevant zijn en als gelijksoortig worden beschouwd.
Gegeven	Een vastgelegde waarneming of bewering over een getypeerde eigenschap van een object.
Gegevensdienst	Een verzameling operaties die toegang bieden tot een of meer datasets of gegevensverwerkingsfuncties. (bron: DCAT 2.0)
Gegevenskwaliteit	De mate waarin een geheel van eigenschappen en kenmerken van één of meer gegevens voldoet aan eisen.
Informatieobject	Een op zichzelf staand geheel van gegevens met een eigen identiteit. (bron: MDTO)
Objecttype	De typering van een groep objecten die binnen een domein relevant zijn en als gelijksoortig worden beschouwd. (bron: Metamodel Informatie Modellerling 1.2)
Operatie	Een geautomatiseerde functie die gegevens verwerkt.
Uitwisselafsprak	Een afspraak tussen partijen over wie, wanneer, welke gegevens onder welke condities uitwisselt.
Verifieerbare verklaring	Een verzameling van attributen, vergezeld van een bewijs dat deze afkomstig zijn van een specifieke verklarende partij.

6.3 Rollen

Rollen zijn een clustering van taken, bevoegheden en verantwoordelijkheden. De architectuur benoemt de belangrijkste rollen in de context van gegevensuitwisseling en verbindt ze aan de functies om de belangrijkste verantwoordelijkheden duidelijk te maken.

Aanbieder	Een rol die verantwoordelijk is voor het aanbieden van gegevens van bronhouders op een manier die aansluit bij de behoeften en het gebruik van afnemers.
Afnehmer	Een rol die ervoor zorgt dat aangeboden gegevens beschikbaar zijn voor gebruik.
Bronhouder	Een rol die verantwoordelijk is voor het inwinnen, beheren en het verbeteren van de kwaliteit van gegevens.
Clearing house	Een rol die ervoor zorgt dat aangetoond kan worden dat gegevensuitwisselingen hebben plaatsgevonden en clearing en settlement hiervan kan uitvoeren.
Domeinregisseur	Een rol die verantwoordelijk is voor het inrichten en besturen van een afsprakenstelsel voor gegevensuitwisselingen in een domein.
Gebruiker	Een natuurlijk persoon die gegevens en/of functionaliteit gebruikt voor het uitvoeren van werkzaamheden.
Intermediair	Een rol die toegevoegde waarde levert in de keten tussen aanbieders en afnemers.
Toetsingscommissie	Een rol die een onafhankelijk oordeel kan vellen over de wenselijkheid van het uitwisselen van gegevens vanuit het perspectief van privacy en ethiek.

6.4 Huidige voorzieningen

De Generieke Digitale Infrastructuur bestaat uit een aantal generieke voorzieningen, die breed gebruikt kunnen worden door overheidsorganisaties. Daarnaast zijn er op het gebied van gegevensuitwisseling ook een aantal andere generieke voorzieningen die breder binnen de overheid gebruikt kunnen worden. In deze paragraaf wordt een overzicht gegeven van de belangrijkste voorzieningen die we onder de aandacht willen brengen. Deze voorzieningen zijn gerelateerd aan de functies om inzicht te geven in hun functionaliteit. Ze zijn ook voorzien van eigenschappen die beschrijven wie verantwoordelijk is voor het beheer en waar meer informatie over de voorziening kan worden gevonden.

BSNk	Een voorziening die polymorfe identiteiten en pseudoniemen kan genereren, versleutelen en ontsleutelen.
CPA register	Het CPA Register slaat gegevens op over de organisatie, de gebruiker, service, certificaten, en digikoppeling. Dit om het de gebruikers makkelijk te maken om op basis van opgeslagen gegevens CPA's te maken.
Centraal Aansluitpunt	Het Centraal Aansluitpunt (CA) is het knooppunt voor berichtenverkeer tussen systemen voor overheidsorganisaties.
Centrale OIN Raadpleegvoorziening	De Centrale OIN Raadpleegvoorziening (COR) is de voorziening die de uitgegeven openbare Organisatie-identificatienummers (OIN) beheert.
Digilevering	Digilevering levert berichten over belangrijke gebeurtenissen.

