Referentiearchitectuur

Regie op Gegevens

**November 2021**

**INHOUDSOPGAVE**

[1 Inleiding 3](#_Toc85814919)

[1.1 Versiehistorie 3](#_Toc85814920)

[1.2 Doelstelling RoG 3](#_Toc85814921)

[1.3 Doelstelling referentiearchitectuur 3](#_Toc85814922)

[1.4 Scope van deze referentiearchitectuur 4](#_Toc85814923)

[2 Juridisch kader 5](#_Toc85814924)

[2.1 Europese ontwikkelingen t.a.v. de data-economie 5](#_Toc85814925)

[2.2 Relevante wetgeving voor Regie op gegevens 6](#_Toc85814926)

[2.3 Wet Digitale Overheid 7](#_Toc85814927)

[3 Leidende principes 8](#_Toc85814928)

[4 Functiemodel Regie op Gegevens 9](#_Toc85814929)

[4.1 Functionele domeinen 9](#_Toc85814930)

[4.2 Functiemodel Regie op Gegevens 9](#_Toc85814931)

[5 Gegevens 14](#_Toc85814932)

[5.1 Waarde in het maatschappelijk verkeer 14](#_Toc85814933)

[5.2 Informatiepositie 14](#_Toc85814934)

[5.3 Informatiepositie per sector 15](#_Toc85814935)

[5.4 Identificerende gegevens 15](#_Toc85814936)

[5.5 Overige persoonsgegevens en bronnen 16](#_Toc85814937)

[5.6 Ontwikkeling naar federatieve data infrastructuur 16](#_Toc85814938)

[5.7 Gegevenswoordenboek 17](#_Toc85814939)

[5.8 Gegevensservices 17](#_Toc85814940)

[5.8.1 Verzamelen 17](#_Toc85814941)

[5.8.2 Integreren 18](#_Toc85814942)

[5.8.3 Afleiden 18](#_Toc85814943)

[5.9 Eigenaarschap van gegevens 18](#_Toc85814944)

[6 Proces 19](#_Toc85814945)

[6.1 Actoren 19](#_Toc85814946)

[6.2 Triggers 19](#_Toc85814947)

[6.3 Interactiepatronen 20](#_Toc85814948)

[6.3.1 Interactiepatroon Burger wint in 20](#_Toc85814949)

[6.3.2 Interactiepatroon Dienstverlener wint in 21](#_Toc85814950)

[7 Applicatie 23](#_Toc85814951)

[7.1 Applicatieservices Regie op Gegevens 23](#_Toc85814952)

[7.2 Schets services *Burger wint in* 23](#_Toc85814953)

[7.3 Schets services *Dienstverlener wint in* 26](#_Toc85814954)

[7.4 Persoonlijk digitale omgevingen 27](#_Toc85814955)

[7.5 Europese portemonnee voor digitale identiteit 27](#_Toc85814956)

[8 Infrastructuur 29](#_Toc85814957)

[9 Governance: vertrouwensraamwerk 30](#_Toc85814958)

# Inleiding

## Versiehistorie

|  |  |  |
| --- | --- | --- |
| Versie 0.2 | 20-8-2020 | Initiële versie voor interne review |
| Versie 0.3 | 8-9-2020 | Versie voor externe review |
| Versie 0.4 | 12-1-2021 | Feedback externe review verwerkt |
| Versie 0.5 | 12-5-2021 | Aanpassing hoofdstuk 2 en enkele tekstuele aanpassingen t.b.v. de leesbaarheid. |
| Versie 0.6  (versie 2021) | 25-10-2021 | Andere opmaak i.v.m. leesbaarheid  Toevoeging Europese ontwikkelingen  Aanvullingen op hoofdstukken Applicaties en Infrastructuur |

## Doelstelling RoG

De overheid maakt voor de uitoefening van haar taken intensief gebruik van persoonlijke

gegevens van burgers. Zowel de overheid zelf als de burgers hebben er belang bij dat die

gegevens correct en actueel zijn, efficiënt worden gebruikt, en veilig worden bewaard en

gebruikt, conform geldende wetgeving.

Een burger kan inzien welke gegevens de overheid heeft en waarvoor deze worden gebruikt, en

kan deze zo nodig (laten) corrigeren of wijzigen als ze onjuist of niet meer actueel zijn. Ook heeft

hij het recht om (basis)gegevens die de overheid al heeft niet onnodig (opnieuw) te verstrekken.

Dit is staand beleid en wettelijk verankerd in de Algemene wet bestuursrecht (Awb), de

Algemene verordening gegevensbescherming (AVG) en wetgeving voor de basisregistraties.

Daarmee is de basis voor regie op de eigen gegevens gelegd.

Het kabinet wil deze bestaande regiemogelijkheden uitbreiden met een belangrijk nieuw spoor,

door burgers in staat te stellen hun eigen gegevens zelf, digitaal te delen met private dienstverleners, zoals zorgverleners, onderwijsinstellingen, schuldhulpverleners of woningcorporaties.

Hierdoor kunnen deze hun klanten betere diensten leveren, en wordt de administratieve

rompslomp beperkt ([Beleidsbrief Regie op Gegevens: nadere uitwerking](https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brieven/2019/07/11/beleidsbrief-regie-op-gegevens-nadere-uitwerking/beleidsbrief-regie-op-gegevens-nadere-uitwerking.pdf), p. 2).

Onder regie op persoonlijke gegevens wordt in de brief verstaan (p. 1): de handelingsopties die de

burger heeft als het gaat om de gegevens die overheidsorganisaties en nader te bepalen andere

organisaties in het BSN-domein (w.o. zorgverleners) over hem vastleggen.

Hierbij wordt onderscheid gemaakt in drie vormen van regie:

1. **inzage en correctie**

de eigen gegevens kunnen inzien en controleren, kunnen inzien welke gegevens worden en zijn uitgewisseld, en de gegevens kunnen (laten) corrigeren;

1. **eenmalige verstrekking**

kunnen weigeren om gegevens te verstrekken die binnen de overheid al beschikbaar zijn;

1. **delen van gegevens**

de eigen gegevens zelf, digitaal kunnen delen met dienstverleners buiten de overheid.

## Doelstelling referentiearchitectuur

De doelstellingen van Regie op Gegevens zijn (of worden momenteel) vertaald naar wetgeving, beleid en principes (vgl. hoofdstuk 2). Dit geeft richting en kleur aan het gewenste maatschappelijke effect. Anderzijds zijn er al verscheidende initiatieven waarin concrete voorzieningen voor het delen van gegevens gerealiseerd zijn of worden. Deze referentie-architectuur wordt gepositioneerd als generiek model tussen wetgeving en beleid enerzijds en de concrete initiatieven die al onderweg zijn of nog gaan komen anderzijds. Anders gesteld: de wat-vraag (wat moet er geregeld/ingericht worden om de doelstellingen te kunnen realiseren met als “scharnierpunt” het Functiemodel RoG) staat centraal en minder de hoe-vraag (met welke concrete oplossingen wordt die wat-vraag ingevuld). Die hoe-vraag wordt dus ingevuld door de (architectuur van de) sectoren/projecten zelf.

## Scope van deze referentiearchitectuur

De doelstelling van Regie op Gegevens is de burger regie te laten voeren op zijn eigen persoonsgegevens door de mogelijkheid te bieden persoonsgegevens in administraties van de overheid in te zien, daar waar nodig te corrigeren en indien gewenst de delen met derden. Inzage heeft betrekking op de persoonsgegevens die de overheid in zijn administraties heeft opgenomen én inzicht geven in welke persoonsgegevens tussen welke overheden worden gedeeld. Het functiemodel in deze referentiearchitectuur ondersteunt deze doelstelling, naast de doelstelling van het delen van gegevens vanuit een overheidsadministratie met de burger zelf.

Om de doelstellingen van Regie op Gegevens ten aanzien van het delen van gegevens te realiseren zijn in de toekomstige oplossing twee fasen te onderkennen, te weten:

1. ontsluiten (ter beschikking stellen) van de persoonsgegevens aan burgers (of met volmacht aan dienstverleners) uit bronnen van de overheid, eventueel met gebruik making van gegevensservices en vertrouwensservices;
2. gebruik van deze persoonsgegevens door burgers in hun relatie met dienstverleners (dus nadat ze door de overheid ter beschikking gesteld zijn).

In de eerste fase is de rol van de overheid die van *bronhouder* (leverancier van gegevens) terwijl in de tweede fase de rol van de overheid (ten hoogste) *marktmeester* zal zijn. Deze referentiearchitectuur beperkt zich tot de **eerste fase (de overheid als bronhouder)**. De tweede fase wordt ingevuld door wet- en regelgeving in combinatie met het vertrouwensraamwerk.

# Juridisch kader

## Europese ontwikkelingen t.a.v. de data-economie

[Europese ontwikkelingen](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_nl) ten aanzien van een interne markt voor data (d.w.z. de samenwerking tussen 27 lidstaten waar Nederland onderdeel van is en een bijdrage aan levert) hebben directe invloed op de ontwikkeling van de data-economie in Nederland. Die [Europese samenwerking](https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/europa/europees-beleid/) is al een aantal jaren gericht op het creëren van een interne markt voor gegevens zodat gegevens vrij kunnen stromen binnen de EU en tussen sectoren, e.e.a. met inachtneming van de Europese waarden. De EU stelt hierover in zijn [Europese Datastrategie](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en) ([gehele tekst](https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52020DC0066)):

*De EU werkt aan een interne markt voor data, waarin:*

* *gegevens tussen de verschillende EU-landen en de sectoren kunnen circuleren ten voordele van iedereen*
* *de Europese regels volledig in acht worden genomen, vooral wat betreft privacy, gegevensbescherming en mededinging*
* *eerlijke, praktische en duidelijke regels voor de toegang tot en het gebruik van data gelden*

*De EU wordt een aantrekkelijke, veilige en dynamische data-economie door:*

* *duidelijke en eerlijke regels op te stellen voor toegang tot en hergebruik van data*
* *te investeren in de volgende generatie van instrumenten en infrastructuren voor opslag en verwerking van data*
* *de krachten te bundelen voor de ontwikkeling van Europese cloudcapaciteit*
* *in belangrijke sectoren Europese data samen te brengen in de vorm van gemeenschappelijke en interoperabele dataruimten*
* *gebruikers de rechten, tools en vaardigheden te geven om volledige controle over hun data uit te oefenen*

Een aantal onderdelen van deze Europese ontwikkeling van de data-economie heeft directe invloed op Regie op Gegevens. De belangrijkste is misschien wel de ontwikkeling van de [Europese Digitale Identiteit](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_nl) (op basis van [eIDAS-verordening](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32014R0910&from=NL) uit 2014) ten behoeve van elektronische identificatie en waarmerken van die identificatie met behulp van vertrouwensservices.

Naar aanleiding van een [recente evaluatie](https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-evaluation-regulation) ([rapport](https://ec.europa.eu/newsroom/dae/redirection/document/76620)) is door de Europese Commissie *voorgesteld* deze ontwikkeling uit te breiden op het gebied van het waarmerken van gegevenssets (dus de combinatie tussen identiteit en uitspraken over die identiteit, de *provision of electronic attributes,* sectie 9 van het [amendement](https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0281)) en de eis aan de lidstaten om (direct of indirect) te voorzien in een eWallet voor burgers zodat zijn hun rechten beter kunnen effectueren.

Interoperabiliteit (door standaardisatie) wordt van groot belang geacht voor de succesvolle realisatie van deze strategie. De lidstaten ontwikkelen daartoe gezamenlijk [de IT-standaarden](https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation_en). Hiervoor wordt ieder jaar [een plan](https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2021) opgesteld. Voor Regie op gegevens is o.a. van belang de standaarden voor [*Electronic identification and trust services*](https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/electronic-identification-and-trust-services)en [*e-privacy*](https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/e-privacy)*.*

Naast de eIDAS-verordering en de GDPR/AVG zijn (tenminste op onderdelen) van belang voor Regie op Gegevens:

1- [Data Governance Act](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_nl)

* het voor hergebruik beschikbaar stellen van overheidsgegevens, wanneer die gegevens onderworpen zijn aan rechten van anderen;
* delen van gegevens tussen bedrijven tegen vergoeding, in welke vorm dan ook;
* toestaan dat persoonsgegevens worden gebruikt met behulp van een “bemiddelaar voor het delen van persoonsgegevens”, die als taak heeft personen te helpen hun rechten uit hoofde van de algemene verordening gegevensbescherming (AVG) uit te oefenen;
* het gebruik van gegevens op altruïstische gronden toestaan.

