Kader voor regie op gegevens 0.1

een voorstudie voor een kader voor regie op gegevens

REGIE OP GEGEVENS
Zelf geregeld, veilig en betrouwbaar!

Colofon

Uitgegeven door	Programma Regie op Gegevens
Informatie	regieopgegevens@ictu.nl
Uitgevoerd door	Programma Regie op Gegevens
Datum	Maart 2019
Status	Definitief

Voorwoord

Een van de speerpunten van het kabinet is om mensen meer regie op hun gegevens te geven, door inzage in die gegevens, door inzage in het gebruik daarvan, door de mogelijkheid van correctie, en door deze te kunnen delen met derden. Een ambitie die ook terugkomt in de kabinetsbrede Nederlandse Digitaliseringsstrategie en de agenda NL DIGIbeter voor de overheid zoals die beiden in de zomer van 2018 gepresenteerd zijn. Raymond Knops, de staatssecretaris van BZK, zal nog voor de zomer hierover een kabinetsvisie aan de Tweede Kamer sturen.

Het programma Regie op Gegevens levert hier een bijdrage aan en focust op invulling geven aan gegevensdeling tussen het publieke en het (semi)private domein onder regie van de mens zelf. Het delen van gegevens is in ontwikkeling, maar er is nog geen antwoord op een aantal generieke vraagstukken zoals de interoperabiliteit tussen verschillende stelsels, randvoorwaarden en afspraken voor vertrouwen in het delen van deze gegevens. Deze afspraken en randvoorwaarden zijn noodzakelijk om te komen tot een zogenaamde 'vertrouwens-infrastructuur'.

Een van de strategische doelen van het programma is om in samenwerking met overheden, private en maatschappelijke organisaties, te werken aan deze vertrouwens-infrastructuur om hergebruik van gegevens mogelijk te maken.
Met deze voorstudie willen we een basis leggen voor een gemeenschappelijke taal. Het is een denkkader om vanuit hier tot een verdere inhoudelijke uitwerking te komen en is tot stand gekomen met de inzet van verschillende publieke en private partijen.

Op dit moment ontstaan er verschillende afsprakenstelsels en concrete oplossingen om individuen en bedrijven te ondersteunen bij het hebben van regie op hun persoonlijke gegevens. Deze afsprakenstelsels en -implementaties zullen (cross-)sectoraal ontstaan of op een specifiek thema of specifieke plek/toepassing. Voorbeelden daarvan zijn MedMij (VWS), EduMij (OCW), MaaS (IenW), de vernieuwingen in het gegevenslandschap bij SZW of voor MKB-ers vanuit EZK. Deze oplossingen zullen naar verwachting ook naast elkaar bestaan.

Gezamenlijke, niet-vrijblijvende kaders moeten uiteindelijk zorgen voor een adequate juridische basis, heldere eisen ten aanzien van privacy en veiligheid, voldoende mate van uniformiteit in de gebruikersbeleving en interoperabiliteit tussen de stelsels en implementaties onderling. Dit uitlijnen van de kaders gebeurt op hoofdlijnen: (domein)specifieke invulling zal geschieden door de sectoren zelf.
De aanpak van de ontwikkeling van het kader is erop gericht om verschillende relevante partijen (publiek en privaat) te betrekken, via het opstarten van een werkgroepentraject met belanghebbenden. Dit werkgroepentraject zal in het voorjaar van 2019 van start gaan.
Deze voorstudie markeert daarmee ook de overgang van het programma Regie op Gegevens van stimulerend en verkennend, naar ook meer faciliterend en richtinggevend om te komen tot een kader voor regie op gegevens.

REGIE OP GEGEVENS
Zelf geregeld, veilig en betrouwbaar!

Inhoudsopgave

Managementsamenvatting

Regie op gegevens

Regie op gegevens als principe maakt onderdeel uit van het regeerakkoord, de digitaliseringsstrategie 'Nederland Digitaal' en de digitale agenda 'NLDIGIbeter'. Dit principe geeft mensen de mogelijkheid om hun (persoonlijke) gegevens te gebruiken om hun leven, werk of bedrijf te organiseren, terwijl belangrijke waarden als veiligheid en privacy geborgd zijn. Met de mens ook digitaal in het middelpunt, wordt maatwerk in dienstverlening mogelijk, over de grenzen van publiek en privaat heen.

Regie geeft personen, teneinde hun informatiepositie in het dienstverlenende proces te versterken, de mogelijkheid voor de volgende *regiehandelingen*:

- *Inzien*: iedere persoon heeft in beginsel het recht om bij iedere organisatie die gegevens over hem of haar registreert die gegevens in te zien.
- *Veranderen*: iedere persoon heeft het recht om organisaties te verzoeken gegevens te wijzigen, de verwerking daarvan te beperken of te verwijderen.
- *Delen*: iedere persoon heeft in de regel het recht zelf te bepalen wie gebruik mag maken van zijn of haar gegevens en voor welk doel. Daarnaast heeft ieder persoon het recht om aan te geven wie gegevens mag inzien en aan wie de gegevens mogen worden verzonden.[1]

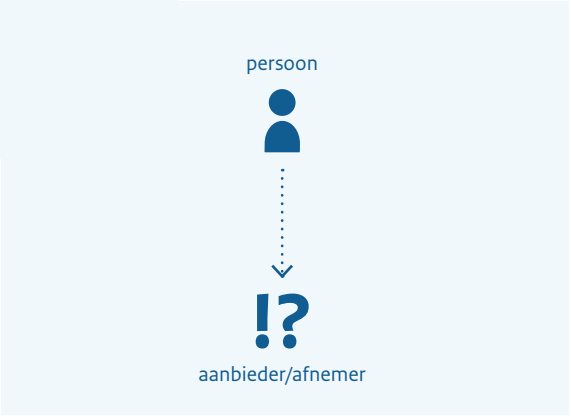
Inzien en veranderen (ook wel corrigeren genoemd) oefen je als persoon op dit moment vaak uit ten opzichte van één enkele organisatie, al dan niet ondersteund door een generieke voorziening (zie figuur 1). Het delen van gegevens gaat per definitie over 'verkeer van gegevens'. Over je gegevens opvragen bij een organisatie en delen met een andere organisatie.
Of over een organisatie toestemming geven om een gegeven van/over jou op te vragen bij een andere organisatie. Het inrichten van dit verkeer is niet als individuele organisatie te regelen, maar vergt onderlinge afspraken tussen aanbieders en afnemers van gegevens, waarbij de persoon centraal staat.

Doel van het kader voor regie op gegevens (RoG)

Op dit moment ontstaan er verschillende afsprakenstelsels en concrete oplossingen om individuen en bedrijven te ondersteunen bij het managen van hun persoonlijke gegevens.
Deze RoG-afsprakenstelsels en RoG-implementaties zullen (cross-)sectoraal ontstaan of op een specifiek thema of specifieke plek/toepassing. Deze oplossingen zullen naar verwachting ook naast elkaar bestaan.

Datadelen is in ontwikkeling, maar er is nog geen antwoord op een aantal generieke vraagstukken zoals de interoperabiliteit tussen verschillende stelsels, randvoorwaarden en afspraken voor vertrouwen in datadelen. Deze afspraken en randvoorwaarden vormen met elkaar een '*vertrouwens-infrastructuur*' en worden beschreven in het kader voor regie op gegevens.

Het doel van het kader voor regie op gegevens, is het zorgdragen dat mensen (en organisaties) met RoG-stelsels en toepassingen kunnen gaan (samen)werken, omdat het voor iedereen navolgbaar is – dankzij de gezamenlijke normen en eisen – dat er veilig en betrouwbaar met gegevens wordt omgegaan.



Figuur 1. *Inzage en correctie ingericht binnen een organisatie*

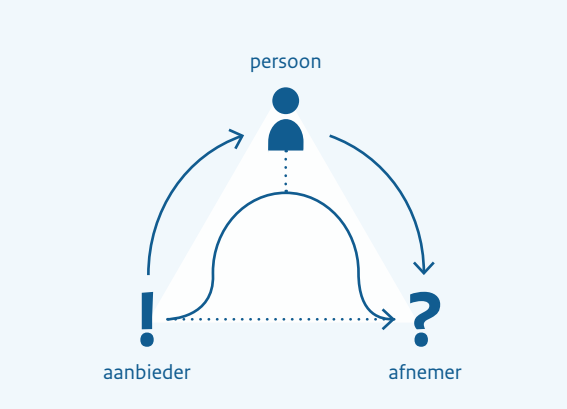
1 Daarmee dus dat de gebruikte gegevensvorm interoperabel is.

Bij de totstandkoming van het kader voor regie op gegevens wordt uitgegaan van een iteratief en dynamisch proces, waarbij reeds bestaande afsprakenstelsels en gegevensdiensten tegelijkertijd zowel input leveren aan het ontwikkelen en verfijnen van de kaders, dan wel dat zij erdoor begeleid worden in hun verdere ontwikkeling.

Dit document is de voorstudie voor een 'Kader voor regie op gegevens, versie 0.1.' Het is een voorstel hoe een kader voor regie op gegevens in opzet en uitgangspunten eruit ziet. Het presenteren van deze voorstudie is een nadrukkelijke uitnodiging om deel te nemen aan een brede discussie, op meerdere niveaus, teneinde te komen tot een breed gedragen kader in 2019.

Regie op gegevens: het denkraam

Om te komen tot basis afspraken en randvoorwaarden is een gemeenschappelijke taal nodig, die in dit document wordt ontwikkeld. Daarvoor wordt een denkraam geïntroduceerd voor datamanagement waaronder de eerdergenoemde '*Regiehandelingen*'. Daarnaast de '*Regiedriehoek*' (zie figuur 2) met daarin drie primaire rollen die zijn betrokken in regie op gegevens: *aanbieders* en *afnemers* van persoonlijke gegevens, en de *persoon* waarop die gegevens betrekking hebben. Tot slot is een viertal '*regiemodellen*' onderscheiden om



Figuur 2. *Verkeer van gegevens onder regie*

vorm te geven aan de verschillende uitwerkingsmogelijkheden van de regiehandelingen. Zij verschillen in de aard en de kracht van de regiehandelingen die de persoon kan uitoefenen, in de ruimte die aan de persoon wordt geboden en in de aard van de zorg voor zijn/haar informatie die aan de persoon wordt toevertrouwd.

Principes voor regie op gegevens

Voor het verder uitwerken van het kader voor regie op gegevens is het van belang om gezamenlijk de principes vast te stellen waar de uitwerking van het kader aan getoetst kan worden. In een aantal werksessie is tot de volgende hoofd- en inrichtingsprincipes gekomen.

De hoofdprincipes:

- *Mens Centraal*: door mensen de mogelijkheid te bieden om regie op hun eigen persoonlijke gegevens te hebben, krijgen zij meer grip op hun persoonlijk leven.
- *Digitale autonomie*: door vergroting van inzicht in – en invloed op – persoonlijk gegevensverkeer, verstevigen personen hun positie ten opzichte van aanbieders en afnemers. Deze ontwikkelingen op het gebied van digitale zelfbeschikking van mensen vragen erom in goede banen te worden geleid.
- *Inclusiviteit*: regie op gegevens kan en moet eraan bijdragen dat zoveel mogelijk mensen vrijelijk deelnemen aan het (digitale) maatschappelijke leven, met al hun persoonlijke verschillen in mogelijkheden, omstandigheden en culturen.

De inrichtingsprincipes:

- *Vertrouwen:* afsprakenstelsels voor, en implementaties van regie op gegevens vergroten het vertrouwen van personen, aanbieders en afnemers, in regie op gegevens.
- *Transparantie:* personen, aanbieders en aanvragers zijn open en eerlijk over hun intenties en gedrag in regie op gegevens.
- *Interoperabiliteit:* afsprakenstelsels voor, en

implementaties van regie op gegevens borgen de koppelbaarheid tussen de diensten en gegevens van betrokken personen, aanbieders en afnemers.
- *Dataminimalisatie*: afsprakenstelsels voor – en implementaties van – regie op gegevens, zorgen voor uitwisselingen van persoonlijke gegevens, die passend zijn bij de behoefte van de persoon, en de vraag van de afnemer.

Bouwstenen voor het kader voor regie op gegevens

In deze eerste opzet voor een kader van regie op gegevens is een onderverdeling gemaakt in vier lijnen waarlangs het kader verder wordt uitgewerkt:
- Juridische kaders, waarbij in deze versie een analyse is gemaakt van de AVG op het concept van Regie op Gegevens;
- Functionele kaders, met als belangrijkste bouwblokken de rollen, functionaliteiten, interactiemodel en compliance maatregelen;
- Technische kaders, met als bouwblokken bericht- en datastandaarden, identity en acces management (identificatie, authenticatie en autorisatie), integratie/connectiviteit, metadata en beveiliging;
- Organisatorisch en operationeel kader, dat verder wordt uitgewerkt in 2019.

De functionele en technische kaders bestaan uit richtinggevende uitspraken (statement) en een beschrijving waarom dit statement is opgesteld (rationale). In deze versie van het kader voor RoG zijn geen concrete invullingen gegeven van deze bouwstenen, omdat deze versie van het kader een duiding geeft van de in te vullen bouwstenen. Verdere uitwerking zal gebeuren met input vanuit de diverse stakeholders uit de publieke en private sector.

In het kader voor regie op gegevens worden geen nieuwe standaarden en/of kaders opgesteld, en wordt afgestemd met bestaande (overheids)-programma's c.q. bouwstenen.

1 Inleiding

In deze inleiding staan we stil bij het principe 'regie op je gegevens hebben', de praktische toepassing ervan in de praktijk: 'regie op gegevens', de context, ontwikkelingen en visie die we in dit verband zien. Vervolgens verbinden we dit aan het doel van het opstellen van een kader voor regie op gegevens en de eerste opzet hiervan in de voorliggende 0.1 versie van een kader voor regie op gegevens.