Digimelding	Met Digimelding kunnen mogelijke onjuistheden in de gegevens van een (basis)registratie uniform, betrouwbaar en efficiënt worden teruggemeld aan de bronhouder van deze registratie.
Digipoort	Digipoort is de voorziening waar berichtenverkeer van en naar de overheid afgehandeld wordt.
Nationaal Geo Register	Een register en portaal met door de Nederlandse overheid beschikbaar gestelde geografische gegevens.
RINIS voorzieningen	RINIS levert diensten voor de uitwisseling van gegevens tussen overheidsorganisaties
Stelselcatalogus	De Stelselcatalogus geeft inzicht in welke gegevens er in welke registraties worden bijgehouden, welke betekenis deze gegevens hebben, en hoe gegevens uit de verschillende registraties zich tot elkaar verhouden.
data.overheid.nl	Een register en portaal met door de Nederlandse overheid beschikbaar gestelde gegevens.
developer.overheid.nl	Een register en portaal met door de Nederlandse overheid ontwikkelde API's.

6.5 Standaarden

In de domeinarchitectuur is een lijst van standaarden opgenomen die relevant zijn in het kader van gegevensuitwisseling. De basis voor deze lijst zijn de lijsten van Forum Standaardisatie. We hebben ervoor gekozen om alleen de generieke standaarden op te nemen en niet de toepassings specifieke standaarden. Deze standaarden zijn aangevuld met andere standaarden die breder worden gebruikt of relevant zijn. Deze aanvullende standaarden zijn te beschouwen als aanbeveling vanuit deze architectuur. De aanbeveling is vooral om deze standaarden te bestuderen en hun inzet te overwegen bij het inrichten of aanpassen van gegevensuitwisseling. De standaarden zijn voorzien van een aantal standaard eigenschappen zoals de beheerorganisatie en een URL naar meer informatie. Ze zijn ook gekoppeld aan functies en bedrijfsobjecten zodat hun toepassingsgebied duidelijk is. Bij de standaarden van Forum Standaardisatie zijn ook de status en het functioneel toepassingsgebied overgenomen.

AMQP	Het Advanced Message Queuing Protocol (AMQP) is gericht op het betrouwbaar uitwisselen van berichten.
API Features	De OGC API features standaard is bedoeld voor het creëren, wijzigen en bevragen van geografische gegevens op het web.
API Tiles	De OGC API Tiles standaard ondersteunt het bevragen van geografische gegevens als tiles.
API Records	API records is een specificatie voor het kunnen creëren, wijzigen en bevragen van metadata over geografische gegevens.
ArchiMate	ArchiMate is een taal voor het modelleren van enterprise-architectuur.
AsyncAPI	AsyncAPI is een taal voor het specificeren van asynchrone API's.
CSV	Comma-separated values (CSV) bestanden bestaan uit regels met gegevens waarbij tussen gegeven een komma (of ander scheidingsteken) wordt geplaatst.
DCAT	Data Catalog Vocabulary (DCAT) is een metadatastandaard en is ontworpen om interoperabiliteit tussen gegevenscatalogi, gepubliceerd op het internet, te vergemakkelijken.
DQV	De Data Quality Vocabulary (DQV) standaard is bedoeld om informatie over de kwaliteit van gegevens te publiceren.
Digikoppeling	Digikoppeling maakt veilige gegevensuitwisseling tussen overheden mogelijk. De standaard beschrijft afspraken om gegevens juist te adresseren, leesbaar en uitwisselbaar te maken en veilig en betrouwbaar te verzenden. De standaard bestaat uit een viertal koppelvlakspecificaties voor gestructureerd gegevensuitwisseling met en tussen overheidsorganisaties.
Digikoppeling Koppelvlakstandaard Grote Berichten	Digikoppeling Koppelvlakstandaard Grote Berichten standaardiseert hoe grote bestanden worden uitgewisseld.
Digikoppeling Koppelvlakstandaard REST-API	Digikoppeling Koppelvlakstandaard REST-API standaardiseert hoe gegevens synchroon worden uitgewisseld met resources op basis van RESTful API's.
Digikoppeling Koppelvlakstandaard WUS	Digikoppeling Koppelvlakstandaard WUS standaardiseert hoe gegevens worden uitgewisseld op basis van de SOAP standaard.