2- [Data Market Act](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_nl)

* Stelt regels voor poortwachters

3- [Data Services Act](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_nl)

* Stelt regels voor alle online intermediairs (w.o. transparantie en verantwoording)

4- [Single Digital Gateway](https://ec.europa.eu/growth/single-market/single-digital-gateway_nl)

* Geeft invulling aan het grensoverschrijdende *once-only* principe en de regie van de burger hierop.

## Relevante wetgeving voor Regie op gegevens

In 2020 heeft een inventarisatie plaatsgevonden naar het relevante [juridische kader voor Regie op Gegevens](https://rog.pleio.nl/files/view/c3d604c2-e461-4836-b7fe-ebe8936fa5ff/1584609034juridisch%20kader%20voor%20regie%20op%20gegevens%20%5bprdf-3226194%5d.pdf). Samengevat bestaat dit uit:

1. Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG)
2. Verdieping AVG: toestemming als grondslag voor het verwerken van persoonsgegevens versus toestemming voor een regietoepassing
3. Wet basisregistratie personen (Wet BRP)
4. Wet algemene bepalingen burgerservicenummer (Wabb)
5. eIDAS-verordening (directe werking)
6. Wet elektronisch bestuurlijk verkeer (Webv)
7. Algemene beginselen van behoorlijk bestuur
8. Geheimhoudingsplichten
9. Vertegenwoordigen en machtigen in het BW en de Awb
10. Verantwoordelijkheden en aansprakelijkheden
11. Mededinging en de Wet Markt en Overheid (Wet M&O)
12. Archiefwet
13. Tijdelijk besluit digitale toegankelijkheid overheid
14. Diverse wet- en regelgeving voor bronnen van aanbieders

Voor een nadere toelichting wordt verwezen naar het rapport dat via bovenstaande link toegankelijk is gemaakt.

## Wet Digitale Overheid

Het [wetsvoorstel Wet digitale overheid (Wdo)](https://www.digitaleoverheid.nl/dossiers/wet-digitale-overheid/dossier-documenten/wetsvoorstel-digitale-overheid/) legt de basis voor de verdere digitalisering van de overheid. [De eerste tranche (deel) van Wdo](https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/wet-digitale-overheid-in-het-kort/) gaat over veilig inloggen op dienstverlening bij (semi-) overheidsinstanties. De Wet digitale overheid is de [opvolger](https://www.digitaleoverheid.nl/nieuws/wet-gdi-als-wet-digitale-overheid/?pk_campaign=nieuwsbrief-18-2017) van de Wet Generieke digitale infrastructuur (GDI). De [GDI](https://nl.wikipedia.org/wiki/Wet_digitale_overheid#Generieke_digitale_infrastructuur) bestaat uit een set voorzieningen t.a.v. Identificatie & Authenticatie, Dienstverlening, Gegevens en Interconnectiviteit.

Het wetsvoorstel is een zogeheten kaderwet; de wet regelt algemene principes, verantwoordelijkheden en procedures, maar geen gedetailleerde regels. De wet zorgt zo voor flexibiliteit bij nieuwe ontwikkelingen. Maar ook dat belangrijke waarden en zekerheden voor burgers, zoals gebruikersvriendelijkheid, betrouwbaarheid, veiligheid, privacy en digitale inclusie altijd geborgd zijn.

Deze wet:

* legt de taken en verantwoordelijkheden vast voor veilige toegang tot de digitale overheid
* legt verplichtingen op aan mede-overheden om veilig en betrouwbaar aan te sluiten, en hun dienstverlening in te delen op een betrouwbaarheidsniveau
* stelt regels over de bekostiging daarvoor
* biedt zekerheden voor burgers en bedrijven
* biedt uitgangspunten voor informatiebeveiliging en de verwerking van persoonsgegevens.

Het wetsvoorstel gaat over veilig inloggen op dienstverlening bij (semi-) overheidsinstanties. In de Wdo staat welke van deze instanties te maken krijgen met de nieuwe regels voor de toegang tot hun elektronische dienstverlening. Dit zijn:

* bestuursorganen in de zin van de Awb, zoals gemeenten en uitvoeringsinstanties (UWV, SVB, Belastingdienst, DUO, RDW, etc.);
* aangewezen organisaties als de zorgsector, onderwijsinstellingen en pensioenfondsen
* de rechterlijke macht.

De uitwerking van de Wdo als kaderwet vindt plaats in de lagere regelgeving. Zoals in algemene maatregelen van bestuur (AMvB’s) en ministeriële regelingen. Zo is er ruimte voor innovatie, verdere keuzes en nieuwe voorzieningen en functionaliteiten.

Dit voorstel maakt het mogelijk om straks via publieke én private inlogmiddelen digitaal zaken te doen met bijvoorbeeld gemeenten en zorginstanties. Alleen middelen die door de overheid op veiligheid en betrouwbaarheid zijn gecontroleerd worden toegelaten. Die zijn dan in het publieke domein toegestaan. Hoewel inloggen bij diensten van commerciële/private partijen zoals webwinkels niet in deze wet wordt geregeld, kunnen burgers met de gecontroleerde private middelen ook daar inloggen. Zo heeft het wetsvoorstel toch een breder effect en voordeel voor veilig inloggen.

Voor de [tweede tranche](https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/vooruitblik-op-tweede-tranche-wet-digitale-overheid/) van de Wet digitale overheid (Wdo) komen de volgende onderwerpen in aanmerking komen voor wettelijke verankering. Dit zijn:

* **Het kader voor het verantwoord delen van digitale persoonsgegevens met partijen binnen en buiten de overheid (regie op gegevens**);
* Het beleggen van de verantwoordelijkheid voor het [stelsel van basisregistraties](https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/basisregistraties-en-stelselafspraken/stelsel-van-basisregistraties/%22) en het bewaken van de werking daarvan, waaronder het correct (en verplicht) gebruik van authentieke gegevens in het stelsel;
* Hoe kunnen in de Wdo het burger- en bedrijvendomein verder naar elkaar toe groeien?

# Leidende principes

In fase 1 van het programma Regie op Gegevens zijn aan de hand van de (beoogde) wetgeving en beleid meer in detail de principes waarlangs Regie op gegevens ingevuld dient te worden, nader uitgewerkt. Het resultaat hiervan is uitgewerkt in een [matrix](https://rog.pleio.nl/files/view/ca321af6-49fe-4c2a-9ae1-7bfe2ba26eda/1584609941matrix%20bij%20het%20kader%20voor%20rog_februari2020.pdf). In dit hoofdstuk zijn de principes op hoofdlijnen nader toegelicht.



# Functiemodel Regie op Gegevens

In de bijlage Functionele beschrijving RoG is geanalyseerd welke functies (= inrichtingsonafhankelijke bewerkingen) nodig zijn om regie op gegevens door burgers mogelijk te maken. In dit hoofdstuk worden deze functies gegroepeerd in functionele domeinen en een functiemodel. Dit model beschrijft dus de “wat-vraag” (wat is nodig om…?) en niet de “hoe-vraag” (welke techniek is hiervoor nodig?).

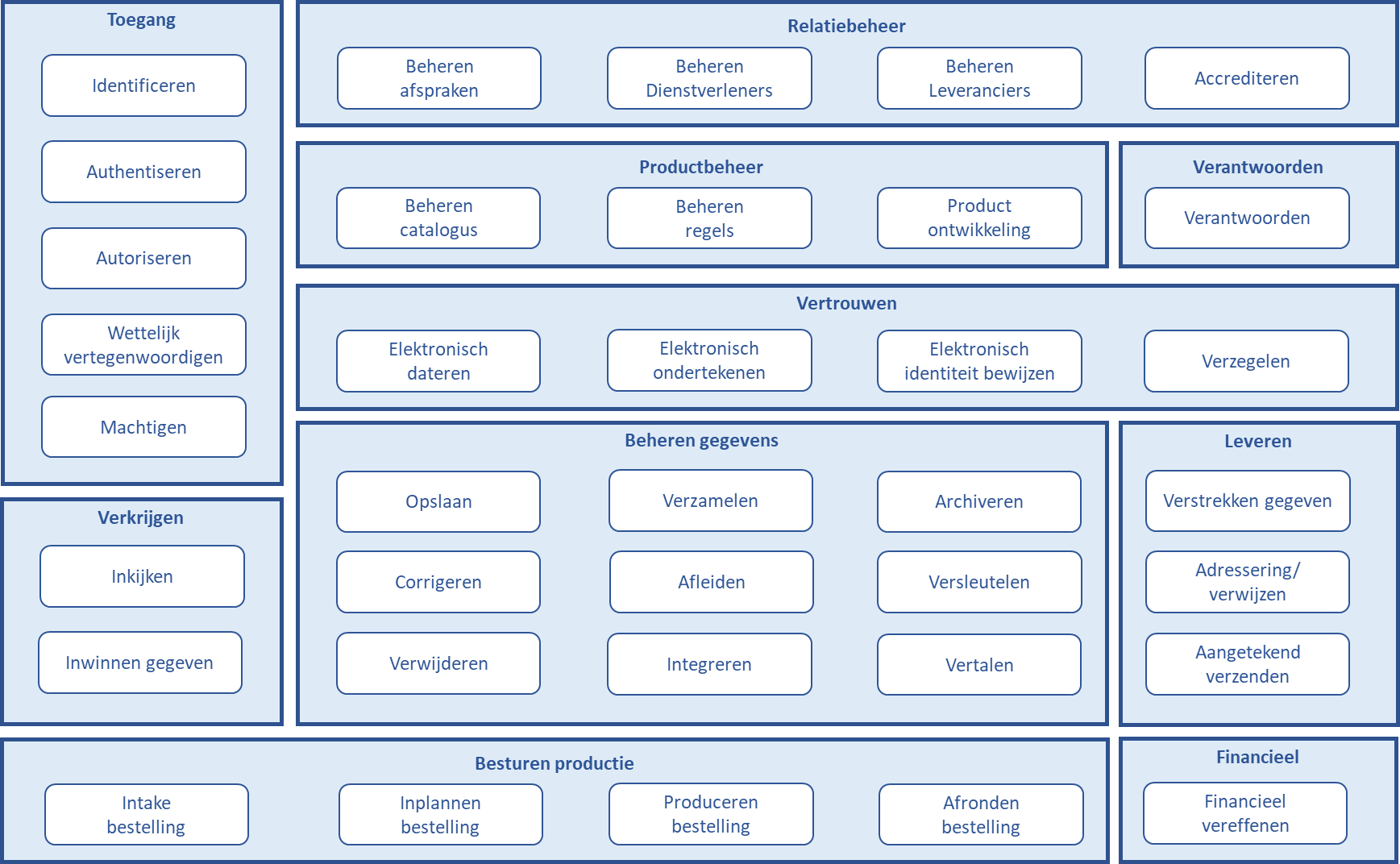
## Functionele domeinen

De volgende functionele domeinen worden onderkend:

1. Toegang
2. Verkrijgen gegevens
3. Relatiebeheer
4. Productbeheer
5. Besturen productie
6. Beheren gegevens (gegevensservices)
7. Creëren vertrouwen (vertrouwensservices)
8. Verstrekken gegevens
9. Verantwoorden
10. Financieel

## Functiemodel Regie op Gegevens

In het Functiemodel (in het Engels: *Capability Model*) RoG worden per functiedomein de functies nader uitgewerkt.