Regie op gegevens als principe maakt onderdeel uit van het regeerakkoord, de digitaliserings-strategie 'Nederland Digitaal' en de digitale agenda 'NLDIGIbeter'.

1.1 Wat is 'Regie op je gegevens hebben'

Het delen van persoonlijke gegevens[2] is op zichzelf geen nieuw concept. Er zijn legio voorbeelden te noemen van situaties waarin mensen gegevens delen om zaken te regelen, denk bijvoorbeeld aan het aanvragen van een hypotheek, het regelen van zorg, het regelwerk als er een dierbare overlijdt of zorgen dat alle organisaties waarvan je dat belangrijk vindt weten dat je verhuisd bent. Vaak gaat het dan niet alleen om gegevens die je zelf als persoon aanlevert, maar wil een organisatie een 'gevalideerd' gegeven ontvangen: je moet je identiteit bewijzen, een loonstrookje laten zien of een diploma meesturen.

Nu is het vaak nog zo dat je als persoon een papieren of digitale 'kopie' krijgt als overzicht van welke gegevens een organisatie van je heeft: een afschrift, kopie of gewaarmerkt PDF. Zo'n kopie kun je dan zelf opsturen (per post of digitaal) of uploaden. Het is in heel veel gevallen niet mogelijk om dit soort 'gevalideerde gegevens' vanuit de 'bron-organisatie' digitaal te delen met een organisatie waar je iets mee wilt regelen. Bijvoorbeeld: de inkomensgegevens die je werkgever van je heeft digitaal delen met de bank waar je een hypotheek wilt aanvragen. Je moet de gegevens vaak zelf ophalen of aanvragen bij de organisatie en inleveren bij de ander, en dat kan ook anders.
Ook inzage in wie die gegevens gebruikt (en waarvoor), of het doorgeven van correcties zijn vaak nog niet (handig) digitaal geregeld.

Bij 'regie op je gegevens' gaat het er over dat mensen (persoonlijke) gegevens kunnen gebruiken om hun leven, werk of bedrijf te organiseren, terwijl belangrijke waarden als veiligheid en privacy geborgd zijn. Met de mens ook digitaal in het middelpunt, wordt maatwerk in dienstverlening mogelijk, over de grenzen van publiek en privaat heen.

Als het verkeer van persoonlijke gegevens in de digitale samenleving tegelijk vrij is, betrouwbaar, en veilig voor de mens en zijn leefwereld, verbetert en bevordert dat de digitale dienstverlening en versterkt dat het burgerschap in de informatiesamenleving.

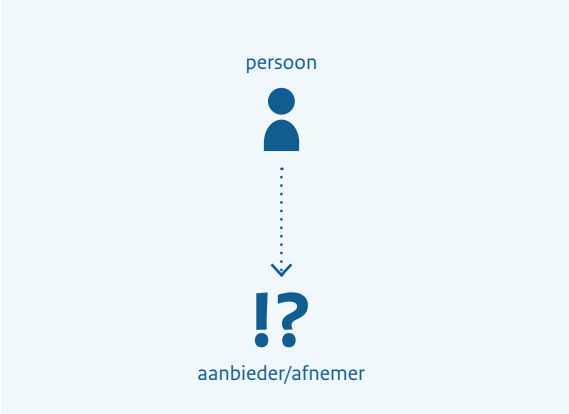
Regiehandelingen

Regie op gegevens is nodig, zodat mensen zelf digitaal zaken kunnen regelen. Veilig en betrouwbaar. Om die reden is het een ambitie van het kabinet. Regie betekent hier personen – teneinde hun informatiepositie in het dienstverlenende proces te versterken – de mogelijkheid te geven voor regiehandelingen:

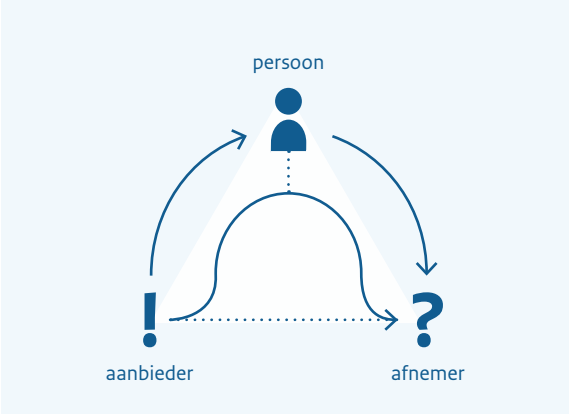
- *Inzien:* iedere persoon heeft in beginsel het recht om bij iedere organisatie die gegevens over hem of haar registreert die gegevens in te zien.
- *Veranderen:* iedere persoon heeft het recht om organisaties te verzoeken gegevens te wijzigen, de verwerking daarvan te beperken of te verwijderen.
- *Delen:* iedere persoon heeft in de regel het recht zelf te bepalen wie gebruik mag maken van zijn of haar gegevens en voor welk doel. Daarnaast heeft iedere persoon het recht om aan te geven wie gegevens mag inzien en aan wie de gegevens mogen worden verzonden.[3]

2 Dit document erkent het onderscheid tussen persoonsgegevens zoals bedoeld in de AVG en bredere sets van persoonlijke gegevens die ook gedeeld kunnen worden. De AVG gaat over het verwerken van persoonsgegevens; 'regie op je gegevens hebben' gaat over persoonlijke gegevens die gebruikt worden. Zie hoofdstuk 4 voor een nadere uitleg.

3 Daarmee dus dat de gebruikte gegevensvorm interoperabel is.



Figuur 3. *Inzage en correctie ingericht binnen een organisatie*



Figuur 4. *Verkeer van gegevens onder regie*

Inzage en veranderen zijn regiehandelingen die je als persoon ten opzichte van een enkele organisatie kan uitoefenen (Figuur 3).

Het delen van gegevens gaat per definitie over 'verkeer van gegevens' (Figuur 4). Over je gegevens opvragen bij een organisatie en delen met een andere organisatie. Of over een organisatie toestemming geven om een gegeven van/over jou op te vragen bij een andere organisatie. Het delen van gegevens tussen de persoon, aanbieder(s) en afnemer(s) is onwerkbaar wanneer elke organisatie dit op een eigen manier regelt. Daarom ontstaan de laatste tijd afsprakenstelsels en implementaties voor regie op gegevens die gezamenlijk afspraken maken over hoe je dit kan organiseren op een manier die zowel voor organisaties als de betreffende persoon gemakkelijk, veilig en efficiënt is.

Als je het kunnen delen van gegevens mogelijk maakt en inricht op basis van gezamenlijke afspraken, dan maak je ook de andere regiehandelingen – inzage en veranderen – mogelijk of makkelijker.

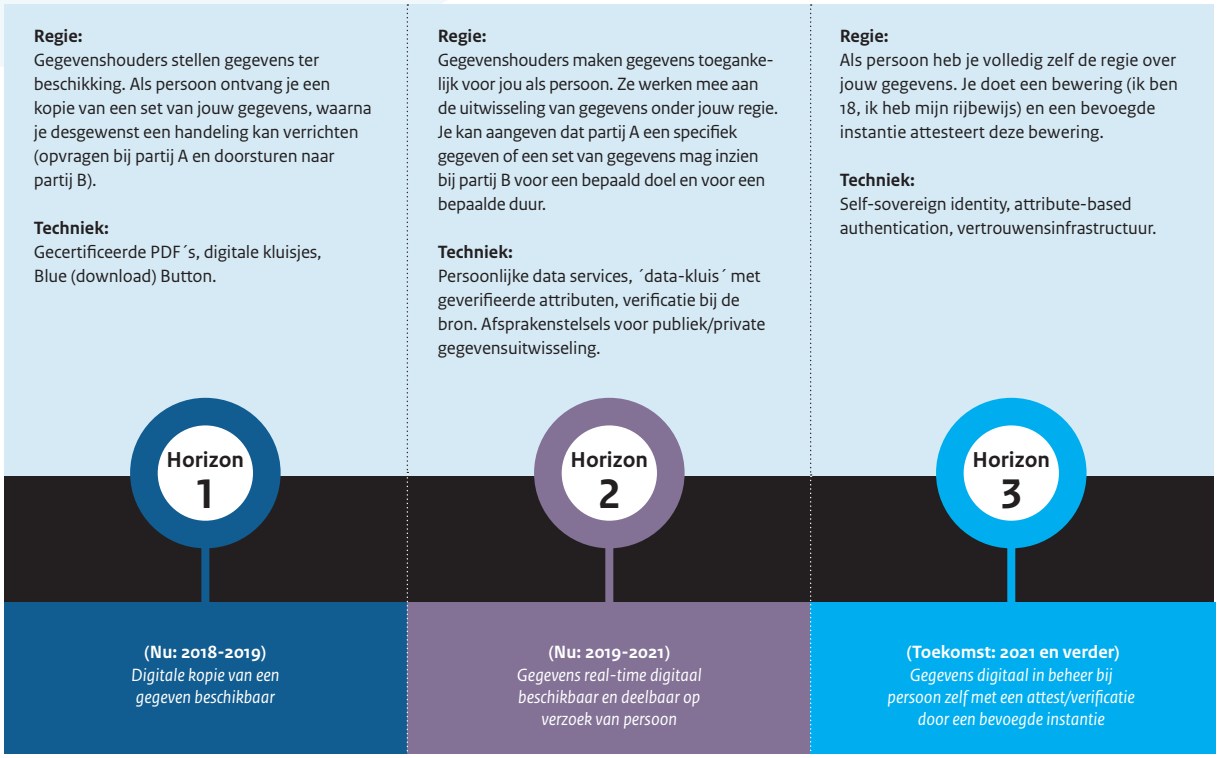
1.2 Visie op de ontwikkeling

Het programma heeft een visie ontwikkeld die drie fasen in de ontwikkeling van het principe 'regie op gegevens' beschrijft. Deze is gebaseerd op '***de 3 horizonnen van innovatie***' (zie Figuur 5).

1. Eerste horizon (2018-2019);
2. Tweede horizon (2018-2021);
3. Derde horizon (2021 en verder).

Kenmerkend aan *horizon 1* is dat organisaties op hun eigen manier enkele persoonlijke gegevens uit hun administraties digitaal ter beschikking stellen op een digitale manier. Als persoon ontvang je een kopie van zo'n set van jouw gegevens, waarna je zelf desgewenst een handeling kan verrichten (opvragen bij partij A en doorsturen naar partij B). Denk hierbij aan gecertificeerde Pdf's, een download knop (Blue Button) of digitale kluisjes.
Op *horizon 2* maken gegevenshouders gegevens uit de bron, digitaal toegankelijk voor personen en andere organisaties. Ze werken mee aan de uitwisseling van gegevens onder de regie van de betreffende persoon. Hierbij kan een persoon aangeven dat partij A een specifiek gegeven of een set van gegevens kan inzien voor een bepaald doel en een bepaalde periode. Hiervoor is een set van afspraken nodig hoe en onder welke voorwaarden partijen gegevens aan personen ter beschikking stellen.

Tot slot is in *horizon 3* de persoon volledig zelf in regie over zijn gegevens. Een persoon doet een bewering (ik ben 18 – of – ik heb een kind gekregen) en een bevoegde instantie kan deze bewering attesteren. Gegevens zijn hierdoor digitaal in beheer bij de



Figuur 5. *Visie op de ontwikkeling: Horizonnen Regie op Gegevens*

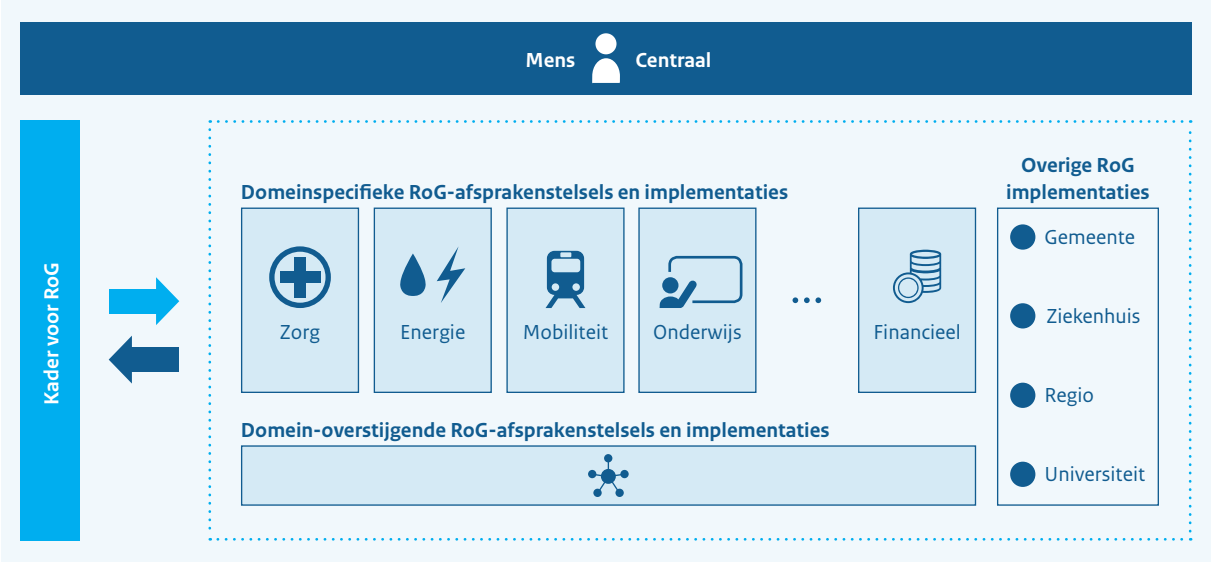
persoon zelf met een attest/verificatie door een bevoegde instantie. Voorbeelden hiervan zijn terug te vinden in self-sovereign identity en attribute-based authentication.
Het 'kader voor regie op gegevens' is primair geschreven voor de regiehandeling 'delen'. Dit delen van gegevens wordt ondersteund door RoG-afsprakenstelsels en implementaties die worden vormgegeven in horizon 2 en 3. Het kader voor regie op gegevens is ondersteunend voor ontwikkelingen op horizon 1 om na te gaan wat nodig is om eventueel door te groeien naar horizon 2 of 3.