Digikoppeling Koppelvlakstandaard ebMS2	Digikoppeling Koppelvlakstandaard ebMS2 standaardiseert hoe gegevens asynchroon en betrouwbaar worden uitgewisseld op basis van de ebMS standaard.
FSC	De Federated Service Connectivity (FSC) standaard beschrijft hoe organisaties kunnen interacteren op een uniforme en geautomatiseerde wijze.
FTP	Het File Transfer Protocol (FTP) is een protocol dat uitwisseling van bestanden over het internet tussen computers vergemakkelijkt. Het standaardiseert een aantal handelingen die tussen besturingssystemen vaak verschillen.
GML	De Geography Markup Language (GML) is een XML-gebaseerde vorm voor het uitdrukken van schema's voor geografische gegevens.
Geo-standaarden	De Geo-standaarden maken het mogelijk om op een eenduidige manier gegevens met een geografische component uit te wisselen. Ze bestaan uit: NL ISO 19115, NL ISO 19119, NL WFS, NL WMS, ISO 19136:2007, NEN 3610:2011 en GeoPackage 1.2.
GeoJSON	GeoJSON is een op JSON gebaseerd formaat voor geografische gegevens.
GeoPackage	GeoPackage is een bestandsformaat voor het vastleggen van geografische gegevens.
GraphQL	GraphQL is een protocol en vraagtaal voor het bevragen van gegevens.
IIIF	Het International Image Interoperability (IIIF) framework beschrijft standaarden voor het ontsluiten van beeldmateriaal.
IMX Model Mapping	IMX Model Mapping beschrijft een vertaling van één of meer bronnen naar een doel en is bedoeld om gebruikt te worden voor een IMX orchestratie.
ISO 15836	ISO 15836-1:2017 beschrijft de Dublin Core metadata-elementen, die de basis vormen voor metadata over informatie-objecten.
ISO 704	ISO 704:2022 beschrijft de basisprincipes en methoden voor het voorbereiden en samenstellen van begrippenkaders.
JAdES	JAdES is een standaard voor het zetten van elektronische handtekeningen voor elektronische berichten in het JSON formaat.
JCDR	Juriconnect Decentrale Regelgeving (JCDR) is een afgesproken tekstvolgorde (syntax) voor verwijzingen naar decentrale regelgeving in de voorziening Decentrale Regelgeving en Officiële Publicaties (DROP).
JSON	JavaScript Object Notation (JSON) is een deelverzameling van de programmeertaal JavaScript. Het is een formaat om net zoals XML gegevens op te slaan en te versturen.
JSON Schema	JSON Schema wordt gebruikt voor het beschrijven van op JSON gebaseerde koppelvlakken voor gegevensuitwisseling
JWE	JSON Web Encryption (JWE) is een standaard voor het versleutelen van gegevens.
JWT	JSON Web Token (JWT) is een compacte, URL-veilige manier om verklaringen uit te wisselen tussen twee partijen.

MDTO	Metagegevens voor duurzaam toegankelijke overheidsinformatie (MDTO) is een norm voor het vastleggen en uitwisselen van eenduidige metagegevens om de duurzame toegankelijkheid van overheidsinformatie mogelijk te maken.
MIM	Het Metamodel voor Informatiemodellering (MIM) dient als gemeenschappelijk vertrekpunt voor het opstellen van informatiemodellen, zodat informatiemodellen en de daarop gebaseerde standaarden voor gegevensuitwisseling meer compatibel worden.
NEN 3610	Het Basismodel geo-informatie (NEN3610) bevat de termen, definities, relaties en algemene regels voor de uitwisseling van informatie over ruimtelijke objecten.
NEN-ISO 23081	NEN-ISO 23081-1 behandelt de principes die metagegevens voor informatie- en archiefbeheer onderbouwen en regelen.
NEN-ISO/IEC 18013-5	ISO/IEC 18013-5 is een internationale standaard die betrekking heeft op identiteitsdocumenten voor mobiliteitsdoeleinden, met de nadruk op smartphone-toepassingen.
NL GOV profile for CloudEvents	NL GOV profile for CloudEvents is een set Nederlandse afspraken over het gebruik van de internationale standaard CloudEvents. Het beschrijft hoe een plaatsgevonden gebeurtenis gerapporteerd en uitgewisseld kan worden.
NL ISO 19115	Nederlands metadatataprofiel op ISO 19115 geografie. Het Nederlandse metadatataprofiel voor geografie beschrijft hoe je de metadata van geo-datasets opstelt.
NL ISO 19119	Nederlands metadatataprofiel op ISO 19119 services. Dit metadatataprofiel beschrijft de verplichte metadata elementen van een service op een dataset of dataset serie.
NL WFS	Nederlands WFS profiel 1.1 op ISO 19142 voor Web Feature Services 2.0. Een WFS ondersteunt minimaal het opvragen van geo-informatie. Aanvullend biedt een WFS mogelijkheden om geo-informatie in de database direct te bewerken.
NL WMS	Nederlands profiel WMS op ISO 19128 versie 1.1. WMS maakt het mogelijk om een rasterbeelden op te vragen.
NL-SBB	De Nederlandse Standaard voor het Beschrijven van Begrippen (NL-SBB) geeft aan hoe begrippen in een begrippenlijst, taxonomie of thesaurus eenduidig worden beschreven.
OCL	De Object Constraint Language (OCL) is een taal voor het specificeren van beperkingsregels, ontwikkeld in de context van UML.
ODF	Open Document Format (ODF) maakt het mogelijk om reviseerbare documenten uit te wisselen die voor bewerking niet afhankelijk zijn van een bepaalde leverancier of applicatie. ODF is een duurzaam toegankelijk documentformat.
ODRL	De Open Digital Rights Language (ODRL) is een taal voor het vastleggen van afspraken over gebruik van gegevens en diensten.
OData	Het Open Data-protocol (OData) is een best practice voor het structureren en bevragen van REST APIs. OData maakt het makkelijker om