|  |  |
| --- | --- |
| **Toegang** | |
| Identificeren | Vaststellen wie is een gebruiker, een andere computer of applicatie is. |
| Authentiseren | Authentiseren is de activiteit waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs. |
| Autoriseren | De vrager is bevoegd indien de bestelling overeen komt met de gemaakte afspraken (door wie, over wie, welk gegeven, waarom en wanneer). Controleren op vereiste toestemming maakt hier onderdeel van uit. |
| (Wettelijk) vertegenwoordigen | Indien een persoon handelingsonbekwaam is omdat deze minderjarig, onder bewindvoering of curatele staat, treedt een vertegenwoordiger (ouder, voogd, bewindvoerder, curator) op in zijn naam. Deze vertegenwoordiger treedt in de plaats van de persoon. |
| Machtigen | Machtigen (*het verlenen van een volmacht*) heeft hier betrekking op het verlenen van toestemming aan een dienstverlener om in het kader van een offerte nader gespecificeerde gegevens die zich in de administratie van de overheid bevinden op te halen en rechtstreeks aan die dienstverlener te verstrekken. Onderdeel van machtigen is ook het beheren van de machtigingen (dus overzicht geven, verlenen, wijzigen en intrekken).  Een andere vorm van volmacht verlening is de vertegenwoordiger (zoals schuldhulpverlener, echtscheidingsconsulent e.d.) die in opdracht van de vertegenwoordigde burger namens deze burger optreedt. |

|  |  |
| --- | --- |
| **Vertrouwen (waarmerken)** | |
| Elektronisch dateren | Een gegeven of set van gegevens wordt hiermee voorzien van een datum zodat vastgelegd is wat de datum van creëren/levering is. Komt overeen met *elektronische tijdstempel* uit [eIDAS](https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0281) (amendement artikel 3 punt 16). |
| Elektronisch ondertekenen | Een gegeven of set van gegevens wordt hiermee voorzien van een elektronische verklaring van de afzender dat deze ook daadwerkelijk de afzender is. Komt overeen met *elektronische ondertekening* uit eIDAS. |
| Elektronisch identiteit bewijzen | Een gegeven of een set van gegevens wordt hiermee voorzien van bewijs van de identiteit van de betrokkene. Komt overeen met *elektronische identiteitsbewijs* uit eIDAS. |
| Elektronisch verzegelen | Een gegeven of set van gegevens wordt hiermee voorzien van een elektronisch waarborg dat de set overeenkomt met de inhoud van de bron/verklaring van de afzender nadat deze door de afzender verzonden is (integriteit van de inhoud en afzender). Komt overeen met *elektronisch zegel* uit eIDAS. |

|  |  |
| --- | --- |
| **Beheren gegevens** | |
| Opslaan gegevens | Gegevens die ingewonnen zijn kunnen voor later gebruik opgeslagen worden. |
| Corrigeren | Wanneer de burger kennis heeft van de onjuistheid van een gegeven in de administratie van de overheid, dan kan hij een verzoek tot correctie indienen. De overheid zal dit gegeven in onderzoek nemen en indien nodig aanpassen. |
| Verwijderen | Wanneer een gegeven niet meer geldig is, dan kan dit gegeven verwijderd worden. Verwijderen kan betekenen vernietigen (bijv. i.v.m. het *recht om vergeten* te worden) maar ook een gegeven van een einddatum voorzien zodat op een later tijdstip de historie te achterhalen is. Archiveren wordt als een aparte functie onderkend. |
| Verzamelen | Gegevens worden binnen deze activiteiten gereed gemaakt voor verzending. Dit kan gebeuren tijdens het inwinnen maar ook tijdens de opslag of bij levering. Afhankelijk van het gegeven en de manier waarop deze vanuit de administratie beschikbaar is, bestaat het klaar maken voor levering uit het *verzamelen* van de benodigde gegevens, indien nodig *filteren* van de verzameling en *samenstellen* indien gegevens uit verschillende bronnen in één levering bijeengebracht moeten worden. |
| Integreren | Met de functie integreren (aggregeren) worden gegevens in onderlinge samenhang gebracht op een zodanige manier dat deze verwerkt kunnen worden door de gebruiker. Waar de functie Verzamelen meer doelt op de logistiek van gegevens, doelt de functie Integreren meer op de inhoud en onderlinge samenhang van gegevens (bijv. in tijd). |
| Afleiden | Afleiden gaat nog een stap verder dan integreren: binnen deze functie worden op basis van regels conclusies getrokken en nieuwe gegevens (de conclusie) gegenereerd. Afleiden speelt een belangrijke rol binnen dataminimalisatie in het kader van privacybescherming. |
| Archiveren | Indien gewenst kunnen gegevens opgeslagen worden voor later gebruik. Deze functie onderscheidt zich van de functie Opslaan Gegevens door het doel van de opslag: beschikbaar voor gebruik in het primaire proces versus beschikbaar voor verantwoording/reconstructie/onderzoek enz. achteraf. |
| Versleutelen | Als onderdeel van een bredere beveiligingsstrategie kunnen gegevens op verschillende momenten in het proces versleuteld worden. Breder geformuleerd kan deze functie *Beveiligen* genoemd worden, waarbij versleutelen een van de opties is. |
| Vertalen | Indien gewenst kunnen gegevens vanuit het Nederlands vertaald worden naar andere talen en vice versa. |

|  |  |
| --- | --- |
| **Verkrijgen** | |
| Inkijken | Het inzien van zijn gegevens in de administratie van een overheidsorganisatie om kennis te nemen van de inhoud. |
| Inwinnen gegeven | Een gegeven wordt vanuit de omgeving van de bron in de eigen omgeving gebracht met als doel deze direct te gebruiken of op te slaan voor later gebruik. |

|  |  |
| --- | --- |
| **Leveren** | |
| Verstrekken gegeven | De gevraagde gegevens worden door de bron (i.c. overheid) conform afspraak aan de afnemer (burger of dienstverlener) verstrekt (push). |
| Adressering/ verwijzen | Een vorm van leveren van een gegeven kan ook zijn het verwijzen naar een bron waar het gewenste gegeven opgehaald kan worden (pull). |
| Aangetekend verzenden | Een bericht (“elektronisch pakketje”) wordt met extra waarborgen verzonden (vooral: bewijs van ontvangst). Komt overeen met *elektronisch* aangetekende verzendinguit eIDAS. |

|  |  |
| --- | --- |
| **Relatiebeheer** | |
| Beheren afspraken | Leveringen van gegevens van leverancier (i.c. overheid) naar dienstverlener geschiedt enkel op basis van afspraak. Deze afspraken moeten gemaakt, aangepast en beëindigd kunnen worden. |
| Beheren dienstverleners | Om een goede samenwerking te borgen, is het voor de leverancier noodzakelijk te weten wie zijn afnemers zijn en wat daar speelt (dus zowel operationeel, tactisch als strategisch relatiebeheer richting dienstverleners). |
| Beheren leveranciers | Om een goede samenwerking te borgen, is het voor de dienstverlener noodzakelijk te weten wie zijn leveranciers zijn en wat daar speelt (dus zowel operationeel, tactisch als strategisch relatiebeheer richting dienstverleners). |
| Accrediteren | Dit is de activiteit die de deelname van een dienstverlener en een leverancier aan een (sectoraal) ecosysteem beheert. Hieronder valt toelaten, wijzigen en verwijderen van deelnemers aan samenwerkingsverbanden/ ecosystemen alsmede toezicht op de naleving van de regels. |

|  |  |
| --- | --- |
| **Productbeheer** | |
| Beheren catalogus | Beheren catalogus is de activiteit die het actuele aanbod aan gegevens inclusief levervoorwaarden van de leverancier inzichtelijk maakt. |
| Beheren regels | Binnen de activiteit Beheren regels worden de afleidings- en samenstellingsregels (in relatie tot de gegevens) beheerd. |
| Productontwikkeling | Gegevens die niet in de catalogus opgenomen zijn of niet tegen de gewenste levervoorwaarden, kunnen binnen de activiteit Productontwikkeling leverbaar gemaakt worden (inclusief aanpassing van de levervoorwaarden). Het resultaat van productontwikkeling is een nieuw gegeven in de catalogus. |

|  |  |
| --- | --- |
| **Besturen productie** | |
| Intake bestelling | De bestelling wordt geregistreerd en aan de hand van de afspraak beoordeeld. |
| Inplannen bestelling | Indien nodig wordt de bestelling ingepland voor productie en levering (een bestelling kan meerdere periodieke leveringen bevatten). |
| Produceren bestelling | De bestelling wordt aan de hand van de specificaties gereed gemaakt voor levering. |
| Afronden bestelling | Na levering is de bestelling gereed. Registratie hiervan vindt plaats in een productiesysteem. Deze afronding kan ook de trigger zijn voor financieel afwikkelen. |

|  |  |
| --- | --- |
| **Financieel vereffenen** | |
| Financieel vereffenen | Indien overeengekomen vindt financiële vereffening plaats. |

|  |  |
| --- | --- |
| **Verantwoorden** | |
| Verantwoorden | De wet (waaronder AVG) en de betrokken organisaties zelf stellen eisen aan de registratie van alle relevante handelingen in het kader van delen van gegevens. Doel van deze registratie is verantwoording (naar de burger als ook intern) mogelijk te maken. Organisaties leggen verantwoording af aan de burger over de verwerking van zijn persoonsgegevens. |

# Gegevens

## Waarde in het maatschappelijk verkeer

De eIDAS-verordening uit 2014 regelt, samengevat, de *identificatie* van een natuurlijke persoon (met erkenning van andere Europese inlogmiddelen) en de vertrouwensservices waarmee gegevens over die persoon elektronisch *gewaarmerkt* kunnen worden. Bij de [evaluatie](https://ec.europa.eu/newsroom/dae/redirection/document/76620) van deze verordening in 2020 bleek dat de spelers in de markt dit weliswaar een stap in de goede richting vonden, maar dat echte waarde van (persoons)gegevens pas gecreëerd wordt als het identificerende gegeven in relatie met de relevante gegevens over die persoon gewaarmerkt geleverd worden. Dus:

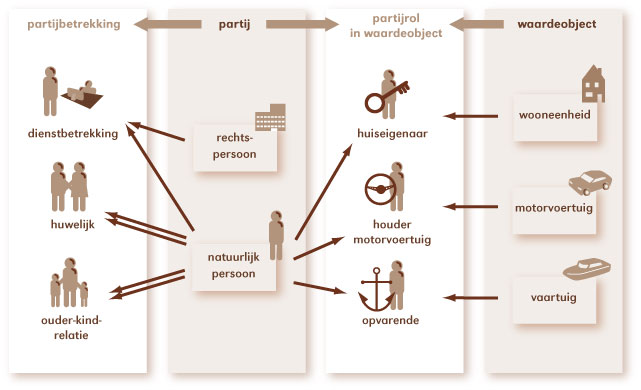
* persoon A heeft een zwemdiploma,
* persoon B is rijbevoegd,
* persoon C vormt geen risico voor Covid19-besmetting,
* persoon D is houder van een gekentekend voertuig

Omdat de huidige verordening op dit punt tekort schiet, wordt deze in het (voorstel voor) [amendement](https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0281) van 2021 aangevuld met de mogelijkheid om identificerende gegevens (blauw) te koppelen aan kenmerken (groen) middels een relatie (rood). Deze kunnen vervolgens met behulp van de vertrouwensservices (zie domein 7 van het functiemodel) gewaarmerkt worden om garanties over inhoud en bron/afzender te geven. Het is deze drie-eenheid (identificerende gegevens, kenmerken en bron) die waarde creëert.

## Informatiepositie

Het belang hiervan komt ook tot uiting in de informatiepositie van de burger. De doelstelling van Regie op Gegevens is - geheel in lijn met de Europese Datastrategie- de burger meer inzicht te geven in de persoonsgegevens die de overheid over hem heeft vastgelegd en hem tevens de mogelijkheid te geven om deze persoonsgegevens te gebruiken in transacties buiten de overheid. Voor het (her)gebruik van die gegevens binnen de overheid geldt al het *once-only-*principe.

Deze persoonsgegevens worden gebruikt in overeenkomsten met dienstverleners om de gewenste informatiepositie ten behoeve van die overeenkomst in te vullen. De informatiepositie van de burger wordt hier dus gedefinieerd als een set van gegevens betreffende die burger, nodig om de overeenkomst met de dienstverlener aan te kunnen gaan. Deze set beschrijft *de persoon* en de *relatie* met objecten en andere personen, e.e.a. in de *context* van de overeenkomst *waarin deze gebruikt wordt*.



Zo zal een informatiepositie (de gewenste gegevensset) ten behoeve van het aankopen van een huis een andere zijn dan een informatiepositie van diezelfde burger ten behoeve van een behandelovereenkomst met een arts. Dezelfde persoon, echter andere relevante gegevens. Conclusie: er is altijd een relatie te leggen tussen de informatiepositie (de gevraagde gegevensset) en het doel (de context) waarvoor deze gegevens gebruikt worden.

## Informatiepositie per sector

De gebeurtenis in het leven van een burger bepaalt dus de overeenkomst die de burger met een dienstverlener wil aangaan om een product of dienst geleverd te krijgen. Op basis van de overeenkomst is vast te stellen welke gegevens nodig zijn om tot die overeenkomst te komen. Burger en dienstverlener kunnen het gesprek over welke gegevens nodig zijn aangaan op het moment dat de burger die dienst wil gaan afnemen.

Dat zal voor de meeste burgers niet eenvoudig zijn, dus ligt het voor de hand om deskundige vertegenwoordigers van burgers (zo spreekt bijvoorbeeld de [Data Governance Act](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52020PC0767&from=EN) in artikel 9 lid 1 onder c over *gegevenscoöperaties*) vooraf hierover in gesprek te laten gaan met deskundige vertegenwoordigers van dienstverleners die namens een sector afspraken maakt over (onder meer) de gegevensset die verzameld wordt op het moment dat een burger zich meldt voor het afnemen van een dienst. Afspraken hierover kan dan onderdeel uitmaken van het Vertrouwensraamwerk waar betrokken partijen zich aan conformeren.