1.3 Waarom een kader voor regie op gegevens?

Gezamenlijk afspraken maken zodat mensen regie over hun eigen persoonlijke gegevens kunnen hebben, en het invullen van randvoorwaarden zorgt voor vertrouwen waardoor dienstverlening, samenwerking en handel zich ongehinderd kunnen ontwikkelen, terwijl privacybelangen en digitale rechten beschermd worden. Deze afspraken en randvoorwaarden vormen met elkaar een '*vertrouwensinfrastructuur*' en zijn het doel voor het kader voor regie op gegevens.

Een kader als basis voor diverse RoG-afsprakenstelsels en -implementaties

Op dit moment ontstaan er verschillende afsprakenstelsels en concrete oplossingen om individuen en bedrijven te ondersteunen bij het managen van hun persoonlijke gegevens.
Deze RoG-afsprakenstelsels en -implementaties zullen (cross-)sectoraal ontstaan of op een specifiek thema of specifieke plek/toepassing. Deze oplossingen zullen naar verwachting ook naast elkaar bestaan.



Figuur 6. *Het kader ter ondersteuning van de RoG-afsprakenstelsels en implementaties*

Vragen die in deze context van opkomende RoG-afsprakenstelsels en implementaties regelmatig gesteld worden, zijn:

- Komen persoonlijke gegevens niet in verkeerde handen voor verkeerde doelen?
- Krijgen wel alle personen de beschikking over de nieuwe mogelijkheden?
- Zijn wel alle personen berekend op de taak die hen met deze sterkere rol ten deel valt?
- Hoe kunnen de beheerders-van-oudsher van persoonlijke gegevens de kwaliteit ervan nog beheren, zodat zij hun taken kunnen blijven uitvoeren?
- Wat is het effect van deze versterking van de informatiepositie op de wijze waarop personen zichzelf gaan redden, in vele aspecten van hun leven: qua gezondheid, qua financiën, qua mobiliteit, qua wonen, qua werken?

Het is de bedoeling dat het kader voor regie op gegevens toewerkt naar antwoord op deze vragen, en onzekerheden wegneemt. Als daar aanleiding toe is, kan het kader tevens een aanzet geven tot beleidsvorming, bijvoorbeeld om een gewenste norm een wettelijke basis te geven of om waarborgen te introduceren. Het beoogt ook de verschillende sectorale ontwikkelingen van stelsels door de overheid met elkaar uit te lijnen ten aanzien van visie en uitgangspunten ten aanzien van regie op gegevens.
Daarnaast zijn er verschillende – niet RoG – kaders waar een relatie mee bestaat ten aanzien van het concept van ‘regie op gegevens’. Denk bijvoorbeeld aan wet- en regelgeving inzake privacy en gegevensbescherming, waaronder de Algemene Verordening Gegevensbescherming (AVG), de Wet Digitale Overheid (WDO), de Nederlandse Overheid Referentie Architectuur (NORA), Forum Standaardisatie, ISO 27001, ISO 27002 en de overheidsbrede kenniscommunity ‘Gebruiker Centraal’. Het uitgangspunt is dat er geen nieuwe standaarden en/of kaders opgesteld worden, indien gebruik gemaakt kan worden van bestaande overheidsprogramma’s of bouwstenen.

Kader stimuleert en ondersteunt de ontwikkeling van regie op gegevens

Het kader beoogt een borgende en een stimulerende werking in het veld van RoG-afsprakenstelsels en -implementaties. Daarnaast zorgt een kader voor eenheid, herkenbaarheid van kwaliteit, veiligheid en samenwerkzaamheid (interoperabiliteit). Dit bevordert het vertrouwen en verlaagt de gebruiksdrempel. Bovendien kunnen afsprakenstelsels en implemen-

taties op elkaar gaan voortbouwen en op elkaars schouders gaan staan.

Het kader voor regie op gegevens is géén afsprakenstelsel, maar is een kader dat een basis legt waaraan RoG-afsprakenstelsels en RoG-implementaties zich houden.

1.4 Over dit document: kader voor regie op gegevens 0.1

Dit document is een voorstel hoe een kader voor regie op gegevens in opzet en uitgangspunten er uit ziet. Doel is om op basis van dit document, en een bijbehorend plan van aanpak voor 2019, de route uit te zetten om te komen tot een eerste toepasbare versie van een kader voor regie op gegevens in 2019.

Hierbij wordt uitgegaan van een iteratief en dynamisch proces, waarbij reeds bestaande afsprakenstelsels en gegevensdiensten tegelijkertijd zowel input leveren aan het ontwikkelen en verfijnen van de kaders, dan wel dat zij erdoor begeleid worden in hun verdere ontwikkeling. Het presenteren van deze voorstudie is een nadrukkelijke uitnodiging om deel te nemen aan een brede discussie, op meerdere niveaus, teneinde te komen tot een breed gedragen kader.

Dit document is gebaseerd op een aantal bijeenkomsten die de afgelopen maanden door het programma Regie op Gegevens is georganiseerd met de Community Uniforme Set van Eisen: scrum- en werksessie, designathon, masterclass en een toetsingsbijeenkomst voor een eerste concept 0.1 van het kader voor regie op gegevens. Een aantal voorafgaande documenten is gebruikt als input, zoals het Greenpaper Regie op Gegevens, Analyse afsprakenstelsels en het paper over de uitkomsten van de designathon.

Enkele onderwerpen in dit document worden verduidelijkt aan de hand van een tweetal fictieve casus.

Casus 1: BereikMij

Goed bereikt worden is in ieders belang, via welk kanaal dan ook: fysiek, telefonisch, e-mail, een sociaal medium, een bankrekening. Er kan zelf regie gevoerd worden op adressen, die eventueel voorzien zijn van een authenticiteitsbewijs, van een basisregistratie bijvoorbeeld. Lid worden van een vereniging? Verhuizingen doorgeven? Krant op vakantieadres? Correspondentieadressen op maat? Als persoon kan je het zelf regelen.

Casus 2: HypoThese

Vaak zullen de meeste mensen wel geen hypotheek aanvragen, maar als het gebeurt, is het een hele papierwinkel, met gegevens die uit vele hoeken bij elkaar moet worden gebracht. De hypotheekverstrekker vraagt om gegevens van bijvoorbeeld werkgever, Belastingdienst, pensioenverzekeraar, soms ook van gemeente, DUO of rechtbank. Met HypoThese, een online RoG-dienst voor regie op je woongegevens, kan dat.

1.5 Governance van het kader voor regie op gegevens

Onderdeel van een kader is de governance, zowel ten aanzien van kader voor regie op gegevens zelf, alsook ten aanzien van de criteria waar afsprakenstelsels aan getoetst worden. De uitwerking van de governance voor het kader voor regie op gegevens is in deze 0.1 versie buiten scope gelaten. Dat wordt in de volgende fase opgepakt.

1.6 Opbouw van het document

Dit document is gestart met de context en doel van het kader, relatie met andere kaders en governance van dit document (Hoofdstuk 1). Hoofdstuk 2 gaat in op de belangrijkste principes waarop een 'kader voor regie op gegevens' zich kan baseren.

In hoofdstuk 3 wordt vervolgens ingegaan op 'regie op gegevens' op basis van de 'regiedriehoek'. In hoofdstuk 4 wordt ingegaan op het juridisch kader voor 'regie op gegevens/regie op gegevens'. Hoofdstuk 5 gaat in op de technische, functionele en operationele kaders.

Tenslotte sluit het document af met een bijlage met gehanteerde begrippen.

2 Regie op gegevens: de principes

Mensen willen (persoonlijke) gegevens kunnen gebruiken om hun leven, werk of bedrijf te organiseren, terwijl belangrijke waarden als veiligheid en privacy geborgd zijn. Met de mens ook digitaal in het middelpunt, wordt maatwerk in dienstverlening mogelijk, over de grenzen van publiek en privaat heen.

Zoals in de inleiding is opgemerkt, zorgt gezamenlijk afspraken maken en invullen van relevante randvoorwaarden voor vertrouwen waardoor dienstverlening, samenwerking en handel zich ongehinderd kunnen ontwikkelen, terwijl privacybelangen en digitale rechten beschermd worden. Dit vormt de zogeheten '*vertrouwens-infrastructuur*'. Het is niet handig (of wenselijk) als iedere organisatie zelf gaat verzinnen op welke manier ze dit inrichten en organiseren. Om dit gezamenlijk te regelen, moeten er een aantal gezamenlijke kaders worden afgesproken. Kaders die ervoor zorgen dat personen erop kunnen vertrouwen dat er vertrouwelijk met gegevens wordt omgegaan en dat gegevens op andere plekken herbruikbaar zijn. Kortom, een vertrouwensinfrastructuur waarbij wordt uitgegaan van een aantal belangrijke principes.

Voor het verder uitwerken van het kader voor regie op gegevens is het van belang om gezamenlijk de principes vast te stellen waar de uitwerking van het kader aan getoetst kan worden. In een aantal werksessie is tot de volgende hoofd- en inrichtingsprincipes gekomen.

Een principe is een gezamenlijk gemaakte, fundamentele en richtinggevende uitspraak die herhaaldelijk toegepast kan worden. Principes zijn daarbij generiek, worden zelden gewijzigd. In dit hoofdstuk gaan we uit van een aantal principes die als grondbeginsel dienen. Deze principes zijn ingedeeld in twee categorieën, namelijk: hoofd- en inrichtingsprincipes. De hoofdprincipes:

- Mens centraal;
- Digitale autonomie;
- Inclusiviteit.

De inrichtingsprincipes:
- Vertrouwen;
- Transparantie;
- Interoperabiliteit;
- Dataminimalisatie.

2.1 Hoofdprincipes

Mens centraal

Door mensen de mogelijkheid te bieden om regie op hun eigen persoonlijke gegevens te hebben, krijgen zij meer grip op hun persoonlijk leven. Uitgangspunt is dat het leven van mensen (de 'leefwereld') centraal staat en niet de organisatie-inrichting of systemen (de 'systeemwereld'). Ook worden de informatiestromen waar een persoon regie over kan voeren niet verkaveld in domeinen.

Meer mogelijkheden om regie op je eigen gegevens te voeren, verbetert de grip op het persoonlijke leven. Zo verbetert de regie op iemands huisvestingsinformatie de grip op iemands woonsituatie, verbetert de regie op iemands schuldeninformatie de grip op iemands financiële situatie en verbetert de regie op iemands gezondheidsinformatie de grip op iemands gezondheidssituatie.

Digitale autonomie

Door vergroting van inzicht in – en invloed op – persoonlijk gegevensverkeer, verstevigen personen hun positie ten opzichte van aanbieders en afnemers. Deze ontwikkelingen op het gebied van digitale zelfbeschikking van mensen vragen erom in goede banen te worden geleid.

Een sterkere informatiepositie vergroot de gelijkwaardigheid van mensen ten opzichte van de organisaties waarmee zij te maken hebben. Zo'n gelijkwaardiger informatiepositie is een randvoorwaarde om mensen mee te kunnen laten doen in de samenleving. Om mensen invulling te kunnen geven aan de grotere mate van redzaamheid. Wanneer persoonlijke gegevens vrijer gaan stromen in de regiedriehoek, vraagt vooral de positie van mensen om bescherming tegen ongewenste effecten.

Inclusiviteit
Regie op gegevens kan en moet eraan bijdragen dat zoveel mogelijk mensen vrijelijk deelnemen aan het (digitale) maatschappelijke leven, met al hun persoonlijke verschillen in mogelijkheden, omstandigheden en culturen.

Inclusiviteit wordt versterkt door meerdere interactie- en dienstverleningsconcepten aan te kunnen bieden, door diverse aanbieders. Door persoonlijke gegevens toegankelijk te maken voor personen, kunnen zij kiezen voor specifiek op hun behoeften toegesneden dienstverlening met gebruikmaking van hun persoonlijke gegevens.

Het is onmogelijk om in alle oplossingen vanaf het eerste moment voor volledige inclusiviteit te zorgen, maar waar mogelijk moet inclusiviteit worden nagestreefd.

HypoThese

Het helpt je ook een sociale huurwoning aanvragen, attendeert op bestemmingsplanwijzigingen, toont energieverbruik inzien en helpt bij verlaging daarvan, en nog veel meer. Voor elke woonsituatie biedt HypoThese ondersteuning.

2.2 Inrichtingsprincipes

Vertrouwen
Afsprakenstelsels voor, en implementaties van regie op gegevens vergroten het vertrouwen van personen, aanbieders en afnemers, in regie op gegevens.

Vertrouwen betekent hier de goede bedoelingen van alle actoren en er op rekenen dat ze doen wat ze (toe)zeggen om zo samen te werken en bij te dragen aan het collectief.
Vertrouwen houdt ook in dat de verschillende actoren ervan uit kunnen gaan dat de informatiestroom, veilig, betrouwbaar en juist is. Security-by-design en privacy-by-design dragen ondermeer hieraan bij.

HypoThese

Omdat er bij een hypotheekaanvraag nogal wat hoogstpersoonlijke gegevens nodig zijn, van financiële of andere aard, zijn beveiliging en privacy ingebed in het ontwerp van HypoThese, en mogen alleen organisaties aangesloten zijn op HypoThese als zij hebben aangetoond aan dezelfde hoge standaarden te voldoen.

Transparantie
Personen, aanbieders en afnemers zijn open en eerlijk over hun intenties en gedrag in regie op gegevens.

Iedereen die meedoet in regie op gegevens, in welke rol dan ook, is eerlijk over zijn intenties bij deelname, in de betekenis en de bedoeling van de persoonlijke gegevens waarmee hij omgaat en over welk gebruik hij ervan maakt met inachtneming van welke waarborgen. Het betekent ook dat aanbieders van gegevens kunnen uitleggen in welk verband en op welke wijze de aangeboden gegevens zijn verzameld en verwerkt, zodat de persoon kan weten hoe die

gegevens geïnterpreteerd kunnen worden en waarvoor deze herbruikbaar zijn.