	interoperabele REST-implementaties te bouwen, waardoor data die via API's wordt uitgewisseld op een uniforme wijze weergegeven kan worden.
OWL	Web Ontology Language (OWL) kan worden gebruikt voor het vastleggen van kennis voor ontsluiting door computers, om de samenhang van die kennis te controleren of impliciete kennis expliciet te maken.
OpenAPI specification	De OpenAPI Specification standaardiseert de beschrijving van API's, inclusief de gegevens die in deze API's worden gebruikt als invoer en uitvoer.
OpenID for Verifiable Credentials	Deze standaard maakt het mogelijk om verifieerbare verklaringen te gebruiken in de context van OpenID Connect.
PDF	Portable Document Format (PDF) is een standaard die de opmaak van documenten beschrijft, waardoor ze er op alle apparaten en in alle omgevingen hetzelfde uitzien.
PDF/UA	Een PDF/UA document is een PDF document dat voldoet aan aanvullende eisen van digitale toegankelijkheid.
PROV	PROV is een verzameling standaarden voor het beschrijven van de provenance van gegevens.
RDF	Resource Description Framework (RDF) is een standaard voor het uitdrukken van gegevens als linked data, gebruik makend van een drie-eenheid (triple) die bestaat uit een subject, een predicaat en een object.
RDFS	Resource Description Framework Schema (RDFS) biedt een standaard taal waarmee de structuur van gegevens in termen van klassen, eigenschappen en datatypen kan worden beschreven.
REST-API Design Rules	REST-API design rules is een lijst afspraken die ontwikkelaars volgen tijdens het bouwen van een REST-API voor de publieke sector. Door de regels te hanteren wordt de API voorspelbaar.
RIF	Rule Interchange Format (RIF) is een standaard voor het uitwisselen van regels over gegevens.
RuleSpeak	RuleSpeak is een taal voor het beschrijven van bedrijfsregels op een manier die dicht tegen natuurlijke taal aanligt.
SBVR	Semantics Of Business Vocabulary And Business Rules (SBVR) is een taal voor het beschrijven van bedrijfsregels.
SD-JWT	Selective Disclosure JWT (SD-JWT) is een standaard die het mogelijk maakt om een subset van verklaringen in een getekende JWT te delen.
SD-JWT VC	SD-JWT-based Verifiable Credentials (SD-JWT VC) is een specificatie die het mogelijk maakt om verifieerbare verklaringen op basis van de SD-JWT standaard te beschrijven en deze ook in JWS JSON te serialiseren.
SHACL	Shapes Constraint Language (SHACL) is een standaard om gegevensstructuren die in de vorm van Linked Data zijn vastgelegd te beschrijven en te valideren.
SKOS	Simple Knowledge Organization System (SKOS) is een gegevensmodel om duidelijke lijsten met termen en begrippen op te stellen. Met deze termenlijsten kan informatie uit verschillende databases aan elkaar worden gekoppeld. SKOS maakt de relaties tussen begrippen inzichtelijk