## Identificerende gegevens

Onderdeel van de informatiepositie vormen de identificerende gegevens (de blauwe gegevens uit paragraaf 5.1). Deze kunnen gedefinieerd worden als een unieke set persoonskenmerken dat op exact één individu betrekking heeft. Vaak is de enkele combinatie tussen *achternaam* en *geboortedatum* al voldoende om één individu uniek te identificeren. Voor die gevallen waarin dat niet toereikend is, is het toevoegen van één of enkele persoonskenmerken (bijv. voornaam, geboorteplaats) voldoende om in een populatie de anderen te uniek identificeren. Het [Interoperabiliteitskader elektronische identificatie en vertrouwensdiensten](https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1501) (behorend bij eIDAS 2015) maakt voor een natuurlijk persoon onderscheid in een minimale pakket persoonsidentificatiegegevens en een set van mogelijke aanvullingen:



Binnen de context van Regie op Gegevens wordt ervan uitgegaan dat de **overheid** de identiteit van een persoon aan de hand van identificerende gegevens vaststelt (en niet de burger zelf of een andere partij).

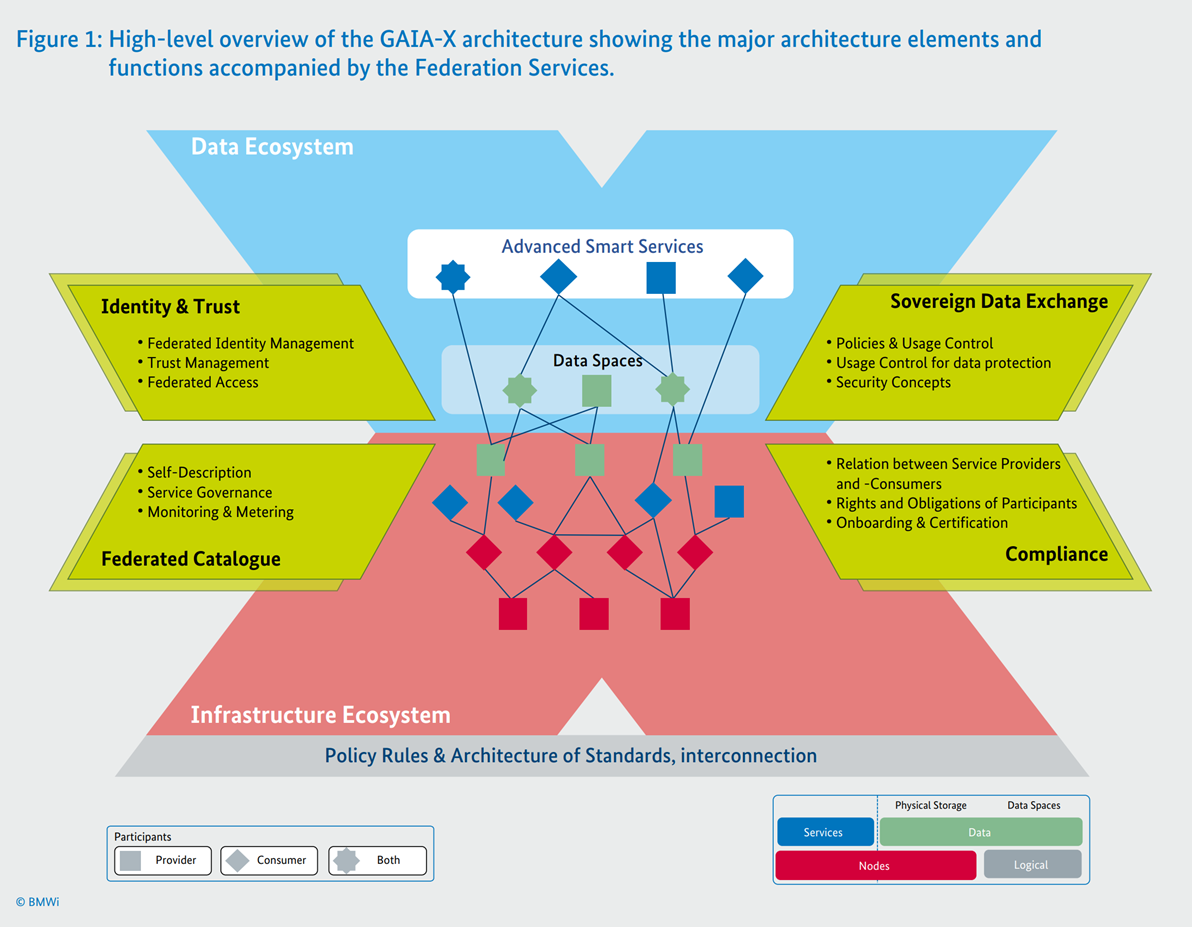
## Overige persoonsgegevens en bronnen

In paragraaf 5.1 werd al gewezen op het feit dat waarde gecreëerd wordt door de combinatie van identificerende gegevens, kenmerken en bron. Hierbij wordt met kenmerk (ook wel elektronisch attribuut genoemd) bedoeld ieder gegeven dat een bewering doet over die persoon. De overheid heeft een grote hoeveelheid en diversiteit aan beweringen over personen in zijn bronnen opgenomen. Deze bronnen bij de overheid zijn allereerst de basisregistraties, die oorspronkelijk bedoeld zijn om informatieposities rondom natuurlijke personen, rechtspersonen en locaties op te bouwen voor hoofdzakelijk intern overheidsgebruik. Ook zijn er vele informatieposities opgebouwd in sectorale registraties, bedoeld voor intern overheidsgebruik.

In de NORA zijn de [Basisregistratie](https://www.noraonline.nl/wiki/Basisregistraties) en [Sectorregistraties](https://www.noraonline.nl/wiki/Sectorregistraties) als bouwblokken opgenomen (een [overzicht](https://www.noraonline.nl/wiki/Alle_sectorregistraties) van 145 registraties op basis van een inventarisatie uit 2017). Zowel de [basisregistraties](https://www.noraonline.nl/wiki/Alle_basisregistraties) als sectorregistraties bevatten persoonsgegevens die mogelijk ontsloten dienen te worden. Naast deze registraties zijn er natuurlijk vele andere bronnen binnen de overheid waarin zich persoonsgegevens bevinden die voor ontsluiting in aanmerking komen. Er is ook een overzicht van datasets die in het kader van Open Data beschikbaar worden gesteld op [data.overheid.nl](https://data.overheid.nl/).

## Ontwikkeling naar federatieve data infrastructuur

Een belangrijke ontwikkeling in het delen van gegevens in Europees verband is [GAIA-X](https://www.ncsc.nl/actueel/weblog/weblog/2020/gaia-x) (gestart in 2020). Het [Duits-Franse GAIA-X-initiatief](https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html) richt zich op het realiseren van een pan-Europese ‘federatieve data infrastructuur’. Omdat die in belangrijke mate moet gaan steunen op onderling verbonden cloud diensten wordt GAIA-X ook gezien als een belangrijk vehikel om veilige Europese cloud voorzieningen te realiseren. Vanuit Nederland is Normcommissie ([NEN](https://www.nen.nl/gaia-x)) hierbij betrokken. In de [GAIA-X architectuur](https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=5) (2020) en [verdere uitwerking](https://www.gaia-x.eu/sites/default/files/2021-06/Gaia-X_Architecture_Document_2106.pdf) (2021) wordt het onderstaand model uitgewerkt, waarbij wordt ingezet op een Europees federatief model op de onderdelen Identity en trust, Woordenboek, Soevereine Gegevensuitwisseling en Compliance:



De visie op de **doorontwikkeling van het stelsel van basisregistraties** sluit naadloos op deze ontwikkeling aan:

*“Het hiervoor genoemde doel van onderlinge verbonden stelsels kan worden gerealiseerd door het huidige stelsel van 10 basisregistraties verder te ontwikkelen tot een stelsel waarin steeds meer partijen samenwerken om hun sectorale basisdata op de stelselmanier te ontsluiten, dus met waarborgen voor het vertrouwen bij burgers, afnemers en data aanbieders. Hiermee groeit het stelsel van basisregistraties uit tot een bredere nationale datafederatie van hoogwaardige databronnen die daartoe gerechtigde gebruikers flexibel, naar behoefte, kunnen toepassen en die op Europees niveau aansluiting biedt op soortgelijke stelsels van andere landen.”*

*“De NL-datafederatie is geen IT systeem en geen datapakhuis, maar een virtuele dataverzameling waarbij op registratieniveau of op sectorniveau het lokale aanbod volgens het principe van “data bij de bron” binnen het federatieve stelsel wordt ontsloten. Daarbij zorgt het adopteren van stelselafspraken, stelselstandaarden en stelselfuncties in combinatie met het toepassen van dezelfde identificerende gegevens/koppelsleutels ervoor dat individuele databronnen een datastelsel worden en dat data tussen de op het NL-datafederatie aangesloten partijen kan stromen*. *Van deze federatie kunnen zowel private als publieke databronnen deel uitmaken.” (Toekomstbeeld Stelsel van Basisregistraties v08c, p. 3 e.v.).*

## Gegevenswoordenboek

Gezien de omvang van het aantal mogelijk gewenste persoonsgegevens en bronnen is vindbaarheid van het juiste gegeven een uitdaging. Hiervoor bestaan al veel initiatieven waarop aangesloten kan worden. Het vinden van een gegeven begint met een eenduidige beschrijving van de betekenis van de gebruikte begrippen (waarbij bij voorkeur wordt gelinkt met de relevante wet- en regelgeving) in een gegevenswoordenboek. Daarnaast zijn aspecten als gegevenskwaliteit (juistheid, actualiteit enz.) en herkomst/bron van belang. Op Europees niveau wordt hiervoor verwezen naar [EU thesauri](https://op.europa.eu/nl/web/eu-vocabularies/thesauri) terwijl [BegrippenXL](https://www.begrippenxl.nl/) op nationaal niveau als ingang kan dienen. Daarnaast is er de bestaande (en beheerde) inventarisatie van [Gegevenswoordenboeken](https://www.noraonline.nl/wiki/Gegevenswoordenboeken) (inmiddels meer dan 25, waaronder de [Stelselcatalogus](https://www.stelselcatalogus.nl/)) in de NORA. Deze zijn/worden volgens de standaard JSON/Linked Data machineleesbaar en interpreteerbaar aangeboden.

## Gegevensservices

Wat nu als de gegevens in de bron niet overeenkomen met de vraag van burger en/of dienstverlener maar dat de vraag wel af te leiden is uit de gegevens die wel beschikbaar zijn? Dan zijn bewerkingen met behulp van gegevensservices nodig. Naast de CRUD (create, read, update en delete) wordt worden de bewerkingen *verzamelen*, *integreren* en *afleiden* hier nader toegelicht.

### Verzamelen

Gegevens worden binnen deze activiteiten gereed gemaakt voor levering (push of pull). Dit kan gebeuren tijdens het inwinnen (“doorlevering”) maar ook tijdens de opslag of bij levering. Afhankelijk van het gegeven en de manier waarop deze vanuit de bron beschikbaar is, bestaat het klaar maken voor levering uit het verzamelen van de benodigde gegevens, indien nodig filteren van de verzameling en samenstellen indien gegevens uit verschillende bronnen in één levering bijeengebracht moeten worden. Uitgangspunt bij verzamelen is dat er geen bewerking aan het gegeven zelf gedaan wordt, m.a.w. de onderdelen worden verzameld, in een doos gestopt, gewaarmerkt en aangeboden voor verzending.

### Integreren

Met de functie integreren (aggregeren) worden gegevens in onderlinge samenhang gebracht op een zodanige manier dat deze verwerkt kunnen worden door de gebruiker. Waar de functie Verzamelen meer doelt op de logistiek van gegevens, doelt de functie Integreren meer op de inhoud en onderlinge samenhang van gegevens door middel van de regels in een informatiemodel (bijv. in tijd zoals bij “omzet per maand” het geval zal zijn). In deze functie kunnen nieuwe gegevens ontstaan. Een voorbeeld van een voor de gebruiker in samenhang gebrachte gegevensset is natuurlijk het Kadaster (IMKAD) en andere basisregistraties.

### Afleiden

Afleiden gaat nog een stap verder dan integreren: binnen deze functie worden op basis van regels (algoritmen) conclusies getrokken en nieuwe gegevens (de conclusie) gegenereerd. Afleiden speelt een belangrijke rol binnen dataminimalisatie in het kader van privacybescherming.