BereikMij

Als iemand een adres voor een specifiek doel deelt met een afnemer, mag dat niet voor andere doelen worden gebruikt, zoals marketing. Als iemand een adres specifiek voor marketingdoeleinden deelt, dan mag dat wel.

Interoperabiliteit
Afsprakenstelsels voor – en implementaties van – regie op gegevens borgen de koppelbaarheid tussen de diensten en gegevens van betrokken personen, aanbieders en afnemers. Waarbij ook tussen domeinen makkelijk informatie, door een persoon, gedeeld kan worden.

Interoperabiliteit verwijst naar de functionaliteit om gegevens uit te wisselen en om het delen van deze gegevens mogelijk te maken. Persoonlijke gegevens moeten tussen verschillende dienstverleners uitgewisseld kunnen worden. Gebruik van een gegeven uit een ander systeem dient conform afspraken te gaan zodat dit mogelijk wordt gemaakt. Interoperabiliteit betekent ook dat vendor lock-in voorkomen kan worden.

Interoperabiliteit speelt vooral een grote rol bij de derde regievorm (zie inleiding, paragraaf 1.1): het delen van gegevens. Het delen van gegevens gaat namelijk per definitie over 'verkeer van gegevens', hiervoor is het kunnen ontvangen/lezen van gegevens door een ander dan de bron-organisatie een vereiste.

BereikMij

Elk kanaal kent zijn eigen gestandaardiseerde adresseringssystematieken en -formaten. Die worden in het afsprakenstelsel 'BereikMij' beheerd en gedeeld. En door alle deelnemers aan dat stelsel gebruikt. Hetzelfde afsprakenstelsel kan ook door aanbieders en afnemers gebruikt worden om hun eigen adressen te beheren en met personen, en elkaar, te delen.

Dataminimalisatie
Afsprakenstelsels voor – en implementaties van – regie op gegevens, zorgen voor uitwisselingen van persoonlijke gegevens, die passend zijn bij de vraag van de afnemer, en de behoefte van de persoon.

Een belangrijke bijdrage aan dataminimalisatie kan worden geleverd als gegevens bij de bron worden ingezien en niet worden gekopieerd (zie ook de horizonnen 2 en 3 in de inleiding). Verder is het belangrijk dat elke uitwisseling slechts dat deel van de gegevens betreft dat echt nodig is voor een specifiek doel. Dataminimalisatie draagt bij aan privacy-by-design[4]. De persoon is niet altijd gebaat bij dataminimalisatie, maar zal ook kunnen streven naar datamaximalisatie voor inzicht in persoonlijke gegevens.

4 Dit houdt in dat bij de ontwikkeling van nieuwe producten en diensten organisaties zo vroeg mogelijk aandacht moeten besteden aan het beschermen van de persoonsgegevens en zo ook aan dataminimalisatie.

3 Regie op gegevens: het model

In dit hoofdstuk staan we stil bij het model voor 'regie op je gegevens hebben'. De rollen in dit model worden beschreven in de 'regiedriehoek'. Vervolgens gaat dit hoofdstuk in op de verschillende regie varianten die binnen het model te onderkennen zijn. In dit hoofdstuk wordt ook aangegeven op welke manier de term 'toestemming' wordt gebruikt in dit document.

3.1 De regiedriehoek

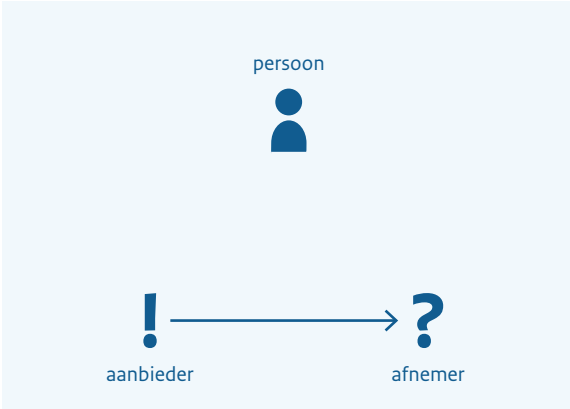
Drie rollen zijn betrokken in regie op gegevens: *aanbieders* en *afnemers* van persoonlijke gegevens, en de *persoon* waarop die gegevens betrekking hebben. Momenteel zijn personen vaak niet of amper betrokken bij het verkeer van hun persoonlijke gegevens van aanbieder naar afnemer, anders dan dat zij er het onderwerp van zijn. Personen zelf ontberen een informatiepositie in het persoonlijk gegevensverkeer. Zij staan aan de zijlijn (zie figuur 7).

Dat is waarin het principe 'regie op je gegevens hebben' verandering brengt. Door personen de mogelijkheid te bieden regiehandelingen uit te voeren op het persoonlijk gegevensverkeer, kunnen zij zich een persoonlijke informatiepositie verwerven en een eigen, gelijkwaardige rol gaan spelen in deze driehoek (zie figuur 8). De persoon wordt aanwezig in de relatie tussen aanbieder en afnemer: de regiedriehoek wordt opgespannen.

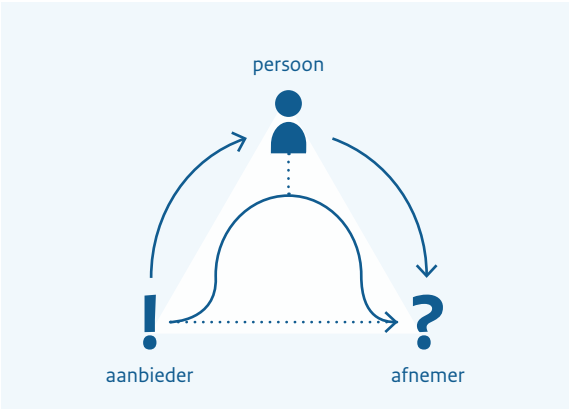
Als soorten regiehandelingen gelden daarbij[5]:

- Inzage hebben in hun persoonlijke gegevens (*Inzien*). Iedere persoon heeft in beginsel het recht om bij iedere organisatie die gegevens over hem of haar registreert die gegevens in te zien.
- Persoonlijke gegevens te veranderen (*Veranderen*). Iedere persoon heeft het recht om organisaties te verzoeken gegevens te wijzigen, de verwerking daarvan te beperken of te verwijderen.
- Persoonlijke gegevens te delen of hergebruiken (*Delen*). Ieder persoon heeft in de regel het recht zelf te bepalen wie gebruik mag maken van zijn of haar gegevens en voor welk doel. Daarnaast heeft ieder persoon het recht om aan te geven wie gegevens mag inzien en aan wie de gegevens mogen worden verzonden.

Door persoonlijke gegevens bij aanbieders voor de betrokken personen te ontsluiten voor hergebruik, ontstaat naast de mogelijkheid om deze gegevens te delen, direct ook een vorm van inzage waaraan een mogelijkheid om persoonlijke gegevens te wijzigen gekoppeld kan worden. Op deze manier verbind je delen, inzage en veranderen integraal met elkaar, op een manier die de huidige plicht van elke overheidsorganisatie om inzage en correctie voor burgers binnen de eigen organisatie in te richten ondersteunt.



Figuur 7. *Persoonlijk gegevensverkeer van aanbieder naar afnemer*



Figuur 8. *Persoonlijke gegevensstromen in de regiedriehoek*

5 Ongeacht of in het hoeverre daartoe in zekere situaties het recht bestaat.

Afhankelijk van de regievariant en de daarbij passende regiehandelingen komt de persoon al dan niet zelf in de persoonlijke gegevensstroom te staan.

De term *afnemer* is gekozen omdat het gaat om de rol die persoonlijke gegevens afneemt, van de persoon of de aanbieder. Vaak is die afnemer op haar beurt een aanbieder van diensten, waarvan de persoon dan de (beoogd) afnemer is. De terminologie is dus gekozen vanuit het perspectief van het persoonlijke gegevensverkeer, niet van de dienst die aanleiding en context is van dat verkeer.

Aanbieders en afnemers kunnen om te beginnen zowel publieke als private organisaties zijn.

Menigmaal zal de aanbieder een overheidsorganisatie zijn die een registratie van persoonlijke gegevens onder haar hoede heeft, maar het kan bijvoorbeeld ook een zorgaanbieder zijn, een private partij, die dossier houdt van persoonlijke gezondheidsgegevens. Het kunnen werkgevers, banken, of het UWV zijn, die persoonlijke financiële gegevens hebben die van belang zijn voor belastingaangifte. Zorgaanbieders kunnen ook afnemer zijn in de regiedriehoek, net als allerlei andere soorten bedrijven.

Kortom, in de regiedriehoek kan persoonlijk gegevensverkeer voorkomen van bijna alle soorten: Tussen overheden, tussen bedrijven, tussen overheid en bedrijf (en omgekeerd), tussen de persoon en (overheids)organisaties.

3.2 Toestemming

Het hoort bij regie op persoonlijke gegevens dat helder is dat de persoon een zekere uitwisseling van persoonlijke gegevens goed vindt: toestemming. Veel persoonlijk gegevensverkeer ten behoeve van overheidsdienstverlening, gebeurt momenteel rechtstreeks van aanbieder naar afnemer, waarbij een (materie)wet typisch de wettelijke verplichting regelt. Het is waarschijnlijk dat deze wijze van gegevensuitwisseling blijft bestaan naast vormen waar burgers meer regie over kunnen hebben. Op andere onderdelen kan die regie echter wel worden aangebracht, of versterkt waar zij er in aanleg al is.

Dit document beperkt zich niet tot één grondslag, en dus ook niet tot alleen toestemming in de zin van de AVG. Elke situatie waarin regiehandelingen door personen op hun persoonlijke gegevensverkeer wenselijk, toegestaan en mogelijk zijn, valt binnen het gezichtsveld van dit document. Wanneer in dit document gesproken wordt over 'toestemming' gaat het over de feitelijke/organisatorische handeling. Wanneer in het document wordt gesproken over toestemming in het kader van de grondslag in de AVG wordt dit nadrukkelijk benoemd als toestemming in het kader van de AVG.

3.3 Varianten van regie

De ene regie is de andere niet. Dit document onderscheidt om te beginnen vier varianten. Zij verschillen in de aard en de kracht van de regiehandelingen die de persoon kan uitoefenen, in de ruimte die aan de persoon worden geboden en in de aard van de zorg voor zijn/haar informatie die aan de persoon wordt toevertrouwd. Steeds speelt toestemming een belangrijke rol.

De vier varianten zijn slechts een eerste fundamentele differentiatie van regiemodellen. Voor elke variant bestaan nog vele verschillende manieren van implementeren. De hoofdrollen in de regiedriehoek – persoon, aanbieder en afnemer – hebben bijvoorbeeld de mogelijkheid om voor de uitvoering van hun eindverantwoordelijkheid in de regiedriehoek andere partijen in de hand te nemen: uitvoerders, onderaannemers, dienstverleners, et cetera. Vaak zullen daaronder de partijen te vinden zijn die de AVG verwerkers zou noemen. Hier zijn zeer vele varianten denkbaar.

Op de eindverantwoordelijkheid van de drie hoofdrollen in de regiedriehoek dingen die evenwel niet af.

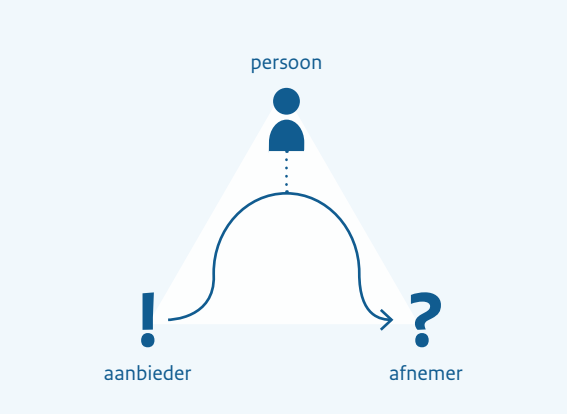
Ook zijn er natuurlijk veel technische varianten mogelijk, hoewel de vier varianten wel elk een eigen karakteristieke familie kennen van technologieën, standaarden en infrastructuren. Op dat punt is binnen de varianten dus beter te standaardiseren dan ertussen. Ook op het gebied van passende governance zijn er belangrijke verschillen tussen de varianten. Hoe dan ook, dit document laat het vooralsnog bij het onderscheid tussen deze vier varianten[6], namelijk:

- De poortwachter-variant;
- De uitgever-variant;
- De eigenaar-variant;
- De auteur-variant.

De poortwachter-variant

In de eerste variant speelt de informatiestroom zich af tussen de onderste twee rollen in de regiedriehoek: van aanbieder naar afnemer. Soms is dat op initiatief van de afnemer, die bepaalde informatie over de persoon nodig heeft voor de (maatschappelijke) dienst die hij levert, soms ook neemt de afnemer het initiatief, omdat deze bijvoorbeeld gehouden is, uit hoofde van zijn wettelijke taak, om de informatie over de persoon aan te bieden aan de afnemer. De persoon staat in deze variant naast de informatiestroom, maar kan er in sommige gevallen wel regiehandelingen op uitvoeren. Daarom heet deze variant de *poortwachter-* of *douanier*-variant. De persoon kan de informatie op zijn minst inzien en mogelijk ook zijn goed- of afkeuring uitspreken over het gebruik van de betreffende informatie door de afnemer[7].

In deze variant is typisch sprake van twee soorten use cases: een pull-use case waarin de afnemer het initiatief neemt om de informatie op te halen en/of een push-use case waarin de aanbieder het



Figuur 9. *Stroom in de poortwachter-variant*

initiatief neemt om de informatie naar de afnemer te brengen. In beide gevallen moet er een rechtsgrond voor dat verkeer zijn. Vaak kan de persoon de stroom wettelijk niet weigeren, soms maakt het verkeer als voorwaarde deel uit van een overeenkomst van de persoon met de afnemer of de aanbieder, soms is ook specifieke toestemming van de persoon nodig. Hoe dan ook, de toestemming[8] van de persoon (ik) betreft steeds het door de aanbieder (jij) ter beschikking stellen van betreffende informatie aan (de verwerker van) de afnemer (hij). De toestemming kan eenmalig zijn, of structureel.