	voor het vergelijken en interpreteren van data uit verschillende systemen. Zo krijgt informatie meer waarde.
SOAP	De Simple Object Access Protocol (SOAP) specificatie beschrijft een berichtformaat gebaseerd op XML.
SPARQL	SPARQL Protocol And RDF Query Language (SPARQL) is een protocol en vraagtaal voor het bevragen van Linked Data databases.
SQL	Structured Query Language (SQL) is een taal voor het opslaan, bewerken en ophalen van gegevens in relationele databases.
Schematron	Schematron is een taal voor het specificeren van beperkingsregels op XML documenten.
StUF	Standaard Uitwisseling Formaat (StUF) is een set basisafspraken over het uitwisselen van gegevens tussen applicaties in het gemeentelijke veld. StUF beschrijft de generieke toepassing van die berichten, niet de specifieke gegevens erin. Als overheidsorganisaties basisregistraties (informatie over personen, adressen of bijvoorbeeld gebouwen) uitwisselen, doen ze dat via standaarden die gebaseerd zijn op StUF.
TOOI	Thesauri en Ontologieën voor Overheidsinformatie (TOOI) is een kennismodel dat is gericht op het definiëren van een gemeenschappelijke taal voor het beschrijven van gegevens en metagegevens zodat overheidsinformatie beter vindbaar, toegankelijk, interoperabel en herbruikbaar wordt.
Verifiable Credentials	Deze specificatie biedt een mechanisme om beweringen over iets of iemand uit te drukken op een manier die cryptografisch veilig is, de privacy respecteert en machinaal verifieerbaar is.
WSDL	Web Service Description Language (WSDL) is een XML taal voor het beschrijven van web services en hoe ze te benaderen.
WS-Security	Web Services Security (WS-Security) is een uitbreiding op de SOAP standaard, specifiek gericht op beveiliging van Web Services.
XACML	eXtensible Access Control Markup Language (XACML) is een op XML gebaseerde taal voor het uitdrukken van autorisatieregels.
XMI	XML Metadata Interchange (XMI) is er om de uitwisseling van metadata tussen UML-tools (Unified Modeling Language) en MOF-gebaseerde (Meta-Object Facility) metadata repositories mogelijk te maken.
XML	Extensible Markup Language (XML) is een standaard voor vastleggen en uitwisselen van gestructureerde gegevens, specifiek gericht op verwerking door machines.
XML Encryption	XML Encryption specificeert hoe de inhoud van een XML document versleuteld kan worden.
XML Schema	XML Schema (XSD) wordt gebruikt voor het beschrijven van op XML gebaseerde koppelvlakken voor gegevensuitwisseling
XML Signature	XML Signature definieert een standaard XML syntax voor digitale handtekeningen.
XSLT	eXtensible Stylesheet Language (XSLT) is een taal voor het opmaken en omzetten van gegevens in XML formaat.

6.6 Begrippen

Deze begrippenlijst bevat een beschrijving van de belangrijkste begrippen zoals gehanteerd in de domeinarchitectuur. Het neemt een voorschot op de nieuwe set van begrippen zoals deze worden gedefinieerd in de NORA begrippenlijst. Die begrippenlijst is echter nog in ontwikkeling en kan nog wijzigen. De intentie is om in de toekomst vooral te verwijzen naar de nieuwe NORA begrippenlijst zodra deze beschikbaar is.

afleidingsregel	Een regel die beschrijft hoe bepaalde soorten gegevens kunnen worden afgeleid uit andere soorten gegevens.
attribuutsoort	De typering van gelijksoortige gegevens die voor een objecttype van toepassing is.
attribuutwaarde	De waarde die een attribuut aanneemt.
begrip	Een eenheid van denken die wordt uitgedrukt door een woord of een groep woorden en verwijst naar de betekenis die daaraan wordt gegeven.
begrippenkader	Een verzameling van begrippen die in een bepaalde context relevant zijn.
beperkingsregel	Een regel die een beperking beschrijft die van toepassing is op één of meerdere soorten gegevens.
bericht	Een verzameling gegevens die als geheel wordt verzonden.
bestand	Geordende verzameling van gegevens in elektronische vorm, die door een elektronisch apparaat onder één naam kan worden behandeld en aangesproken.
bron	Een registratie die is aangewezen als de plaats waarin gegevens worden beheerd.
bronhouder	De verantwoordelijke voor de inhoud en kwaliteit van een registratie.
data	Een verzameling tekens in de vorm van termen of symbolen.
data-aanbieder	Een rol die data beschikbaar maakt voor afnemers door dataservices te ontwikkelen op de bron(nen) van bronhouder(s).
data-afnemer	De rol die data van data-aanbieders beschikbaar maakt voor gebruik ten behoeve van eigen doelstellingen in een eigen context.
data-element	Eenheid van gegevens die in een bepaalde context als ondeelbaar wordt beschouwd.
datacatalogus	Een samengestelde verzameling metadata over datasets en dataservices.
dataset	Een verzameling gegevens die is gepubliceerd of samengesteld door één enkele partij.
domein	Een bepaald gebied in de werkelijkheid waar we over willen spreken.
duurzame toegankelijkheid	De mate waarin gegevens vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig blijven voor iedereen die daar recht op heeft en voor zolang noodzakelijk is.
feit	Een gebeurtenis of omstandigheid waarvan de werkelijkheid vaststaat, doordat het ofwel zintuiglijk waargenomen ofwel instrumenteel gemeten kan worden.
formele historie	De veranderingen van gegevens in een registratie