Artikel 5 lid 1 sub c AVG stelt, als één van de ‘beginselen inzake verwerking van persoonsgegevens’, dat de gegevensverwerking toereikend is, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit laatste wordt ook het principe van dataminimalisatie genoemd en is daarmee onderdeel van de beperkende maatregelen op de inbreuk van de privacy van burgers. Ook binnen de [Wet Digitale O](https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/19/memorie-van-antwoord-bij-wetsvoorstel-digitale-overheid)verheid is privacy by design het uitgangspunt. Binnen de context van RoG zijn hierbij globaal drie strategieën te onderkennen:

1. Alleen die gegevens die strikt noodzakelijk zijn voor het beantwoorden van de vraag (dataminimalisatie door filteren, hiervoor beschreven als een vorm van verzamelen)
2. Conclusie als gegeven en niet de gegevens die leiden tot de conclusie (dataminimalisatie door delen afleiden)
3. Cryptografisch bewijs over gegevens zonder de gegevens zelf te delen (dataminimalisatie door wiskundig bewijs, waaronder diverse [Privacy Enhancing Technologies](https://en.wikipedia.org/wiki/Privacy-enhancing_technologies))

Transparantie naar de burger ten aanzien van het algoritme (naast de gegevens!) dat gebruikt wordt om de gewenste afleiding te doen is, één van de manieren om vertrouwen bij de burger te krijgen. Een van de manieren is de recente ontwikkeling van het [Nationaal Algoritmen Register](https://www.digitaleoverheid.nl/led-nieuws/de-bestuurlijke-regie-over-experimentele-data-en-algoritmen/).

## Eigenaarschap van gegevens

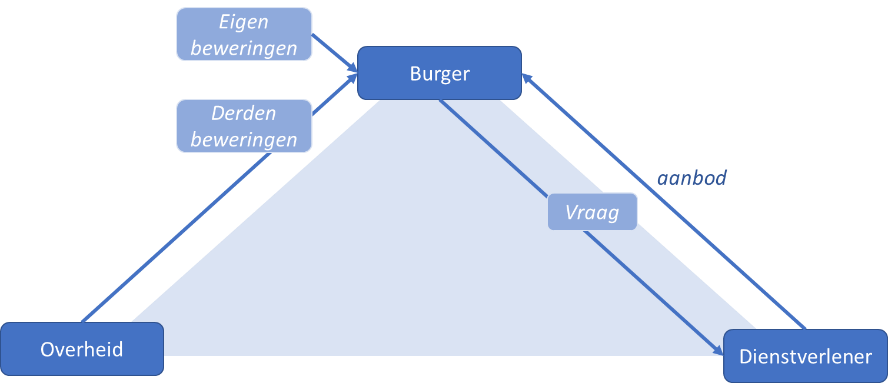
Uitgangspunt is dat de gegevenseigenaar (vaak de bronhouder) verantwoordelijk is voor de kwaliteit van het gegeven uit die bron. Gegevens die rechtstreeks uit de bron komen, door de eigenaar zelf gewaarmerkt worden met behulp van vertrouwensservices en aan de burger ter beschikking gesteld worden, kunnen door die gegevenseigenaar gegarandeerd worden als “overeenkomstig de bron”. Zodra dat waarmerken al door een ander dan de eigenaar wordt gedaan, dan zal die eigenaar die ander hierin al moeten vertrouwen wil die eigenaar de garantie kunnen blijven afgeven. Afspraken hierover kunnen in een vertrouwensraamwerk gemaakt worden.

Dit wordt al gecompliceerder wanneer tussen de weg van bron naar burger/dienstverlener bewerkingen (gegevensservices) plaatsvinden waarbij nieuwe gegevens ontstaan. Is de eigenaar van de brongegevens nog wel in staat om de kwaliteit van dat nieuwe gegeven te garanderen of ontstaat met het creëren van dit nieuwe gegeven ook een nieuwe eigenaar die verantwoordelijk is voor de gegevenskwaliteit? Ook hierover zullen [afspraken](https://ec.europa.eu/info/sites/default/files/summary-data-governance-data-policies_en.pdf) gemaakt moeten worden in een vertrouwensraamwerk.

# Proces

## Actoren

Binnen Regie op Gegevens worden de volgende actoren onderscheiden:



1. **Burger**

Onder burger wordt in deze context verstaan iedere natuurlijke persoon die ingezetene is in Nederland (zoals opgenomen in de BRP). Onder de categorie burger valt daarnaast ook de natuurlijke persoon die opgenomen is in het Register Niet-Ingezetenen RNI (niet-ingezetene met een relatie met de Nederlandse overheid). Burger is ook iedere Europese ingezetene die met een erkend Europees inlogmiddel toegang vraagt tot zijn persoonsgegevens.

Een burger kan zich laten vertegenwoordigen door een wettelijke vertegenwoordiger (indien van toepassing) of door een gevolmachtigde vertegenwoordiger.

1. **Dienstverlener**

Onder dienstverlener wordt in deze context verstaan iedere natuurlijke of rechtspersoon die een product of dienst aan een burger levert.

1. **Overheid (als bron)**

Onder overheid wordt in deze context verstaan iedere overheidsorganisatie die een bron beheert waarin zich persoonsgegevens bevinden. De overheid als marktmeester valt buiten de scope van de referentiearchitectuur. Deze rol wordt uitgewerkt in wet- en regelgeving en het vertrouwensraamwerk.

1. **Intermediair**

Onder intermediair wordt in deze context verstaan iedere natuurlijke of rechtspersoon die als tussenpersoon gegevens- en/of vertrouwensdiensten levert aan burger, dienstverlener of bronhouder (i.c. overheid).

## Triggers

Afbeelding met tekst

Automatisch gegenereerde beschrijvingOm invulling te geven aan het principe Burger Centraal wordt zoveel mogelijk de wereld van de burger als startpunt genomen voor de interactie tussen de actoren. Vanuit het perspectief van die burger is in de regel de aanleiding om persoonsgegevens uit een overheidsadministratie te willen ophalen een gebeurtenis in het leven van die burger naar aanleiding waarin deze producten of diensten geleverd wenst te krijgen van dienstverleners (of overheid). Deze gebeurtenissen kunnen zeer divers van aard zijn (zie kader) en starten iedere keer andere processen/interactiepatronen met andere actoren. Ook de gegevens die de burger per gebeurtenis nodig heeft om zijn product of dienst geleverd te krijgen, verschillen per gebeurtenis. De gebeurtenis start een dus specifiek proces/interactiepatroon en vereist een specifieke set aan gegevens, behorend bij die gebeurtenis.

## Interactiepatronen

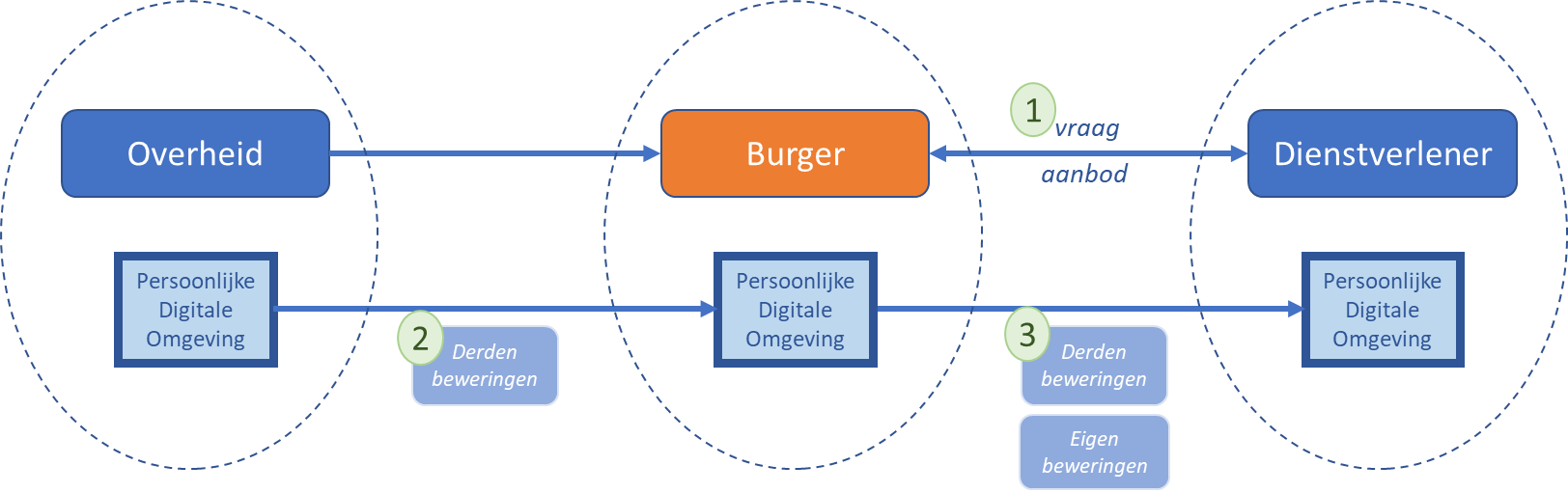
Om het persoonsgegeven van overheidsbron naar uiteindelijk de dienstverlener te krijgen, zijn in beginsel twee routes (de interactiepatronen) mogelijk, te weten:

1. De **burger wint het gegeven zelf in** bij de overheidsbron en levert deze vervolgens aan de dienstverlener of
2. De **dienstverlener wint het gegeven** **in** (met volmacht van de burger) bij de overheidsbron.

Enkele noties:

* Van belang is op te merken dat beide interactiepatronen uiteindelijk **hetzelfde resultaat** opleveren: het persoonsgegeven uit de overheidsbron worden aan de dienstverlener geleverd. Beide interactiepatronen stellen echter andere eisen (waaronder waarmerken en toestemming) en afhankelijk van de situatie kunnen dus keuzes gemaakt worden in de route om hetzelfde resultaat te bereiken.
* Daarnaast geldt het uitgangspunt dat de **burger vrij is om te kiezen** op welke wijze hij de gegevens wil delen. Hieronder worden de interactiepatronen nader uitgewerkt.

### Interactiepatroon Burger wint in



1-

De burger wil een product of dienst afnemen van de dienstverlener. Om een aanbod te kunnen doen heeft de dienstverlener (persoons)gegevens van/over de burger nodig.

Een deel van die informatiepositie zal bestaan uit gegevens die de burger zelf kan/moet invullen (eigen beweringen) en een deel kan bestaan uit gegevens die (op verzoek van de dienstverlener) uit een andere bron afkomstig zal zijn, hier gedefinieerd als derdenbeweringen uit de bron van de overheid. Het deel van de informatiepositie dat de burger met eigen beweringen kan invullen, kan de burger direct aan de dienstverlener leveren.

2-

Voor derdenbeweringen zal de burger dit gegeven eerst uit de bron van de overheid moeten ophalen en in zijn eigen Persoonlijke Digitale Omgeving moeten brengen. Als hij nog over een geldig gegeven uit de overheidsbron in zijn eigen Persoonlijke Digitale Omgeving beschikt, dan kan hij deze natuurlijk direct gebruiken en is ophalen bij de overheid niet nodig.

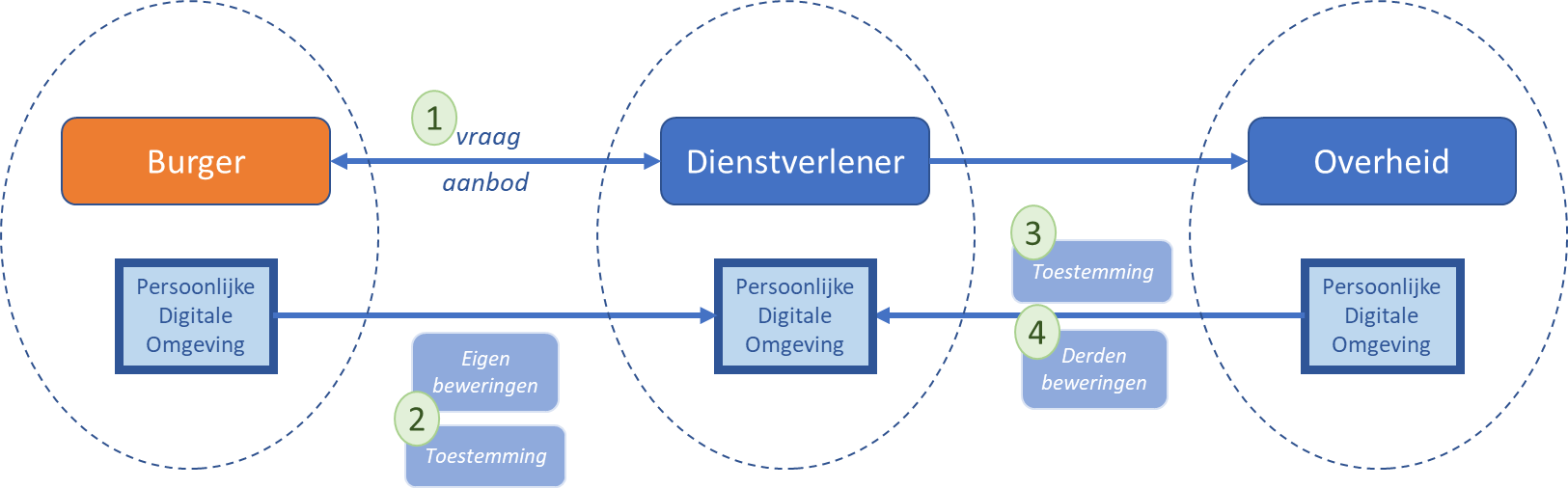
3-

Als de burger de gevraagde gegevens voor de informatiepositie (dus derdenbeweringen en eigen beweringen) compleet heeft, kan hij deze aan de dienstverlener leveren zodat deze het aanbod kan doen.