Voorbeelden zijn:

- De Verklaring Omtrent Gedrag die door een afnemer over een persoon wordt aangevraagd bij (meestal) de gemeente, op verzoek van een afnemer;
- De medicatiegegevens die, met toestemming van de patiënt door apotheken met huisartsen worden gedeeld;
- De Vooringevulde Aangifte bij de Belastingdienst, waarvoor financiële gegevens worden betrokken bij banken en overheidsorganisaties (hoewel de huidige regierol van de persoon hierin beperkt is).

6 De vier varianten zijn geïnspireerd op de vier zogenoemde luiken uit: Gegevenslandschap: een Informatievierluik en paragraaf 3.1.4 daarvan in het bijzonder. Op andere plaatsen in dat document is meer te lezen over technologische, organisatorische, juridische en andere aspecten van dit vierluik.

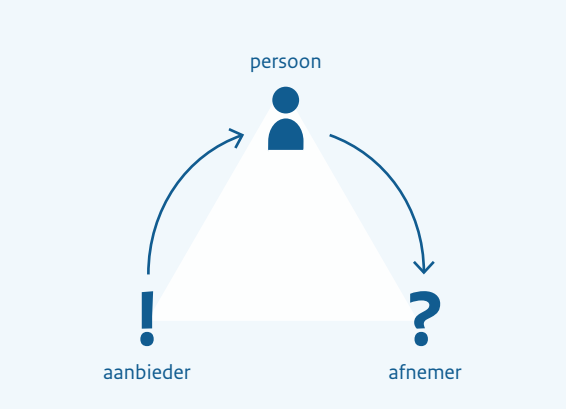
7 Tenzij uitzonderingen zoals bij fraude of veiligheid.

8 Deze term wordt in hoofdstuk 4 verduidelijkt.

De uitgever-variant

De tweede variant gaat verder dan de poortwachter-variant, door het initiatief voor informatieverkeer bij de persoon te leggen. Deze stelt zich op als uitgever van zijn persoonlijke feiten.[9] Die feiten kan hij/zij betrekken bij aanbieders (zijn/haar bronnen) en naar believen ter beschikking stellen aan afnemers (zijn/haar lezers). Het informatieverkeer is daarbij niet inzet van een ruil, maar louter bedoeld om de ander te informeren. De afnemer heeft die kennis nodig voor zijn dienst, maar heeft er daarbuiten geen belang bij. De informatiestroom loopt nu via de persoon, die er daarom ook de nodige zorg voor aan de dag moet leggen. Hij/zij is het die kiest welke persoonlijke feiten worden verzameld bij welke aanbieders en in welke combinaties deze worden gedeeld met welke afnemers.
In de gezondheidszorg is MedMij een actueel voorbeeld van een afsprakenstelsel voor regie op gegevens dat dit model hanteert.

In de uitgever-variant is typisch sprake van een combinatie van twee soorten use cases: een verzamelen-use case waarin de afnemer zijn feiten ophaalt bij een of meer bronnen (de aanbieders) en een delen-use case waarin de persoon aanbieders informeert over zijn persoonlijke feiten. Toestemming zal in dit model zowel voor verzamelen als delen aan de orde zijn, bij het:



Figuur 10. *Stromen in de uitgever-variant*

- Verzamelen betreft de toestemming van de persoon van het door de aanbieder ter beschikking stellen van de betreffende informatie aan de verwerker van de persoon zelf;
- Delen betreft de toestemming van de persoon van het door zijn eigen verwerker (deze term is breder dan verwerker zoals in de AVG) ter beschikking stellen van de betreffende informatie aan de afnemer.

Soms heeft de persoon het wettelijk recht te verzamelen, soms een wettelijke plicht te delen. Soms maakt het verkeer als voorwaarde deel uit van een overeenkomst van de persoon met de afnemer of de aanbieder, soms ook is er specifieke toestemming in het kader van de AVG van de persoon nodig. Steeds kan toestemming eenmalig zijn, maar ook structureel, in de vorm van een abonnement.
In het uitgever-model is het eenvoudig om de aanbieder het zicht te onthouden op wie de afnemer wordt, maar de aanbieder, of het afsprakenstelsel, zou wel beperkingen kunnen opleggen aan de verdere verspreiding van de persoonlijke feiten.

BereikMij

Het BereikMij Afsprakenstelsel is een voorbeeld bij uitstek van de uitgever-variant. Elke persoon, en zelfs elke partij die bereikbaar moet zijn, is de uitgever van zijn eigen adresinformatie. Menigmaal wordt die adresinformatie betrokken van de aanbieder: de partij die een adresseringssystematiek beheert, adressen toekent, of anderszins de authenticiteit van een soort adres kan bewijzen: de BRP voor een BRP-adres, een bank voor een bankrekeningnummer. De persoon informeert een zeer groot en gevarieerd scala aan afnemers over specifieke adressen voor specifieke kanalen.

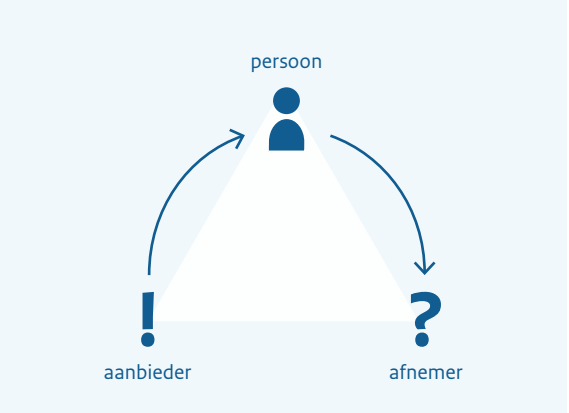
9 Die kunnen vele vormen hebben: gestructureerde gegevens, documenten, et cetera.

Omdat een uitgever geen schrijver is, is de persoon in deze variant niet zomaar de maker van zijn gegevens. Het maakt dus geen deel uit van zijn regiehandelingen om de gegevens te bedenken of aan te passen[10]. Brongetrouwheid van informatie is daarom een belangrijk thema in het uitgevers-model. Daarvoor kunnen maatregelen getroffen worden in het afsprakenstelsel, bijvoorbeeld met waarmerken.

De eigenaar-variant

Ook in de derde variant staat de persoon midden in de informatiestroom, maar in een andere rol dan als uitgever, in een rol zelfs die op gespannen voet staat met de uitgeversrol. In de eigenaar-variant beschouwt de persoon zijn persoonlijke informatie als een asset, als bezit, dat in belangenverhoudingen uitgeruild kan worden. Het initiatief voor informatie-uitwisseling kan nu in elke hoek van de regiedriehoek liggen: een aanbieder kan de informatie tegen een vergoeding aanbieden aan de persoon, maar de persoon kan ook zelf het initiatief tot koop nemen. Een afnemer kan een vergoeding of tegenprestatie bieden voor de persoonlijke informatie, maar de persoon kan ook zelf het initiatief tot verkoop nemen. Hoe dan ook, de informatie-uitwisseling is nu transactioneel van aard, niet informatief, zoals in de uitgever-variant.
Hoewel deze variant niet de eerste is waaraan gedacht wordt in de context van publieke dienstverlening, staat zij hier toch genoemd. Ook publieke organisaties verkopen soms informatie (als aanbieder dus) of zouden aldus verkregen informatie als afnemer kunnen willen gebruiken. Nog belangrijker is echter dat een eventuele verwevenheid tussen de uitgever- en de eigenaar-variant serieuze risico's met zich meebrengt.

In deze variant is sprake van twee soorten use cases: een leveren-use case waarin de persoon de betreffende informatie levert aan de afnemer en/of een afnemen-use case waarin de persoon de betreffende informatie afneemt van de aanbieder. Deze use cases zijn typisch onderdeel van een transactioneel proces,



Figuur 11. *Stromen in de eigenaar-variant*

waarin een contract of een ruil zijn beslag krijgt. De toestemming van de persoon komt typisch tot uitdrukking in de overeenkomst die hij hiervoor met de aanbieder of afnemer sluit, of in de acceptatie door de persoon van de voorwaarden die de aanbieder of afnemer stelt aan zijn ruil met de persoon. Opnieuw kan de toestemming eenmalig zijn of structureel.

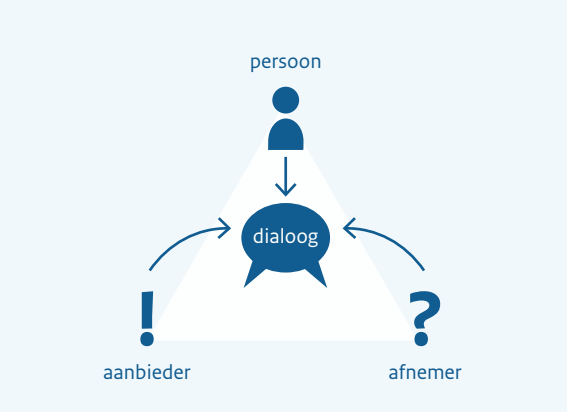
De auteur-variant

De vierde variant is de meest vergaande, die vooralsnog beperkt aan de orde zal zijn. Als vergezicht, gewenst of niet, kan ze echter een goede rol spelen in de ontwikkelingen. Daarom noemen we deze variant kort.
Het is de variant waarin de persoon zelf de inhoud van de informatie (mede)bepaalt, als deelnemer in een dialoog met aanbieders en/of afnemers. Hij/zij kan in die dialoog haar/zijn eigen bedoeling inbrengen, passend bij de specifieke situatie die aan de orde is. Daardoor kan de specifieke leefwereld van de persoon in deze variant het meest tot haar recht komen, in relatie tot de systeemwerelden van aanbieder en afnemer.

Voorbeeld:
De keukentafelgesprekken, zoals die bedoeld zijn in de Wmo, mogen voorlopig dienen als illustratie van zo'n dialoog. Hoewel bij zulke dialogen vooralsnog niet snel aan elektronische middelen wordt gedacht,

10 Zie daarvoor de vierde variant.

is dat wel degelijk mogelijk. Daarvoor zal echter het ontwerp van zulke middelen op andere leest moeten worden geschoeid dan vooralsnog gebruikelijk is[11].



Figuur 12. *Stromen in de auteur-variant*

HypoThese

HypoThese past verschillende regievarianten toe. Voor het aanvragen van een hypotheek kan de gebruiker een eigen hypotheekdossier aanmaken, waarin hij uit zijn persoonlijke gegevens allerlei documenten verzamelt, om daarmee offertes aan te vragen bij een aantal kandidaat-hypotheekverstrekkers. Natuurlijk gebruiken de verstrekkers die gegevens alleen voor het doel van deze specifieke offerte. HypoThese werkt hier in de uitgever-variant. Sommige gegevens mag de kandidaat-hypotheekverstrekker zelf betrekken bij een bron, zoals afschriften van spaarrekeningen bij de bank. Natuurlijk krijgt de HypoThese-gebruiker die gegevens eerst zelf te zien voordat hij toestemming geeft om ze door te zetten naar de kandidaat-hypotheekverstrekker. HypoThese werkt hier in de poortwachter-variant.

11 Zie https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2017/12/Gegevenslandschap-overheid-een-vierluik-van-informatie-Visie-architectuur-ontwikkeling-v1.0.pdf, paragraaf 4.3.

4 Juridisch kader

In dit hoofdstuk staat het juridisch kader om regie op je eigen gegevens te voeren, centraal. Het juridisch kader wordt gevormd door zowel wettelijke kaders als te maken afspraken. Deze wettelijke kaders en afspraken hebben betrekking op acties, te weten: de regieactiviteiten inzage, veranderen en delen (zie paragraaf 3.1); en op het veld, te weten de verschillende rollen van (onder meer) personen, aanbieders en afnemers (zie paragraaf 3.1). De specifieke consumentenrechtelijke bepalingen die gelden bij bepaalde vormen van dienstverlening worden hierna niet besproken, omdat die niet bij iedere vorm van regie op gegevens aan de orde zullen zijn.

Met afspraken wordt gedoeld op de afspraken die moeten worden gemaakt tussen de verschillende rollen. Deze afspraken vormen niet de grondslag voor dienstverlening, maar waarborgen de transparantie, doelmatigheid en veiligheid van de verwerking van persoonlijke gegevens.

De toepasselijke wetten en mogelijke afspraken verschillen per categorie gegevens. Op de verwerking van persoonsgegevens zijn de regels van de AVG van toepassing. Eventuele aanvullende afspraken over het verwerken van persoonsgegevens zullen dan ook steeds in lijn moeten zijn met de AVG en, indien van toepassing, met bijzondere gegevensbeschermingswet- en regelgeving. Op de verwerking van persoonlijke gegevens, voor zover dat niet ook persoonsgegevens zijn, is de AVG niet van toepassing, al kan de AVG wel als inspiratie fungeren bij het maken van afspraken. Alvorens die kaders worden toegelicht, wordt hieronder eerst kort ingegaan op het verschil tussen persoonsgegevens en persoonlijke gegevens.

In deze versie van het kader voor regie op gegevens is met name ingegaan op de betekenis van de AVG voor 'regie op gegevens'. Daarnaast zijn ook andere (generieke) wettelijke kaders van belang om, in het vervolgtraject, te onderzoeken.

4.1 Onderscheid persoonsgegevens en persoonlijke gegevens

Persoonsgegevens is een term afkomstig uit de AVG en betreft, kort gezegd, alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het gaat dan zowel om direct identificeerbare informatie (zoals een naam, identificatienummer of foto) als om indirect identificeerbare informatie (zoals locatiegegevens).