gebeurtenis	Iets dat gebeurt of gebeurd is.
gebeurtenistype	De typering van een groep gebeurtenissen die binnen een domein relevant zijn en als gelijksoortig worden beschouwd.
gegeven	Een vastgelegde waarneming of bewering over een getypeerde eigenschap van een object.
gegevensbehoefte	De behoefte aan een bepaalde verzameling gegevens.
gegevensdienst	Een verzameling operaties die toegang bieden tot een of meer datasets of gegevensverwerkingsfuncties.
gegevenskwaliteit	De mate waarin een geheel van eigenschappen en kenmerken van één of meer gegevens voldoet aan eisen.
gegevensmodel	Een model dat een beschrijving geeft van eenheden gegevens voor een bepaald domein.
geldigheidsperiode	De periode waarin een object een bepaalde toestand had.
grondslag	De basis of datgene waarop iets gebaseerd is.
informatie	Kennis die de onzekerheid over het optreden van een specifieke gebeurtenis uit een gegeven reeks mogelijke gebeurtenissen vermindert of wegneemt
informatiebehoefte	De behoefte aan bepaalde informatie.
informatiemodel	Een model dat een beschrijving geeft van eenheden van informatie of gegevens voor een bepaald domein.
informatieobject	Een op zichzelf staand geheel van gegevens met een eigen identiteit.
informatieproduct	Een dataset gericht op specifieke gebruiksdoelen.
kennis	Verzameling van feiten, gebeurtenissen, overtuigingen en regels, georganiseerd voor systematisch gebruik
kwaliteitsattribuut	Een aspect van een kwaliteitsdimensie.
kwaliteitsdimensie	Een aspect van kwaliteit waaraan gebruikers van gegevens waarde hechten.
kwaliteitsraamwerk	Een verzameling kwaliteitsdimensies en kwaliteitsattributen.
locatie	Een positie relatief ten opzichte van de aarde.
materiële historie	De veranderingen van een object.
metadata	Gegevens die andere gegevens definiëren en beschrijven.
model	Een abstractie van enige aspecten van de werkelijkheid.
modelelement	Een element of component in een model.
object	Een onderscheidbaar iets in het beschouwde domein.
objecttype	De typering van een groep objecten die binnen een domein relevant zijn en als gelijksoortig worden beschouwd.
operatie	Een geautomatiseerde functie die gegevens verwerkt.
regel	Een voorschrift.

registratie	Een plaats waar gegevens worden verzameld en vastgelegd.
registratieperiode	De periode waarin gegevens in een registratie aanwezig en actueel zijn.
verstrekkingpunt	Een gegevensdienst die is aangewezen om gebruikt te worden om bepaalde soorten gegevens te verkrijgen.

6.7 Relatie van architectuurprincipes met ADO en NORA

Deze bijlage relateert de architectuurprincipes zoals beschreven in deze domeinarchitectuur aan de uitgangspunten in de Architectuur Digitale Overheid 2030 en de principes en implicaties in NORA. Het levert daarmee een verdere onderbouwing en verdieping van de architectuurprincipes.

Architectuurprincipe	Uitgangspunt in Architectuur Digitale Overheid 2030	Principe of implicatie in NORA
1.1. Gegevens die kunnen worden gedeeld zijn vindbaar, toegankelijk, interoperabel en herbruikbaar	<ul style="list-style-type: none">• Data wordt beschikbaar gemaakt met toepassing van de "FAIR" principes [...]• Overheids-api's zijn open te gebruiken, ook voor niet-overheidsorganisaties bruikbaar, tenzij wettelijke of privacyeisen dat verhinderen.• Voor het opstellen van informatiemodellen wordt gebruik gemaakt van het Metamodel Informatie Modelleren (MIM).	<ul style="list-style-type: none">• Pas de FAIR dataprincipes toe• Zorg dat overheidsinformatie eenvoudig te raadplegen is• Maak zoveel mogelijk data beschikbaar als open data• Weet welke (bron)gegevens in huis zijn• Bevorder hergebruik van gegevens• Beschrijf informatieobjecten in een model• Gebruik open standaarden voor modellering• Geef de afnemer inzicht in rechten en voorwaarden en plichten• Stel betrokkenen op de hoogte van het doel waarvoor gegevens verzameld worden• Zorg voor open specificaties
1.2. Gegevensuitwisseling is gebaseerd op open standaarden		<ul style="list-style-type: none">• Pas open standaarden toe• Standaardiseer waar mogelijk• Gebruik de standaard met het meest specifieke werkingsgebied• Zorg voor open specificaties• Gebruik een actueel register met standaarden
1.3 De kwaliteit van gegevens is afgestemd op het gebruik		<ul style="list-style-type: none">• Ken je afnemers en stem diensten hierop af• Neem gegevens als fundament• Stel van ieder gegeven de kwaliteit vast• Controleer de verwerking van gegevens• Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces

		<ul style="list-style-type: none"> • Stel onweerlegbaarheid vast
1.4. Gegevensdiensten zijn afgestemd op de behoeften van afnemers		<ul style="list-style-type: none"> • Ken je afnemers en stem diensten hierop af
1.5. De aangewezen bron van de gegevens is leidend	<ul style="list-style-type: none"> • Welke data [...] binnen de overheid uit welke bron komt is duidelijk vastgelegd en afnemers zijn verplicht te zorgen dat data actueel blijven en conform deze bron zijn 	<ul style="list-style-type: none"> • Weet welke (bron)gegevens in huis zijn • Stel voor ieder gegeven de unieke bron vast • Stel de juridische aansprakelijkheid per gegevensobject vast • Verwijs naar de bron • Gegevens eenmalig uitgevraagd, uniek opgeslagen, meervoudig gebruikt • Geef de voorkeur aan halen i.p.v. brengen van gegevens
1.6. Burgers en organisaties hebben regie over hun eigen gegevens	<ul style="list-style-type: none"> • Er is een grondslag nodig om persoonsgegevens te mogen verwerken. Bij de overheid is dit vrijwel altijd een grondslag vanuit een wet. • Burgers en bedrijven kunnen eenvoudig zien welke data de overheid over hen heeft (inzagerecht). • Burgers, bedrijven en overheden kunnen vermeende onjuistheden in data eenvoudig laten corrigeren (correctierecht). • Mensen hebben in bepaalde mate het recht om 'vergeten' te worden. [...] 	<ul style="list-style-type: none"> • Pas doelbinding toe • Stel bij het verzamelen en opvragen van persoonsgegevens de betrokkenen op de hoogte van het doel waarvoor de gegevens worden verzameld en van de rechten die zij mogen uitoefenen
1.7. Persoonsgegevens zijn beschermd bij het uitwisselen van gegevens	<ul style="list-style-type: none"> • Er is een grondslag nodig om persoonsgegevens te mogen verwerken. Bij de overheid is dit vrijwel altijd een grondslag vanuit een wet. • Overheden mogen alleen persoonsgegevens verwerken als het niet anders kan. Dus: als zij zonder deze gegevens hun doel niet kunt bereiken. 	<ul style="list-style-type: none"> • Pas doelbinding toe • Ontwerp diensten met oog voor doelbinding en grondslag • Borg de vertrouwelijkheid van gegevens in maatregelen • Minimaliseer het gebruik van gegevens
1.8. Uitwisselingen van gegevens wordt gelogd als deze later aantoonbaar moet zijn		<ul style="list-style-type: none"> • Richt een sterke logging en audit-trail in • Leg auditlogs vast bij de bronregistratie van het gegeven
2.1. Gegevensuitwisseling is federatief georganiseerd	<ul style="list-style-type: none"> • Voor het delen van data maken we gebruik van de principes van het Federatief Datastelsel. [...] 	