Kenmerken van dit interactiepatroon zijn:

* De **positie van de burger**. Deze staat letterlijk tussen dienstverlener en de bron in en heeft *by design* volledig zicht en controle op de gegevens die vanuit de overheidsbron met de dienstverlener gedeeld worden.
* Geen **koppeling tussen uitvraag bij de bron en doel** waarvoor het gebruikt wordt: de burger hoeft niet aan de bronhouder te verantwoorden waarom/waarvoor het persoonsgegeven ingewonnen wordt.
* de wens van het **waarmerk**: de dienstverlener wil de garantie dat het gegeven uit de bron (de derdenbewering) ook daadwerkelijk van die bron afkomstig is en overeenkomt met die bron. Hier speelt de **vertrouwensservice** (trustservices uit eIDAS) een grote rol.
* Het onderwerp **toestemming** (niet zijnde wettelijke vertegenwoordiging) maakt geen onderdeel uit van dit interactiepatroon.

### Interactiepatroon Dienstverlener wint in



1-

Ook dit interactiepatroon start met de relatie tussen dienstverlener en de burger. Om een aanbod te kunnen doen heeft de dienstverlener (persoons)gegevens van/over de burger nodig. Een deel van die informatiepositie zal bestaan uit eigen beweringen en (mogelijk) een deel uit derdenbeweringen.

2-

Het verschil met het vorige interactiepatroon is dat niet de burger de derdenbewering inwint, maar de dienstverlener aanbiedt om dat namens deze burger te doen. Het is dus de dienstverlener die zich bij de overheid digitaal meldt met het verzoek om een persoonsgegeven uit de bron van de overheid. De bronhouder zal vanwege zijn geheimhoudingsplicht deze gegevens alleen ter beschikking stellen indien de dienstverlener als gevolmachtigde van de burger optreedt, m.a.w. de dienstverlener toestemming heeft van de burger om namens hem de persoonsgegevens bij de overheid in te winnen.

3/4-

De dienstverlener wint met toestemming van de burger zijn persoonsgegevens (derdenbeweringen) in bij de overheid.

Kenmerken van dit interactiepatroon zijn:

* De **positie van de burger**. In dit interactiepatroon staat de dienstverlener tussen de burger en de bron in. Vanuit deze positie heeft de burger *by design* veel minder zicht en controle op de gegevens die vanuit de overheidsbron met de dienstverlener gedeeld worden. Om de burger toch vertrouwen te geven in zowel dienstverlener als overheid en hem uit vrij wil te bewegen gebruik te maken van deze dienst, zijn aanvullende maatregelen gericht op dit vertrouwen noodzakelijk.
* Het onderwerp **toestemming** maakt altijd onderdeel uit van dit interactiepatroon.
* **Koppeling tussen uitvraag bij de bron en doel** waarvoor het gebruikt wordt: de burger geeft toestemming aan de dienstverlener om gegevens namens hem in te winnen. De eis aan de toestemming is dat deze voldoende specifiek en afgebakend is (dus geen toestemming zoals dat nu bij bijv. *cookies* het geval is). Hierdoor kan de overheid mogelijk afleiden welke gegevens, waarvoor en aan wie geleverd worden.
* de wens van het **waarmerk is in dit interactiepatroon minder relevant**: de dienstverlener haalt namelijk zelf de gegevens rechtstreeks bij de vertrouwde bron en heeft daarmee al de nodige garanties op afzender en integriteit van het gegeven. Hier speelt de **vertrouwensservice** (trustservices uit eIDAS) dus minder een rol. Natuurlijk staat het de dienstverlener vrij om tegen vergoeding extra vertrouwensservices zoals digitale handtekening en/of digitale seal te gebruiken.
* Het moment waarop de burger volmacht (toestemming) verleent en aan wie kan verschillen en leiden tot een **variant op bovenstaand interactiepatroon**. Het is namelijk ook mogelijk dat de burger zijn wilsuiting (toestemming tot het leveren van vooraf gedefinieerde persoonsgegevens aan vooraf gedefinieerde dienstverleners in vooraf gedefinieerde gevallen) aan de overheid kenbaar maakt **voordat** de dienstverlener een verzoek bij de overheid tot het leveren van specifieke persoonsgegevens voor deze burger doet. De overheid zal dan in zijn eigen administratie moeten nagaan of de specifieke toestemming van die burger bestaat om vervolgens dit gegeven met toestemming van die burger aan de dienstverlener te kunnen leveren.

# Applicatie

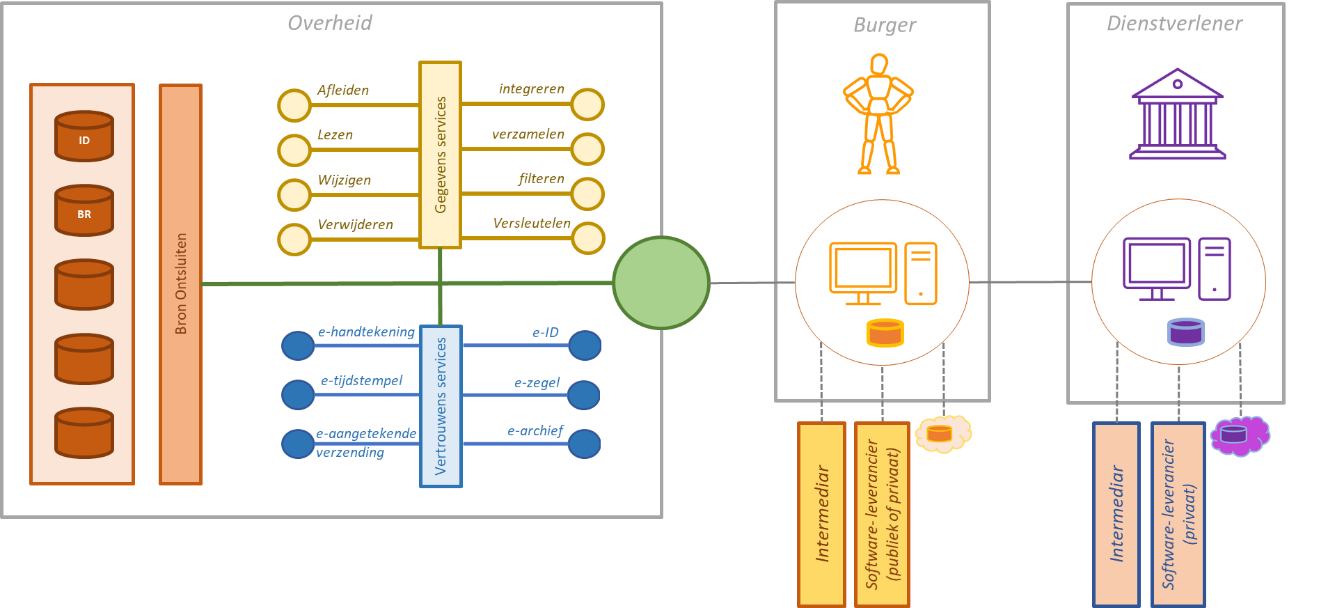
## Applicatieservices Regie op Gegevens

Een interactiepatroon beschrijft het proces dat de levering van het persoonsgegeven uit de administratie van de overheid aan de dienstverlener realiseert. In dit proces worden de functies uit het functiemodel (de inrichtingsonafhankelijke bewerkingen) aaneen geregen om tot het gewenste resultaat te komen. In de servicegeoriënteerde benadering van deze referentiearchitectuur betekent dit dat het eindresultaat voor de burger gerealiseerd wordt door applicatie- en netwerkservices die door werkstroombesturing in de juiste volgorde aangeroepen worden. De belangrijkste services die bij het ontsluiten van persoonsgegevens uit bronnen bij de overheid een rol spelen zijn (naast werkstroombesturing):

1. Toegangsservice (groen)
2. Koppelvlakservices (groen)
3. Gegevensservices (geel)
4. Vertrouwensservices (blauw)
5. Bronontsluitingsservices (geel en rood)

## Schets services *Burger wint in*

Toegepast op het interactiepatroon *Burger wint in* leidt dit tot het volgende model:



Aan de linkerkant de overheid als bron, in het midden de burger die contact maakt met de overheid om een gegeven in te zien, te corrigeren of in te winnen en aan de rechterkant de dienstverlener die een dienst gaat leveren aan de burger.

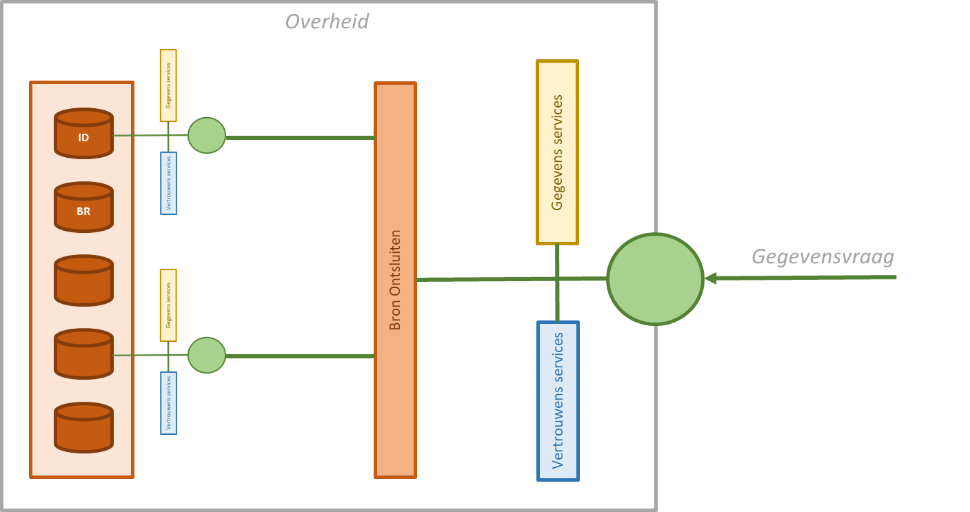
Zowel burger als dienstverlener kan hierbij:

* gebruik maken van een apparaat onafhankelijke toepassing (desktop/laptop/tablet/smartphone)
* met of zonder opslag (lokaal of in de cloud of geen lokale opslag maar altijd gegevens bij de bron)
* onder licentie gebruik maken van “eigen” software voor regiehandelingen (beschikbaar gesteld door private softwareleveranciers of vanuit de overheid) of
* gebruik maken van een “eigen” intermediair die namens de burger of dienstverlener overeengekomen gegevens- en/of vertrouwensdiensten levert.

Ter illustratie is de beschrijving van één *use case* (als variant op vele mogelijkheden) dan:

De burger logt vanuit zijn eigen Digitale Persoonlijke Omgeving met zijn eigen erkende inlogmiddel in bij de overheid (groene bol) en doet een leesactie op een gegeven in de bron (gele gegevensservice “lezen” i.c.m. rode bronontsluiting op de basisregistratie. Hij controleert het gegeven en besluit dat dit gegeven, voorzien van een waarmerk (blauwe vertrouwensservices e-Handtekening, e-Tijdsstempel, e-ID en e-Zegel) in te winnen (gele gegevensservice verzamelen) en in zijn eigen omgeving in de cloud te plaatsen. Vervolgens levert hij dit gewaarmerkte gegeven aan de dienstverlener.