Gegevens over bedrijven of organisaties zullen in veel gevallen niet herleidbaar zijn tot natuurlijke personen en dan dus geen persoonsgegevens zijn. Voorts ziet het persoonsgegevensbegrip alleen op de gegevens over een persoon als zodanig, en niet ook op de drager van die gegevens, zoals een document, of op een geattesteerde bewering.

Zoals in paragraaf 3.2 al is toegelicht, zal bij regie op gegevens een aanvrager niet of niet alleen over persoonsgegevens willen beschikken om een dienst te leveren, maar zeker willen zijn dat een bepaalde bewering over de persoon waar is, bijvoorbeeld door verkrijging van een gewaarmerkt document of door attestatie van een bewering. Daarvoor zijn andere gegevens dan (alleen) persoonsgegevens nodig, zoals documenten of geattesteerde beweringen. Deze andere, aanvullende gegevens worden – samen met persoonsgegevens – aangeduid als "persoonlijke gegevens".

Als voorbeeld kan een diploma worden genomen, waarop staat dat persoon X met geboortedatum Y een masterdiploma in Z heeft behaald. Men zou op drie lagen regie kunnen voeren, te weten:

- De verschillende (persoons)gegevens in het document: de naam, geboortedatum en het gegeven dat persoon X een masterdiploma in Z heeft behaald;
- De geverifieerde/geattesteerde bewering dat persoon X master Z heeft afgerond. Er zijn

Figuur 13. *Persoonsgegevens versus persoonlijke gegevens*

situaties denkbaar waarin een aanbieder niet zozeer persoonsgegevens wil ontvangen om een dienst te leveren, maar er alleen zeker van wil zijn dat de (verder anonieme) afnemer van de dienst is afgestudeerd in een bepaalde richting; of

- Het diploma (het document) als drager van de informatie dat persoon X is afgestudeerd.

Uitgangspunt is dan ook dat regiehandelingen in de regel zien op persoonlijke gegevens, inclusief persoonsgegevens, en niet alleen op persoonsgegevens.

4.2 Juridisch kader voor persoonsgegevens

Bij het voeren van regie zullen vaak (ook) persoonsgegevens worden verwerkt. Bij de verwerking van persoonsgegevens is de AVG leidend. De AVG biedt zowel kaders waarover moet worden nagedacht bij de verwerking van persoonsgegevens als materiële eisen waaraan (in ieder geval) moet worden voldaan. Concreet betekent dat bij regie op gegevens dat de verschillende rollen steeds moeten worden geplot tegen de actoren die de AVG kent. Zo zal een persoon kwalificeren als *betrokkene* en zullen de afnemer en de aanbieder in de regel kwalificeren als *verwerkingsverantwoordelijken*. Een eventuele identiteitsaanbieder en/of identiteitsmakelaar zal veelal kwalificeren als verwerker van de aanbieder of afnemer (zie artikel 4 AVG voor de definities van de verschillende AVG-actoren). Daarmee zal dan ook op grond van artikel 28 AVG een verwerkersovereenkomst moeten worden gesloten.

Overigens zal bij iedere vorm van regie op gegevens ook aan mogelijke andere van toepassing zijnde wet- en regelgeving moeten worden voldaan, zoals de specifieke wetgeving die op bepaalde organisaties van toepassing is. Zo zal een bestuursorgaan steeds ook de Algemene wet bestuursrecht in acht moeten nemen en een bank de Wet op het financieel toezicht.

Voor de regieactiviteiten inzien, veranderen en delen zijn de rechten van betrokkenen uit de AVG relevant. Een persoon kan zijn persoonsgegevens *inzien* door een inzageverzoek op grond van artikel 15 AVG te doen bij de aanbieder of afnemer.

Het inzagerecht van de AVG beperkt zich tot een recht voor een betrokkene om inzage te krijgen in de hem betreffende persoonsgegevens die door een verwerkingsverantwoordelijke worden verwerkt, en omvat niet ook een recht op de documenten/dragers van die persoonsgegevens of op geattesteerde beweringen (artikel 15, eerste en tweede lid, AVG).

Naast het bieden van inzage in de verwerkte persoonsgegevens zal een verwerkingsverantwoordelijke de betrokkene moeten informeren over onder meer de verwerkingsdoeleinden, de

categorieën van persoonsgegevens en de (categorieën van) ontvangers (artikel 15, tweede lid, AVG).

Verder hebben betrokkenen recht op een kopie *van de persoonsgegevens* die worden verwerkt (artikel 15, derde lid, AVG). Bij de honorering van een inzageverzoek *kan* een kopie worden verstrekt van het document dat de drager die de persoonsgegevens bevat (al dan niet met weglakking van de informatie die geen persoonsgegevens bevat). Er kan echter ook een overzicht worden verstrekt dat een kopie van de persoonsgegevens bevat (zie ***Autoriteit Persoonsgegevens***).

Overigens kan inzage door een aanbieder of afnemer worden beperkt of geweigerd in geval een uitzonderingsgrond van artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG zich voordoet, zoals het waarborgen van een taak op het gebied van toezicht.

Het structureel en/of op grote schaal verstrekken van persoonsgegevens door een aanbieder aan of via een betrokkene ten behoeve van regie op gegevens middels het inzagerecht van de AVG, lijkt oneigenlijk gebruik van dit recht. Daarvoor zal veelal een stevigere en specifiekere wettelijke basis nodig zijn.

Overigens kennen sommige domeinen "eigen" inzageregelingen, die zijn opgenomen in bijzondere wetten. Zie bijvoorbeeld de bepalingen in Boek 7 van het Burgerlijk Wetboek inzake de geneeskundige behandeling. Op grond van artikel 7:456 BW moet een hulpverlener een patiënt in beginsel desgevraagd inzage geven in en een afschrift geven van de bescheiden in een patiëntendossier.

Voor het *veranderen* van persoonsgegevens kan een persoon een rectificatieverzoek bij een verwerkingsverantwoordelijke indienen (zie artikel 16 AVG). Ook dat recht kan op grond van artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG worden beperkt of geweigerd.

De AVG heeft als doel de verwerking van persoonsgegevens zodanig te reguleren, dat er geen belemmering meer hoeft te zijn voor het vrije verkeer van persoonsgegevens. Voor het *delen* van persoonsgegevens kent de AVG het recht op overdraagbaarheid van persoonsgegevens (artikel 20 AVG), dat ook wel het recht op dataportabiliteit wordt genoemd. Door gebruikmaking van dit recht kan een persoon zijn persoonsgegevens (die de betrokkene vaak zelf heeft aangeleverd, zoals contactgegevens in een mobiele telefoon) doorgeven van de ene dienstverlener aan een andere dienstverlener. Dat recht kan alleen worden ingeroepen bij verwerkingen van persoonsgegevens die berusten op toestemming of een overeenkomst (zie artikel 6, eerste lid, aanhef en onder a en b, AVG) en als die verwerkingen via automatische procedures worden verricht. Ook dit recht kan worden beperkt of geweigerd en is ongeschikt voor het structureel en/of op grote schaal verstrekken van persoonsgegevens door een aanbieder en/of afnemer aan of via een persoon ten behoeve van regie op gegevens.

Tot slot bevat de AVG *waarborgen* bij het verwerken van persoonsgegevens. Er bestaat in die gevallen, zo is het uitgangspunt, voor de aanbieder een grondslag om die persoonsgegevens te verstrekken aan de afnemer. Dat kan zowel een specifieke grondslag zijn in een bijzondere wet, als een algemene grondslag van de AVG. De algemene grondslagen van de AVG zijn terug te vinden in artikel 6 AVG en betreffen (kort gezegd):

a) De ondubbelzinnige toestemming. Deze toestemming moet een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting betreffen;
b) De uitvoering of totstandkoming van een overeenkomst;
c) De wettelijke verplichting;
d) De vrijwaring van een vitaal belang van de betrokkene;
e) De goede vervulling van een taak van algemeen belang/uitoefening van het openbaar gezag; en

f) Een gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde.

Die grondslagen gaan steeds gepaard met waarborgen voor de persoon, die – in de regel – rusten op de aanbieder en de afnemer als verwerkingsverantwoordelijken. Zo mogen persoonsgegevens alleen worden verzameld voor specifieke, gerechtvaardigde doeleinden en mogen persoonsgegevens niet verder worden verwerkt op een met die doeleinden onverenigbare wijze (het beginsel van doelbinding). Daarnaast moeten de persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (het beginsel van dataminimalisatie). Verder moeten de persoonsgegevens juist zijn en zo nodig worden geactualiseerd (het beginsel van juistheid), niet langer worden bewaard dan noodzakelijk (het beginsel van opslagbeperking) en goed worden beveiligd (het beginsel van integriteit en vertrouwelijkheid) (zie artikel 5, eerste lid, AVG voor de beginselen inzake de verwerking van persoonsgegevens).

Ook moet een zogenoemde gegevensbeschermingseffectbeoordeling/privacy impact assessment worden uitgevoerd door een verwerkingsverantwoordelijke voorafgaand aan een verwerking die een hoog risico inhoudt voor de rechten en vrijheden van personen, zoals bij een structurele verstrekking van gevoelige (zogenoemde bijzondere) persoonsgegevens (artikel 35 AVG e.v.) en moet rekening worden gehouden met de uitgangspunten van gegevensbescherming door ontwerp (*data protection by design*) en gegevensbescherming door standaardinstellingen (*data protection by default*) (artikel 25 AVG).[12] Tot slot kunnen (of moeten [13]) tussen twee verwerkingsverantwoordelijken, zoals een aanbieder en afnemer, afspraken worden gemaakt over de verwerking, bijvoorbeeld in een regeling of overeenkomst.

De aanbieder zal, gelet op voornoemde waarborgen en verplichtingen, alleen persoonsgegevens aan een afnemer verstrekken als dat past binnen het doel waarvoor de aanbieder de persoonsgegevens heeft verkregen of verzameld. Verder houdt de aanbieder rekening met het beginsel van dataminimalisatie. Diezelfde afwegingen maakt de afnemer aan de ontvangende kant op het moment dat hij persoonsgegevens uitvraagt.

Gelet op het bovenstaande zal bij het voeren van regie op persoonsgegevens in ieder geval het denkkader en de materiële eisen van de AVG in acht moeten worden genomen. In het vervolgtraject zullen ook andere generieke kaders geduid gaan worden ten aanzien van regie op gegevens. Daarnaast zal bij toepassingen van regie op gegevens veelal bijzondere wet- en regelgeving aan de orde zijn. Gelet op de veelheid van mogelijke wet- en regelgeving die van toepassing kan zijn, is dergelijke bijzondere wet- en regelgeving in dit kader buiten beschouwing gelaten.

4.3 Juridisch kader voor persoonlijke gegevens (voor zover geen persoonsgegevens)

Als gezegd is op persoonlijke gegevens, voor zover dat geen persoonsgegevens zijn, de AVG niet van toepassing. Er zullen contractuele afspraken moeten worden gemaakt om de doelmatigheid, transparantie en veiligheid van het verwerken van deze gegevens te waarborgen. Om dat te bewerkstelligen kan de geest van de AVG worden gevolgd.

Zo kunnen ook bij het vloeien van persoonlijke gegevens verantwoordelijken en verwerkers worden aangewezen, die met elkaar afspraken moeten maken over de respectieve verantwoordelijkheden (*de rollen*).

12 Data protection by design betekent dat bij de ontwikkeling van producten en diensten (zoals nieuwe informatiesystemen) al zoveel mogelijk aandacht moet worden besteed aan privacy verhogende maatregelen en aan het uitgangspunt van dataminimalisatie. Data protection by default houdt in dat door middel van standaardinstellingen zo privacyvriendelijk mogelijk wordt gewerkt.

13 In het geval van gezamenlijke verwerkingsverantwoordelijkheid, waarbij twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden voor en de middelen van de verwerking bepalen, is het maken van afspraken verplicht. Zie artikel 26 AVG.

Ook voor de regieactiviteiten *inzien, veranderen* en *delen* kan de geest van de AVG worden gevolgd, in die zin dat personen zoveel mogelijk in de positie worden gebracht dat voor hen inzichtelijk is welke persoonsgegevens, door wie, met welk doel, op welke wijze worden verwerkt.

In aanvulling op de te maken afspraken over deze regieactiviteiten zal het mogelijk moeten zijn om een bepaalde waarde toe te kennen aan persoonlijke gegevens, zoals aan documenten of aan beweringen/attestaties, opdat afnemers het vertrouwen kunnen krijgen dat een persoon over de gevraagde kwalificatie(s) beschikt. Vertrouwensdiensten in de zin van de eIDAS-verordening kunnen daarbij een rol spelen.

Voorts moet bij het voeren van regie op documenten en/of op beweringen/attestaties de vraag worden gesteld van wie de (gegevens neergelegd in) documenten zijn. Is het standpunt dat de persoon rechthebbende is, dan resulteert dat in een andere uitgangspositie dan wanneer de aanbieder en/of afnemer rechthebbende is. Gaat het om officiële documenten, zoals identiteitsgegevens of gewaarmerkte uittreksels, dan wordt veelal tot uitgangspunt genomen dat de bron (de aanbieder) rechthebbende is op die gegevens. Hier kan ook het databankenrecht een rol spelen, dat het intellectuele eigendom van databanken regelt.

Kort en goed zijn er veel modellen denkbaar door de verschillende toepassingen van regie op gegevens die mogelijk zijn. Ieder van deze modellen roept eigen vragen op over de technische inrichting, de in te regelen governance en het juridische kader, bijvoorbeeld ook ten aanzien van aansprakelijkheid voor de verstrekking van foutieve informatie. Het valt buiten de reikwijdte van dit algemene kader voor regie op gegevens om al deze aspecten te bespreken.

Tot slot moeten in ieder geval ook de *waarborgen* van de AVG inzake de beginselen van verwerking van persoonsgegevens – te weten: de beginselen van doelbinding, dataminimalisatie, juistheid, opslagbeperking en integriteit en vertrouwelijkheid – tot uitgangspunt worden genomen bij de verwerking van persoonlijke gegevens.