	<ul style="list-style-type: none"> • Per domein / sector dienen afspraken gemaakt te worden over standaarden van berichten (informatiemodel, semantiek, e.d.). 	
2.2. Voorwaarden en afspraken zijn expliciet en inzichtelijk		<ul style="list-style-type: none"> • Maak heldere afspraken over aanbieden en afnemen van diensten • Geef de afnemer inzage in rechten en voorwaarden en plichten • Leg de grondslag en het doel van de gegevensverwerking vast • Neem oorspronkelijke grondslag mee bij hergebruik diensten • Bepaal taken en verantwoordelijkheden van de gegevensverwerking
3.1. Gemeenschappelijke begripsvorming is het startpunt	<ul style="list-style-type: none"> • We harmoniseren definities en betekenis (semantiek) van gegevens. 	
3.2. Metagegevens zijn begrijpelijk voor mensen	<ul style="list-style-type: none"> • [...] Deze dient de daartoe benodigde functionele documentatie aan te bieden. 	
3.3. Gegevens worden contextrijk vastgelegd	<ul style="list-style-type: none"> • Welke data [...] binnen de overheid uit welke bron komt is duidelijk vastgelegd [...] 	<ul style="list-style-type: none"> • Leg de doelbinding vast in de metadata van het gegevensobject • Leg de context van een informatieobject vast in metadata • Maak gegevens herleidbaar tot de bron (herkomst) • Leg de grondslag en het doel van de gegevensverwerking vast
3.4. Metagegevens zijn aan elkaar verbonden		
3.5. Metagegevens zijn beschikbaar als Linked Data	<ul style="list-style-type: none"> • Via het principe van linked data kunnen verbanden tussen dataobjecten in meerdere kernregistraties worden vastgelegd. 	
3.6. De kwaliteit van gegevens is beschreven conform het landelijke raamwerk gegevenskwaliteit		

4.1. Gegevens worden geleverd vanuit herbruikbare gegevensdiensten	<ul style="list-style-type: none"> • De architectuur Digitale Overheid is gebaseerd op service oriëntatie. Organisaties leveren burgers, bedrijven en elkaar services, die in toenemende mate worden aangeboden in de vorm van API's. • Overheidsorganisaties standaardiseren op gelijkvormige en breed inzetbare API's voor het leggen van verbindingen tussen applicaties [...]. • Specificaties van overheids-API's worden openbaar gepubliceerd (conform de in de API standaard vastgelegde kaders, zie bouwsteen). 	<ul style="list-style-type: none"> • Wissel gegevens tussen (web)applicaties uit met API's • Maak diensten herbruikbaar • Bevorder hergebruik van gegevens
4.2. Registraties bieden historische gegevens aan		<ul style="list-style-type: none"> • Leg de doelbinding vast in de metadata van het gegevensobject
4.3. Aanbieders kunnen notificeren over belangrijke gebeurtenissen	<ul style="list-style-type: none"> • Overheidsorganisaties ontwikkelen volledig digitale processen aan de hand van levensgebeurtenissen • Bij een wijziging in opgeslagen gegevens kunnen andere overheidsorganisaties geautomatiseerd een signaal over de wijziging ontvangen. 	
5.1. Informatieproducten zijn herleidbaar naar de onderliggende gegevens en regels	<ul style="list-style-type: none"> • Welke data [...] binnen de overheid uit welke bron komt is duidelijk vastgelegd [...] 	<ul style="list-style-type: none"> • Maak gegevens herleidbaar tot de bron (herkomst)
6.1. Gegevens worden zo vroeg mogelijk gevalideerd		<ul style="list-style-type: none"> • Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces

Tabel 7: Relatie van architectuurprincipes met ADO en NORA

6.8 Betrokkenen

De volgende mensen waren onderdeel van de architectuurwerkgroep gegevensuitwisseling en hebben bijgedragen aan de totstandkoming van dit document.

- Harrie Schuurs, sponsor (Belastingdienst)
- Arnoud Quanjier, voorzitter (VNG)
- Danny Greefhorst, secretaris en redacteur (BZK/Bureau MIDO)
- Hans Markestein (Toeslagen)
- Dennis Passage (Logius)
- Hans Sinnige (RINIS)
- Han Wijlens (Kadaster)
- Bas Wernsen (JenV)
- Ad Gerrits (VNG)
- Miriam Staal (BZK/Bureau MIDO)

De volgende organisaties hebben reviewcommentaar geleverd op een concept versie van deze domeinarchitectuur:

- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, inclusief Logius, Bureau Forum Standaardisatie, de Rijksdienst voor Identiteitsgegevens, Kadaster en Programma Federatief Data Stelsel
- Ministerie van Volksgezondheid, Welzijn en Sport
- Ministerie van Financiën, inclusief de Belastingdienst en dienst Toeslagen
- Ministerie van Justitie en Veiligheid, inclusief de Justitiële ICT Organisatie en de Nationale Politie
- Ministerie van Economische Zaken en Landbouw, inclusief de Rijksdienst voor Ondernemend Nederland
- Vereniging van Nederlandse Gemeenten
- Gemeente Amsterdam
- Interprovinciaal Overleg
- Provincie Overijssel
- Unie van Waterschappen
- Het Waterschapshuis
- UWV
- DUO
- Geonovum
- Inlichtingenbureau