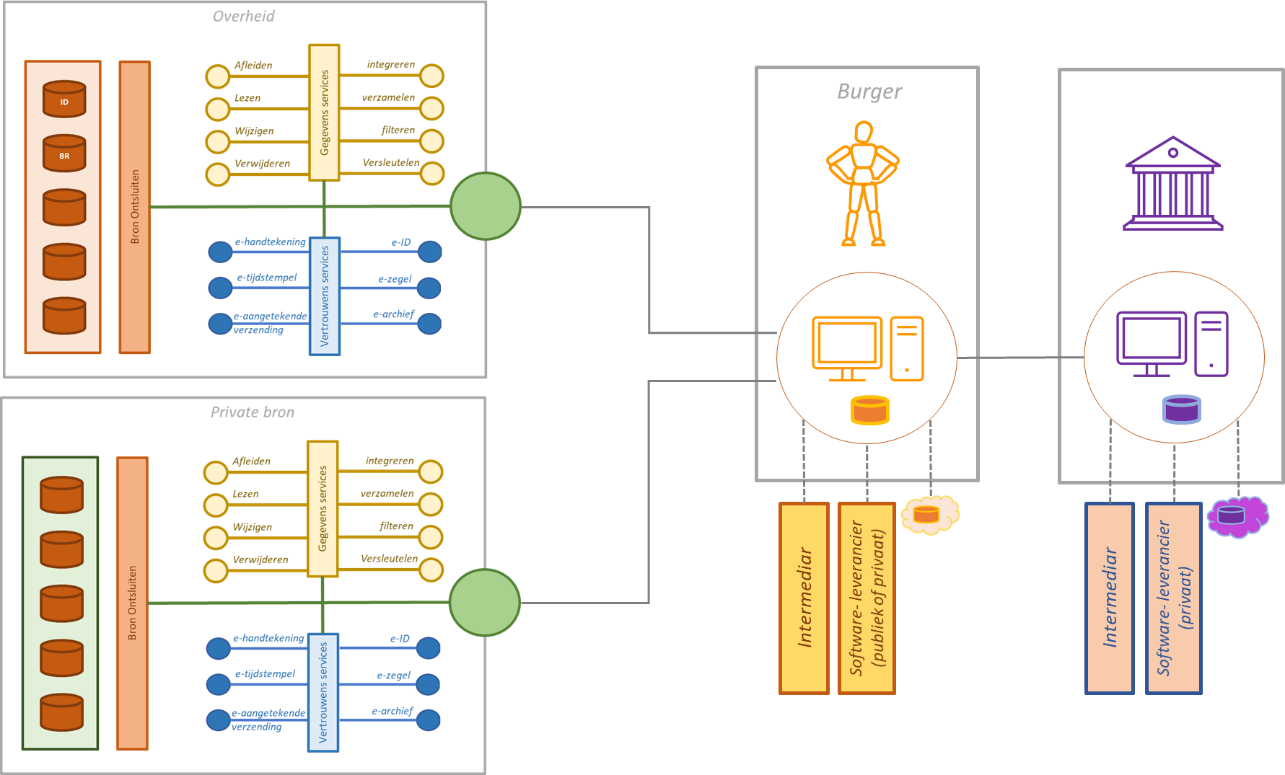
Als ingezoomd wordt op de overheid als bron, dan bestaat die bron uit een hele verzameling van bronnen, vaak verdeeld over net zoveel overheidsorganisaties. Bij het uitvragen van een persoonsgegeven aan een bron ontstaan er twee mogelijkheden:



1. de gegevensvraag wordt gesteld aan het centrale aanspreekpunt (rechter groene stip) en het aanspreekpunt verzamelt bij de bronnen en (indien nodig) bewerkt en/of waarmerkt of
2. de gegevensvrager gaat zelf direct naar de aanspreekpunten van de verschillende bronnen (linker groene stippen) om de gegevens te verzamelen en die iedere bron voor zich (noodzakelijkerwijs) dan bewerkt en/of waarmerkt.

*Op het moment van schrijven (2021) is nog niet vastgesteld wat het voorkeursscenario is.*

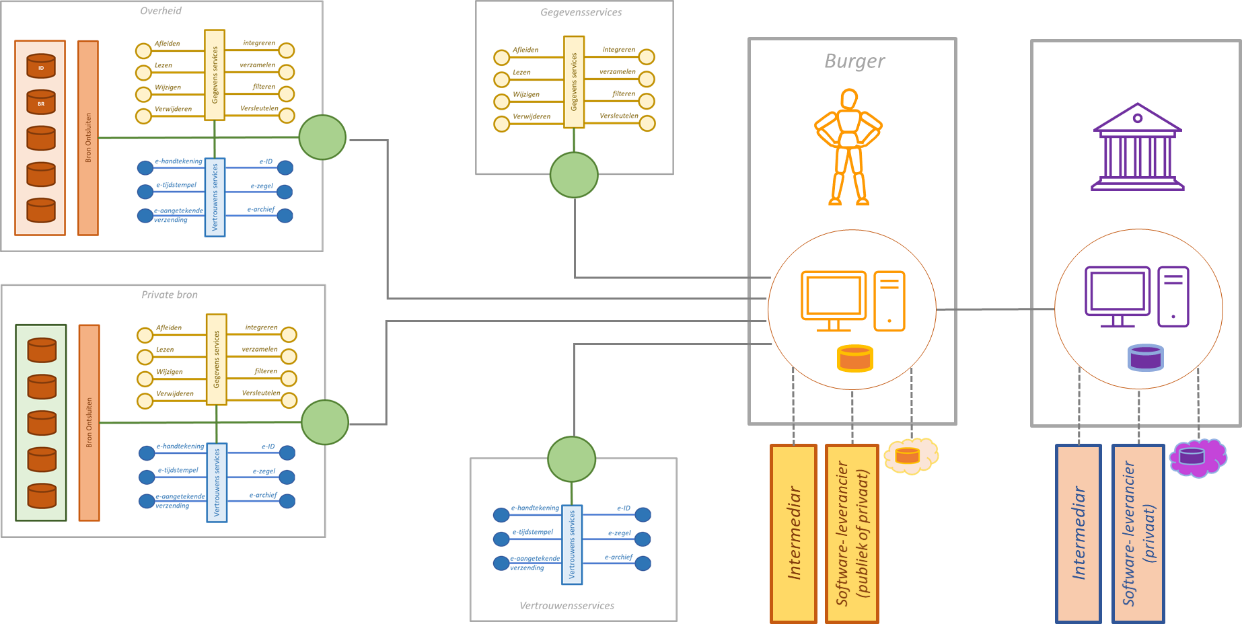
Het bovenstaande model geeft alleen de overheid als bron weer. Vanuit burgerperspectief zal de overheid vaak niet de enige bron zijn vanwaar uit gegevens ingewonnen worden. Ook private bronnen zullen hierin een rol gaan spelen (zoals ze dat nu al vaak doen). De toepassingen die de burger (of in zijn naam de intermediair) zal gaan gebruiken zullen dus zowel gegevens moeten kunnen inwinnen bij bronnen bij de overheid als bronnen bij private partijen. Deze gebruikerswens leidt tot het volgende uitbreiding:



In bovenstaand model zijn zowel de (gele) gegevensservices als de (blauwe) vertrouwensservices opgenomen in het domein van de publieke en de private bron. Dit betekent dat het gegeven of de gegevensset ***voordat*** dit het domein van de overheid of het domein van de private bron verlaat, middels gegevensservices bewerkt kan worden, bijvoorbeeld integratie t.b.v. het aanbrengen van samenhang of afleiding t.b.v. dataminimalisatie in het kader van de bescherming van de privacy.

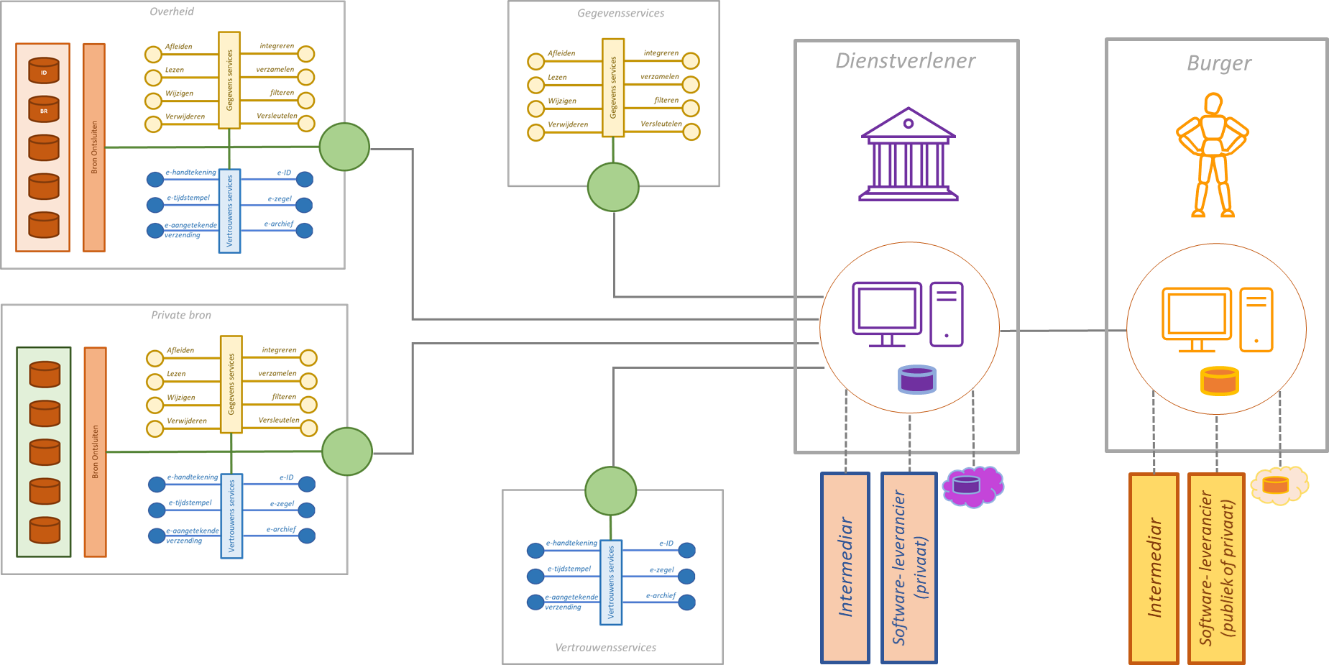
Het ligt voor de hand dat de burger bij het vullen van de concrete informatiepositie gebruik gaat maken van een combinatie van (persoons)gegevens uit zowel publieke als private bronnen (bijvoorbeeld bij het vaststellen van de actuele schuldenpositie) zodat de gegevensservice (bijvoorbeeld integratie of afleiding) moet plaatsvinden ***nadat*** de gegevens het domein van publieke en private bron heeft verlaten.

Als de gegevens bewerkt worden nadat ze het domein van overheid of private partij hebben verlaten, gaat dit zonder aanvullende maatregelen natuurlijk ten koste van het vertrouwen van de dienstverlener in de integriteit van de geleverde gegevens. Hij krijgt immers gegevens aangeleverd waarvan “het zegel verbroken is”. Waarmerken nadat de gegevens bewerkt zijn met behulp van vertrouwensservices zullen daarom in zo’n geval noodzakelijk zijn. Dit leidt tot het volgende aanvulling op het model (waarbij een veelheid aan varianten en combinaties mogelijk is):



## Schets services *Dienstverlener wint in*

Voor het interactiepatroon *Dienstverlener wint in* is zo’n zelfde schets te maken.De betrokken gegevens- en vertrouwensservices zijn in beginsel dezelfde als bij het interactiepatroon *Burger wint in*, alleen speelt hier ook nog het toestemmingsvraagstuk (niet in de figuur opgenomen).



## Persoonlijk digitale omgevingen

In deze referentiearchitectuur wordt gesproken over Persoonlijke digitale omgevingen (PDO). Hiermee wordt gedoeld op iedere digitale oplossing waar een burger (direct of indirect) controle over heeft: het is “zijn omgeving”. Binnen Regie op Gegevens staat het beoogde effect (regie kunnen voeren over de eigen persoonsgegevens) centraal en minder de techniek. Iedere technische oplossing die invulling geeft aan dit beoogde effect, te weten regiehandelingen als inzage, correctie en delen van gegevens, past daarmee binnen de kaders van Regie op Gegevens.