Gelet op het bovenstaande zullen contractuele afspraken moeten worden gemaakt voor het voeren van regie op persoonlijke gegevens, waarbij de AVG als inspiratie dient. Vertrouwensdiensten kunnen een rol spelen om persoonlijke gegevens een te vertrouwen waarde toe te kennen. Per toepassing van regie op gegevens zal, naast generieke juridische kaders, altijd specifiek moeten worden gekeken welke juridische kaders voorts relevant zijn.

5 Functioneel, technisch, organisatorisch en operationeel kader

Dit hoofdstuk beschrijft het kader voor de invulling van regie op gegevens. In paragraaf 5.1 worden de belangrijkste bouwblokken voor de functionele invulling beschreven. Paragraaf 5.2 behandelt het technische kader voor RoG. Tot slot bevat paragraaf 5.3 een overzicht van onderwerpen voor het organisatorische en operationele kader die in de volgende versie van dit document worden uitgewerkt. Deze onderwerpen zijn noodzakelijk voor het stimuleren van het vertrouwen en het waarborgen van de continuïteit en veilig functioneren van RoG-afsprakenstelsels en -implementaties. Bij elke bouwsteen wordt een richtinggevende uitspraak gedaan (statement) en een beschrijving waarom dit statement is opgesteld (rationale). In deze versie van het kader voor RoG zijn nog geen concrete invullingen gegeven van deze bouwstenen. Dit wordt gedaan in de volgende fase, op basis van input van daarvoor in te richten werkgroepen.

5.1 Het functionele kader

Het functionele kader geeft aan wat een initiatief moet kunnen en moet bevatten. Het functionele kader wordt toegelicht aan de hand van de volgende vier onderdelen:

- Rollen in de regiedriehoek;
- Functionaliteiten;
- Interactiemodel (use cases);
- Compliance-maatregelen.

De rollen en het interactiemodel zijn ondergeschikt aan de functionaliteiten van RoG-afsprakenstelsels en RoG-implementaties. De compliance-maatregelen bespreken de manier waarop invulling wordt gegeven aan de functionaliteiten.

Rollen in de regiedriehoek

Statement:

Er dient een uitleg van de volgende rollen uit de regiedriehoek te worden geven:

1. Persoon
2. Afnemer
3. Aanbieder

Indien van toepassing dienen overige (ondersteunende) rollen beschreven te worden.

Rationale:

Rollen in de regiedriehoek geven aan wie welke functie heeft in RoG-afsprakenstelsels of RoG-implementaties. Voor RoG-afsprakenstelsels en RoG-implementaties zijn in ieder geval de volgende rollen uit de regiedriehoek (zie hoofdstuk 3) van toepassing:

1. *Persoon* (*person*): Degene die voor eigen doeleinden regiehandelingen uitvoert, of laat uitvoeren, op persoonlijke gegevens die op hem/haar betrekking hebben.
2. *Afnemer* (*data consumer*): De afnemer is degene die gegevens nodig heeft en gegevens aanvraagt. De afnemer is een juridische entiteit en kan worden gerepresenteerd door een persoon of een machine.
3. *Aanbieder* (*data provider*): De aanbieder is degene die de desbetreffende gegevens bezit of toegang heeft tot de desbetreffende databron. De aanbieder is een juridische entiteit en kan worden gerepresenteerd door een persoon of een machine.

Figuur 14. *Bouwstenen voor het functionele kader*

BereikMij

De hoofdrollen in het BereikMij Afsprakenstelsel zijn de drie rollen in de regiedriehoek, met de persoon als uitgever, de aanbieder als bron en de afnemer als lezer. Daarnaast hebben deze elk hun eigen verwerker. De persoon maakt bijvoorbeeld gebruik van een webdienst waarin hij zijn adressen beheert en de aanbieder en afnemer van hun eigen uitvoerders. De belangrijkste functionaliteiten zijn: het verzamelen door de persoon bij de afnemer en het delen door de persoon met de aanbieder. Hiervoor worden interactiemodellen gebruikt die gebaseerd zijn op RESTful interacties tussen gebruikers en aanbieders van (adres)gegevensdiensten, in de stijl van de web-wereld.

Additionele ondersteunende rollen kunnen van toepassing zijn. In het algemeen geldt, dat gestreefd moet worden om zo min mogelijk rollen aanwezig te hebben, vanwege extra beveiligingsrisico's die nieuwe rollen opleveren. Voorbeelden van onder-steunende rollen zijn bijvoorbeeld:

- Verwerker: De verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Deze term is breder dan verwerking zoals in de AVG.
- Identiteitsaanbieder (Identity provider): De identiteitsaanbieder identificeert en authentiseert een persoon.
- Identiteitsmakelaar (Identity broker): De identiteitsmakelaar bundelt alle mogelijke identiteitsaanbieders zodat aanbieders niet afzonderlijk met elke identiteitsaanbieder hoeven te koppelen.
- Metadata directory beheerder (Metadata directory administrator): De metadata directory beheerder houdt bij welke bedrijven zijn aangesloten bij het RoG-afsprakenstelsel of de RoG-implementatie en maakt het gemakkelijker om de juiste bedrijven te vinden om gegevens mee te delen.

De entiteiten mens, overheid en bedrijf kunnen één of meerdere rollen vervullen. In 2019 wordt verder onderzocht welke overige rollen van toepassing kunnen zijn en welke rollen nog beschreven dienen te worden.

Functionaliteiten

Statement:

Er dient aangegeven te worden welke regiehandeling wordt geboden.

Rationale:

Functionaliteiten geven aan wat er door RoG-afsprakenstelsels of RoG-implementaties mogelijk wordt gemaakt.
De functionaliteiten dienen expliciet benoemd te worden, zodat helder is welke functies het RoG-afsprakenstelsel en/of de RoG-implementaties hebben.
Functionaliteiten die worden geboden kunnen zijn:

1. Personen kunnen persoonlijke gegevens inzien;
2. Personen kunnen persoonlijke gegevens veranderen;
3. Personen kunnen persoonlijke gegeven delen.

Er dient ook te worden ingevuld op wat voor data en voor welke specifieke attributen deze functionaliteiten van toepassing zijn.

Interactiemodel

Statement:

RoG-afsprakenstelsels en RoG-implementaties dienen de mogelijke interacties toe te lichten. Ook moet worden toegelicht waar welke data wordt opgeslagen.

HypoThese

Het HypoThese Afsprakenstelsel gebruikt standaard informatiemodellen en uitwissel-protocollen, passend bij de stijl van het interactiemodel. Het afsprakenstelsel heeft informatiestandaarden opgenomen die al op acceptatie konden rekenen van een groot deel van de hypotheekverstrekkers. Alle het informatieverkeer in de regiedriehoek gaat gepaard met authenticatie van een passend zekerheidsniveau, en doel-specifieke autorisatie.

Rationale:
Het interactiemodel laat zien welke interactie(s) (ook wel: transactie(s)) tussen entiteiten plaatsvinden.

De interactie geeft aan tussen welke entiteiten gegevens wordt gedeeld. Deze entiteiten vervullen een of meerdere rollen uit de regiedriehoek. Rollen zijn toegelicht in het onderdeel "Rollen". De mogelijke interacties die plaatsvinden zijn:

- Mens naar overheid;
- Mens naar bedrijf;
- Bedrijf naar overheid;
- Overheid naar bedrijf;
- Overheid naar mens;
- Bedrijf naar mens;
- Bedrijf naar bedrijf;
- Overheid naar overheid.

Op basis van de geïntroduceerde terminologie in het onderdeel "Rollen" en naar het voorbeeld van onderstaande interactie dient een stappenplan of een visualisatie van het interactiemodel te worden opgezet.
Een voorbeeld van een stappenplan van een interactie:

1. De menselijke afnemer vraagt een service (data uitwisseling) van de aanbieder;
2. De aanbieder vraagt een login van de identiteits-makelaar;
3. De identiteitsmakelaar vraagt de afnemer om zijn identiteitsaanbieder te kiezen;
4. De identiteitsmakelaar vraagt een login van de identiteitsaanbieder;
5. The identiteitsaanbieder authentiseert de menselijke afnemer (op basis van zijn identiteit);
6. De identiteitsaanbieder geeft een identiteits-bevestiging voor de aanbieder vrij aan de identiteitsmakelaar;
7. De identiteitsmakelaar geeft de identiteits-bevestiging door aan de aanbieder;
8. De aanbieder authentiseert de identiteits-bevestiging door de identiteitsaanvrager en de identiteitsmakelaar te valideren;
9. De aanbieder authentiseert de identiteit van de afnemer;
10. De aanbieder autoriseert de afnemer op basis van specificaties rondom de service (data uitwisseling);
11. De aanbieder voert de gevraagde service uit.

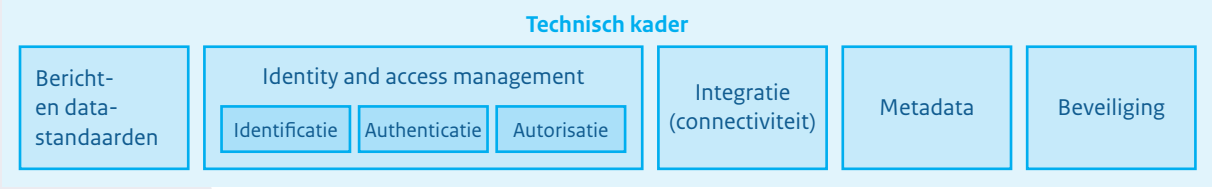
Ook dient aangegeven te worden op welk moment bij/met welke entiteiten (en bij/met welke rollen) data wordt opgeslagen en/of gedeeld, ten behoeve van het streven naar dataminimalisatie.

Compliance-maatregelen
Statement:
Er dient te worden aangegeven hoe binnen de functionaliteiten die worden aangeboden invulling wordt gegeven aan de compliance verplichting.

Rationale:
Compliance-maatregelen zijn maatregelen die genomen worden om compliant te zijn.
Het juridische kader bespreekt aan welke regelgeving RoG-afsprakenstelsels en RoG-implementaties moeten voldoen, maar niet hoe binnen de functionaliteiten invulling wordt gegeven compliant te zijn.

5.2 Het technische kader

Het technische kader geeft een richting aan wat een initiatief (RoG-afsprakenstelsel of implementatie) technisch gezien moet onderschrijven.



Figuur 15. *Bouwstenen voor het technische kader*

Het technische kader wordt beschreven in de volgende zeven onderdelen:

- Bericht- en datastandaarden
- Identificatie;
- Authenticatie;
- Autorisatie;
- Integratie (connectiviteit);
- Metadata;
- Beveiliging.

Bericht- en datastandaarden

Statement:

Er moeten standaarden toegepast worden die in een domein gebruikelijk zijn en succesvol zijn gebleken.

Rationale:

Een standaard is een afspraak die is vastgelegd in een specificatiedocument. Om gegevens uit te wisselen moeten ICT-systemen dezelfde standaard hebben geïmplementeerd. Bericht- en datastandaarden leiden tot meer interoperabiliteit tussen afnemers, aanbieders en personen.
Er bestaan veel verschillende bericht- en datastandaarden. Deze standaarden zijn vaak domein specifiek. Er moet in kaart worden gebracht welke standaarden in een domein gebruikelijk en succesvol zijn. In het huidige kader zijn specifieke domeinstandaarden nog niet opgesteld. Daarvoor is meer onderzoek nodig.

Bij de volgende iteratie van het kader, wordt onderzocht of domein overstijgende standaardisatie ook dient te worden gestimuleerd.
Ook kan gedacht worden aan standaardisatie in specifieke toepassingen (web).

Identificatie

Statement:

Er moet worden toegelicht welke identificatiemethode(n) gebruikt worden en er moet worden vastgelegd welke karakteristieken gebruikt kunnen worden ter identificatie.

Rationale:

Identificatie is het proces waar iets of iemand een identiteit claimt op basis van bepaalde karakteristieken, zoals wachtwoord, attributen of biometrische informatie. Identificatie is nodig zodat bij onrechtmatig gedrag rondom RoG duidelijk is wie verantwoordelijk is. Toelichting van identificatiemethodes en vastlegging van karakteristieken ter identificatie zijn nodig zodat het gewenste betrouwbaarheidsniveau wordt gerealiseerd.

De eisen waaraan het identificatieproces moet voldoen zijn gebaseerd op en in lijn met de eIDAS-verordening. Daar worden drie betrouwbaarheidsniveaus onderscheiden: laag, substantieel en hoog. Verschillende (combinaties van) identificatie-methoden leiden tot verschillende betrouwbaarheidsniveaus. Er moet worden bepaald welk betrouwbaarheidsniveau van toepassing is (afhankelijk van de persoonlijke gegevens die gedeeld worden). Ook dient te worden aangegeven op basis van welke karakteristieken identificatie kan plaatsvinden, omdat volgens de AVG niet meer gevraagd mag worden dan nodig (doelbinding).

Bij de volgende iteratie van het kader, zal mogelijke convergentie van identificatiemethodes worden onderzocht, teneinde de kaders uit te breiden naar een specifieker handelingsperspectief op dit gebied.

Authenticatie

Statement:

Er moet worden toegelicht welke authenticatie-methode(n) gebruikt worden en er moet gebruik worden gemaakt van open standaarden.

Rationale:

Authenticatie is het proces waar de identiteit van iets of iemand gecontroleerd en gevalideerd wordt. Het is belangrijk dat een identiteit gevalideerd kan worden met een bepaalde mate van zekerheid, zodat deelnemende partijen elkaar kunnen vertrouwen. Open standaarden zijn publiekelijk beschikbaar en zorgen voor interoperabiliteit. Een voorbeeld van een open standaard zijn het OpenID authentication framework.