In Europese wetgeving (bijv. eIDAS) wordt gesproken over Europese portemonnees voor digitale identiteit (*e-Wallet)* als technische oplossing voor burgers om regiehandelingen op hun eigen persoonsgegevens te kunnen uitvoeren. In de markt is het gebruikelijk geworden om te spreken over een Personal Data Management dienst (regiehandelingen) met bijbehorende PDM-oplossing. Hiervan zijn er inmiddels vele tientallen beschikbaar, die alle regiehandelingen door de burger mogelijk maken. Overzichten zijn bijvoorbeeld te vinden [hier](https://rog.pleio.nl/file/download/e15c1743-8ebe-41e0-ac43-4de178fb5897/pdm-landschap-2020-regie-op-gegevens-in-nederland3.pdf) (Innovalor) en [hier](https://www.sivi.org/wp-content/uploads/2021/08/PDM-Monitor-Hoofdtekst-1-augustus-2021.pdf) (SIVI).

## Europese portemonnee voor digitale identiteit

In het voorgesteld (dus nog niet vastgesteld) [amendement op de eIDAS-verordening](https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0281) wordt het idee van een *European Digital Identity Wallet* als oplossingsrichting van de in de [evaluatie](https://ec.europa.eu/newsroom/dae/redirection/document/76620) geschetste problemen uitgewerkt. In het oog springende noties in relatie tot Regie op Gegevens en PDM-oplossingen zijn:

1. **Uitgifte portemonnee** (Artikel 6 bis onder 2)

Europese portemonnees voor digitale identiteit worden uitgegeven:

(a) door een lidstaat;

(b) krachtens een mandaat van een lidstaat;

(c) onafhankelijk, maar erkend door een lidstaat.

1. **Functionaliteit** (Artikel 6 bis onder 3)

Met een Europese portemonnee voor digitale identiteit kunnen gebruikers:

(a) op een transparante en door de gebruiker traceerbare wijze veilig de nodige wettelijke persoonsidentificatiegegevens en elektronische attesteringen van attributen aanvragen, verkrijgen, opslaan, selecteren, combineren en delen, zodat zij zich online en offline kunnen authenticeren om openbare en particuliere onlinediensten te gebruiken;

(b) middels gekwalificeerde elektronische handtekeningen ondertekenen.

1. **Eisen aan de portemonnee (**Artikel 6 bis onder 4)

Portemonnees voor digitale identiteit zullen in het bijzonder:

(a) een gemeenschappelijke interface bieden:

1. voor gekwalificeerde en niet-gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde en niet-gekwalificeerde attesteringen van attributen of andere gekwalificeerde en niet-gekwalificeerde certificaten uitgeven met het oog op de afgifte van dergelijke attesteringen en certificaten aan de Europese portemonnee voor digitale identiteit;
2. voor vertrouwende partijen om persoonsidentificatiegegevens en elektronische attesteringen van attributen aan te vragen en te valideren;
3. om lokaal en zonder internettoegang voor de portemonnee, persoonsidentificatiegegevens, elektronische attestering van attributen of andere gegevens, zoals inloggegevens, aan vertrouwende partijen aan te bieden;
4. voor de gebruiker om met de Europese portemonnee voor digitale identiteit te kunnen communiceren en een “EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit” te kunnen weergeven;

(b) waarborgen dat verleners van vertrouwensdiensten van gekwalificeerde attesteringen van attributen geen informatie over het gebruik van die attributen kunnen ontvangen;

(c) aan de voorwaarden van artikel 8 voldoen wat het betrouwbaarheidsniveau “hoog” betreft, met name betreffende de vereisten voor het bewijzen en verifiëren van identiteit, en het beheer en de authenticatie van elektronische identificatiemiddelen;

(d) een mechanisme bieden waarmee de vertrouwende partij de gebruiker kan authenticeren en elektronische attesteringen van attributen kan ontvangen;

(e) waarborgen dat de in artikel 12, lid 4, punt d), bedoelde persoonsidentificatiegegevens uniek en permanent de daarmee verbonden natuurlijke of rechtspersonen vertegenwoordigen.

1. **Validatie van de inhoud** (Artikel 6 bis onder 5)

De lidstaten voorzien valideringsmechanismen voor de Europese portemonnees voor digitale identiteit, zodat:

(a) de authenticiteit en de geldigheid ervan kunnen worden geverifieerd;

(b) de vertrouwende partijen kunnen verifiëren dat de attesteringen van attributen geldig zijn;

(c) de vertrouwende partijen en gekwalificeerde verleners van vertrouwensdiensten de authenticiteit en de geldigheid van gekoppelde persoonsidentificatiegegevens kunnen verifiëren.

1. **Stelsel van elektronische identificatie** (Artikel 6 bis onder 6)

De Europese portemonnees voor digitale identiteit worden uitgegeven op grond van een aangemeld stelsel voor elektronische identificatie met een “hoog” betrouwbaarheidsniveau. Het gebruik van Europese portemonnees voor digitale identiteit is gratis voor natuurlijke personen.

1. **Eisen aan leverancier van portemonnee** (Artikel 6 bis onder 7)

De gebruiker heeft volledige controle over de Europese portemonnee voor digitale identiteit. De afgever van de Europese portemonnee voor digitale identiteit verzamelt geen informatie over het gebruik van de portemonnee die niet noodzakelijk is voor de levering van de portemonneediensten, noch combineert hij persoonsidentificatiegegevens en andere persoonsgegevens die zijn opgeslagen of betrekking hebben op het gebruik van de Europese portemonnee voor digitale identiteit met persoonsgegevens van andere door deze afgever of derden aangeboden diensten als die niet noodzakelijk zijn voor de levering van de portemonneediensten, tenzij de gebruiker daar uitdrukkelijk om heeft gevraagd. Persoonsgegevens met betrekking tot de verstrekking van de Europese portemonnees voor digitale identiteit worden fysiek en logisch gescheiden van andere opgeslagen gegevens. Indien de Europese portemonnee voor digitale identiteit wordt verstrekt door particuliere partijen overeenkomstig lid 2, punten b) en c), is artikel 45 septies, lid 4, van overeenkomstige toepassing.

# Infrastructuur

Het is van belang om vast te stellen dat de doelstelling van Regie op Gegevens met bestaande technische middelen en procedures (wellicht niet altijd even efficiënt) gerealiseerd kunnen worden en gebeurt dan ook al. Gegevensuitwisseling via een email met een gewaarmerkte pdf is natuurlijk al lang mogelijk. Berichten met gegevens erin uitwisselen via SOAP met een XML-bericht over een beveiligde internetverbinding ook. Van meer recente datum (binnen de overheid) is gegevensuitwisseling over een beveiligde internetverbinding middels RESTful API’s in JSON-formaat (of andere). De [Nederlandse API-strategie](https://geonovum.github.io/KP-APIs/API-strategie-algemeen/#architectuur) voorziet in overheidsbreed ontwerp en standaarden.

Uitgangspunt voor het uitwisselen van gegevens binnen de overheid (en deels daarbuiten) is de Generieke Digitale Infrastructuur ([GDI](https://nl.wikipedia.org/wiki/Wet_digitale_overheid)). Deze wordt geborgd in de Wet digitale overheid (Wdo) en bestaat uit standaarden, producten en voorzieningen die gezamenlijk gebruikt worden door overheden, publieke organisaties en in een aantal gevallen ook private partijen. De GDI bestaat uit herbruikbare digitale basisvoorzieningen, standaarden en producten. Hierdoor is het mogelijk om primaire processen doelmatig in te richten en te blijven ontwikkelen. De GDI vormt een dynamisch geheel dat in de toekomst – op basis van technologische ontwikkelingen of nieuwe inzichten – gewijzigd kan worden door het toevoegen van nieuwe generieke voorzieningen (of functionaliteiten van een voorziening) of door het uitfaseren van bestaande generieke voorzieningen.

De voorzieningen in de huidige GDI zijn ondergebracht in vier clusters. Elk cluster heeft een eigen functie:

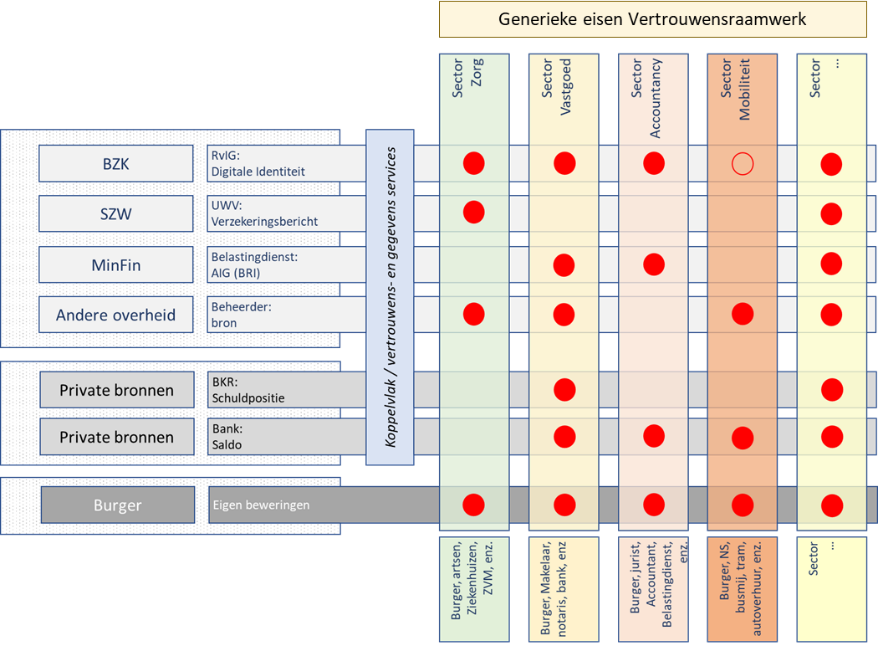
1. digitale identificatie en authenticatie (bv. eHerkenning en DigiD);
2. gegevens (basisregistraties en de bijbehorende stelselvoorzieningen);
3. interconnectiviteit (bv. netwerken en koppelstandaarden); en
4. dienstverlening (bv. het digitaal ondernemersplein en de berichtenbox).

De GDI vormt uiteindelijk geen op zichzelf staand geheel en maakt deel uit van een meer omvattende digitale nationale, Europese en zelfs deels mondiale infrastructuur, bestaande uit een ecosysteem van technologieën, protocollen, hardware, software en content.

# Governance: vertrouwensraamwerk

In de inleiding is al gesteld dat, om de doelstellingen van Regie op Gegevens te realiseren, in de toekomstige oplossing twee fasen te onderkennen zijn, te weten:

1. ontsluiten (ter beschikking stellen) van de persoonsgegevens aan burgers (of met volmacht aan dienstverleners) uit bronnen van de overheid, eventueel met gebruik making van gegevensservices en vertrouwensservices;
2. gebruik van deze persoonsgegevens door burgers in hun relatie met dienstverleners (dus nadat ze door de overheid ter beschikking gesteld zijn).

In de tweede fase is de overheid partij in een in een samenwerking tussen publieke en private partijenwaarin de overheidsbron een van de bronnen is binnen de sectorale samenwerking. Burgers, dienstverleners, publieke bronhouders, private bronhouders en diverse intermediairs zullen tot samenwerking moeten komen. Dit zal enerzijds plaatsvinden op basis van wettelijke kaders en verplichtingen en anderzijds binnen de vrije onderhandelingsruimte van partijen vallen. Doel is in ieder geval tot een vorm van samenwerking te komen waarin partijen elkaar kunnen vertrouwen: een vertrouwensraamwerk.

Een *Trust Framework* ('Vertrouwensraamwerk') is een algemene term die vaak wordt gebruikt om:

1. een juridisch afdwingbare reeks specificaties, regels en overeenkomsten te beschrijven die
2. een meerpartijenstelsel regelen dat is opgezet voor een gemeenschappelijk doel,
3. ontworpen voor het uitvoeren van specifieke transacties tussen een groep van deelnemers,
4. en gebonden aan een gemeenschappelijke reeks vereisten.

Voorbeelden van systemen met meerdere partijen die vertrouwensraamwerk gebruiken, zijn onder meer creditcardsystemen (zoals Visa of MasterCard), elektronische betalingssystemen (zoals SWIFT of NA-CHA), het domeinnaamregistratiesysteem (ICANN) en identiteitssystemen.

Een vertrouwensraamwerk bestaat dus uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en zorgaanbieders op een veilige en efficiënte manier kunnen samenwerken. Partijen die deelnemen committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken. Een canvas voor zo’n vertrouwensraamwerk voor het delen van gegevens is uitgewerkt in [Data Sharing Canvas](https://datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf). Binnen Regie op Gegevens wordt het vertrouwensraamwerk uitgewerkt in het *Vertrouwensraamwerk Regie op Gegevens*.