De eisen waaraan het authenticatieproces moet voldoen zijn gebaseerd op en in lijn met de eIDAS-verordening. Daar worden drie betrouwbaarheidsniveaus onderscheiden: laag, substantieel en hoog. Verschillende (combinaties van) authenticatiemethoden leiden tot verschillende betrouwbaarheidsniveaus. Er moet worden bepaald welk betrouwbaarheidsniveau van toepassing is (afhankelijk van de persoonlijke gegevens die gedeeld worden). Het Forum van Standaardisatie heeft een lijst gepubliceerd waarin een overzicht wordt gegeven van open standaarden.

Bij de volgende iteratie van het kader, zal mogelijke convergentie van authenticatie-methodes worden onderzocht, teneinde de kaders uit te breiden naar een specifieker handelingsperspectief op dit gebied.

Autorisatie

Statement:

Er moet voor alle persoonlijke gegevens worden toegelicht hoe autorisatie georganiseerd is.

Rationale:

Autorisatie legt rechten op toegang tot gegevens van personen en/of bedrijven en/of de overheid vast.

BereikMij

Het BereikMij Afsprakenstelsel gebruikt standaard informatiemodellen en uitwisselprotocollen, passend bij de stijl van het interactiemodel. Adresformaten worden natuurlijk overgenomen van de voor het specifieke kanaal vastgelegde formaat. Het verzamelen van adresinformatie bij aanbieders gaat gepaard met authenticatie met bijvoorbeeld DigiD en specifieke autorisatie om het adres te plaatsen in het adresdossier van de persoon. Bij het delen van adressen met afnemers wordt de authenticatiesystematiek van die afnemer gebruikt en een specifieke autorisatie door de persoon gekoppeld aan een specifiek gebruiksdoel. Menigmaal zal de afnemer daarbij eerst moeten kunnen aantonen dat er een relatie met de persoon bestaat die het gebruik van het betreffende adres rechtvaardigt. Die relatie wordt dan context (metadata) van het betreffende adres.

De afnemer kan op basis van toestemming van personen of delegatie van een toegangsrecht geautoriseerd worden. Dit zorgt ervoor dat personen controle behouden over hun gegevens. RoG-afsprakenstelsels en RoG-implementaties dienen toe te lichten:

- Voor wie, hoe en waar autorisaties en toestemming worden opgeslagen;
- Voor welke gegevens autorisatie en toestemming worden georganiseerd.

Een vorm van het geven van toestemming is het delegeren van toegangsrechten. Het delegeren van toegangsrechten maakt het personen mogelijk om andere personen (of bedrijven) te ‘machtigen’.

Regels rondom autorisatie en toestemming worden op dit moment voornamelijk binnen organisaties of platformen, RoG-afsprakenstelsels en implementaties vastgesteld.

Bij de volgende iteratie van het kader, kan worden onderzocht of meer gemeenschappelijke standaarden in een keten of in een domein moeten worden opgesteld, zodat autorisaties onderling uitgewisseld kunnen worden.

Integratie (connectiviteit)

Statement:

Connectiviteit dient zo laagdrempelig en veilig mogelijk te zijn.

Rationale:

Connectiviteit geeft aan waarmee twee of meerdere bedrijfssystemen verbinding maken met elkaar. Digitale deling van gegevens met andere bedrijven is alleen mogelijk wanneer er verbinding is met andere bedrijven. Connectiviteit is nodig om data (gemakkelijk) te delen.
Bij de volgende iteratie van het kader, zal worden onderzocht of domein overstijgende standaardisatie van protocollen dient te worden gestimuleerd, teneinde de kaders uit te breiden naar een specifieker handelingsperspectief op dit gebied.

Metadata

Statement:

Er moeten metadatastandaarden toegepast worden op een zo hoog mogelijk niveau, waar mogelijk domein overstijgend.

Rationale:

Metadata zijn gegevens over gegevens. Metadata zijn gegevens die de karakteristieken van gegevens beschrijven en bestaan uit inhoudelijke informatie, beschrijvende informatie en beschikbaarheidsinformatie.
Door interoperabiliteit van metadata te waarborgen kunnen systemen en machines digitaal met elkaar communiceren zonder dat daarbij analyses op de gegevens moeten worden gedaan. Gegevens kunnen gelokaliseerd worden zonder dat er menselijke tussenkomst nodig is. Er kan gecommuniceerd worden over de grootte van een dataset, toegangsrechten en de geschiedenis van een dataset. Bovendien kan er informatie uitgewisseld worden zonder dat er toestemming wordt verschaft tot de hele dataset.
Een directory van metadata organiseert een overzicht van de verschillende databases en zorgt ervoor dat gegevens vindbaar zijn.

Er bestaan veel verschillende metadatastandaarden. In verschillende domeinen zijn verschillende metadatastandaarden gebruikelijk. Ten behoeve van domein specifieke interoperabiliteit dienen RoG-afsprakenstelsels en RoG-implementaties metadatastandaarden te gebruiken die gebruikelijk zijn en succesvol zijn gebleken. Daarvoor dienen RoG-afsprakenstelsels en RoG-implementaties in kaart te brengen welke metadatastandaarden in hun domein gebruikelijk en succesvol zijn.

In de toekomst zullen metadatastandaarden gebruikelijker zijn. Bij de volgende iteratie van het kader, wordt onderzocht welke metadatastandaarden in welke domeinen reeds van toepassing zijn.

Beveiliging

Statement:

Er dient in kaart te worden gebracht hoe om te gaan met de belangrijkste kwetsbaarheden en het implementeren van passende maatregelen.

Rationale:

Beveiliging betreft de bescherming van (computer) gegevens tegen risico's zoals het in onbevoegde handen terechtkomen van de gegevens en het, daarmee gepaarde, onbevoegde gebruik ervan. Voor effectieve beveiliging dienen RoG-afsprakenstelsels en RoG-implementaties in kaart te brengen wat hun belangrijkste kwetsbaarheden zijn.

Vanuit de best practices, bijvoorbeeld, richtlijnen van het Nationaal Cyber Security Centrum (NCSC), de OWASP top 10, het eigen risico management, en penetratietesten zijn de belangrijkste kwetsbaarheden vastgelegd.
Maatregelen richting deze kwetsbaarheden dienen in kaart te worden gebracht. Dit kan bijvoorbeeld op basis van de privacy-by-design en privacy-by-default benadering en/of op basis van ISO 27001/27002 maatregelen en/of op basis van eigen beleid.
In de toekomst zullen nieuwe en/of andere beveiligingsmaatregelen worden genomen.

5.3 Het organisatorische en operationele kader

Het goed beschrijven en inrichten van relevante organisatorische en operationele processen draagt bij aan de continuïteit en vertrouwen van regie op gegevens.

In deze versie van het document is de uitwerking van organisatorische en operationele kader buiten scope gelaten. In de volgende versie van het document zullen de relevante onderwerpen voor het organisatorische en operationele kader uitgewerkt worden.
Denk bijvoorbeeld aan de volgende onderwerpen:

- Incident Management;
- Service Level Management;
- Change- Release management;
- Managementinformatie;
- Beheer van informatiebeveiliging;
- Toe- & uittreden;
- Ondersteuning;
- Communicatie;
- Governance op het RoG-afsprakenstelsel of RoG-implementatie.

Bijlage A: Begrippen

Begrip	Omschrijving
Aanbieder	Rol in de regiedriehoek die de desbetreffende gegevens bezit of toegang heeft tot de desbetreffende databron.
Afnemer	Rol in de regiedriehoek die die gegevens nodig heeft en gegevens aanvraagt.
Afsprakenstelsel	Set van juridische, organisatorische, financiële, semantische en technische afspraken, bedoeld om vertrouwen tussen betrokken partijen te borgen in een door het stelsel geboden vorm of aspect van RoG. Deelnemers committeren zich aan de afspraken en kunnen op basis van de reeds overeengekomen afspraken, diensten aanbieden.
Algemene Verordening Gegevensbescherming (AVG)	Verordening van de Europese Unie, die beoogt de rechten van mensen op gegevensbescherming te versterken, conform Artikel 8 van het Handvest van de grondrechten van de Europese Unie.
Authenticatie	Authenticatie is het proces waar de identiteit van iets of iemand gecontroleerd en gevalideerd wordt.
Autorisatie	Autorisatie legt rechten op toegang tot gegevens van personen en/of bedrijven en/of de overheid vast.
Bewering	Aanspraak op de geldigheid van een zeker persoonlijk gegeven.
Bron	Partij waarvandaan gegevens komen of betrokken worden.
Correctierecht	Recht op rectificatie.
Dataminimalisatie	Beperking tot alleen de noodzakelijke verwerking van alleen noodzakelijke gegevens, als aspect van privacy-by-design.
Dataportabiliteit	Overdraagbaarheid van gegevens.
Decentraal	Verspreid over samenhangende of samenwerkende eenheden.
Deelnemer	Partij die zich, al dan niet vrijwillig, gebonden weet aan de afspraken die in een afsprakenstelsel toegewezen zijn aan de rol waarin zij deelneemt.
Doelbinding	Verenigbaarheid van de verwerking van persoonsgegevens met het welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinde waartoe zij zijn verzameld.
eHerkenning	Afsprakenstelsel voor authenticatie van ondernemers voor digitale dienstverlening.
Electronic Identification, Authentication and trust Services (eIDAS)	Verordening van de Europese Unie, van kracht sinds 29 september 2018, betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.
Gegeven	Kenbare informatie.
Gegevensbescherming door ontwerp (Privacy by design)	Plicht van de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen, zoals pseudonimisering, die gegevensbescherming bevorderen, zoals dataminimalisatie.
Gegevensbescherming door standaardinstellingen (Privacy by default)	Plicht van de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen opdat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.
Gelijkwaardigheid	Ongeldigheid van andere dan uitdrukkelijke afhankelijkheden of onderscheiden tussen partijen of rollen.
Governance	Procesbeheer dat de kwaliteit van het kader voor RoG borgt.
Hergebruik	Verwerking van persoonlijke gegevens voor verschillende doelen.

Begrip	Omschrijving
Identificatie	Identificatie is het proces waar iets of iemand een identiteit claimt op basis van bepaalde karakteristieken, zoals wachtwoord, attributen of biometrische informatie.
Interoperabiliteit	Samenwerkzaamheid/koppelbaarheid.
Inzagerecht	Recht van betrokkene op uitsluitsel van verwerkings¬verantwoordelijke over verwerking van hem betreffende persoonsgegevens en, wanneer dat het geval is, kennisname van die gegevens en zekere aanvullende informatie.
Kader voor Regie op gegevens (RoG)	Set van rolsgewijze verantwoordelijkheden inzake RoG, zoals in dit document in eerste aanleg opgenomen, dat beoogt het vertrouwen in, en de interoperabiliteit van afsprakenstelsels en RoG-implementaties te bevorderen door betrokken partij te binden aan die verantwoordelijk-heden.
Leefwereld	Milieu van een mens, zoals door hem/haarzelf begrepen.
Metadata	Gegevens over gegevens.
Overdraagbaarheid	Mogelijkheid tot verstrekking van gegevens, van de ene verwerkingsverantwoordelijke verkregen, aan een andere.
Payment Services Directive 2 (PSD2)	Richtlijn van de Europese Unie, betreffende betalingsdiensten in de interne markt.
Regie op gegevens	Regiehandelingen van of namens betrokkenen op persoonlijke gegevens, en het verkeer daarmee, onder verantwoordelijkheid van de betrokkene zelf.
Persoon	Degene die voor eigen doeleinden regiehandelingen uitvoert, of laat uitvoeren, op persoonlijke gegevens die op hem/haar betrekking hebben.
Persoonlijk gegeven	In toevoeging op de persoonsgegevens in de zin van de AVG, behelst persoonlijke gegevens, gegevens over bedrijven of organisaties die in veel gevallen niet herleidbaar zullen zijn tot natuurlijke personen en dan dus geen persoonsgegevens zijn. Voorts ziet het persoonsgegevensbegrip alleen op de gegevens over een persoon als zodanig, en niet ook op de drager van die gegevens, zoals een document, of op een geattesteerde bewering.
Persoonsgegeven	Persoonsgegevens is een term afkomstig uit de AVG en betreft, kort gezegd, alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het gaat dan zowel om direct identificeerbare informatie (zoals een naam, identificatienummer of foto) als om indirect identificeerbare informatie (zoals locatiegegevens).
Privacy	Bescherming van de persoonlijke levenssfeer, in het bijzonder door bescherming van persoons-gegevens.
Privacy-by-default	Gegevensbescherming door standaardinstellingen.
Privacy-by-design	Gegevensbescherming door ontwerp.
Rechtsgrond	Met betrekking tot zeker verkeer van persoonlijke gegevens: de rechtsregels die erop van toepassing zijn.
Regiedriehoek	Model van de scheiding en verbinding van drie rollen in regie op gegevens: persoon, afnemer en aanbieder.
Semantiek	Betekenis van informatie, of de wetenschap die zich daarmee bezighoudt.
Toegankelijkheid	Vindbaar, bruikbaar en uitwisselbaar.
Toestemming	Specifieke uiting van instemming.
Verifiable claims	Verifieerbare claims, zoals gestandaardiseerd door W3C.
Vertrouwelijkheid	Bescherming van gegevens tegen openbaring aan onbevoegden.
Vertrouwen	Veronderstelling van goede trouw.

Begrip	Omschrijving
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Deze term is breder dan verwerking zoals in de AVG.
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonlijke gegevens of een geheel van persoonlijke gegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Verwerkings-verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoons gegevens vaststelt.

Zelf geregeld, veilig en betrouwbaar!

Met hun gegevens kunnen mensen zaken zelf digitaal regelen. Veilig en betrouwbaar, dankzij gemeenschappelijke afspraken in een vertrouwensstelsel.
Door te zorgen voor meer regie op gegevens voor onze inwoners en ondernemers, versterken we digitale autonomie, beschermen we belangrijke waarden als privacy, verminderen we administratieve lasten, en kunnen we bestaande dienstverlening verbeteren en nieuwe vormen van dienstverlening ontwikkelen.

Met meer regie op gegevens maken we Nederland DIGIbeter.

REGIE OP GEGEVENS
Zelf geregeld, veilig en betrouwbaar!