Regie op gegevens en de AVG

Notitie door Pels Rijcken in opdracht van het programma Regie op Gegevens

Pels Rijcken
& Droogleever
Fortuijn *advocaten*
en notarissen

REGIE OP GEGEVENS
Zelf geregeld, veilig en betrouwbaar!

Colofon

Uitgegeven door	Programma Regie op Gegevens
Informatie	regieopgegevens@ictu.nl
Uitgevoerd door	Pels Rijcken: Sandra van Heukelom-Verhage, Nina Bontje en Tim Gillhaus
Zaaknummer	11007739 (Pels Rijcken)
Datum	31 Oktober 2018
Status	Definitief

Pels Rijcken
& Droogleever
Fortuijn *advocaten*
en notarissen

Voorwoord

Deze rapportage is een van de producten van het programma ‘Burgers en bedrijven in regie op hun gegevens (RoG)’.

Het afgelopen jaar zien we een groeiend aantal initiatieven en experimenten om burgers en bedrijven meer regie op hun gegevens te geven met behulp van RoG-systemen. Onder meer op basis van deze experimenten wordt, binnen het programma, onderzocht wat nodig is om tot werkbare afspraken en structuren te komen voor regie op gegevens. Dit moet resulteren in een kader voor regie op gegevens.

Om voldoende juridische grondslag aan deze experimenten te geven, is aan Pels Rijcken gevraagd te adviseren over de juridische kaders, in het bijzonder hoe we de komende jaren aan de slag kunnen gaan met regie op gegevens in relatie tot de Algemene verordening gegevensbescherming. Met als doel om bestuurders comfort te geven dat er juridisch mogelijkheden zijn om te experimenteren met vormen van regie op gegevens.

In het hiernavolgende advies wordt beoogd om algemene juridische kaders te geven, zodat aan de voorkant, per geval, kan worden toegewerkt naar een ecosysteem waarin het juiste evenwicht wordt gevonden tussen een nieuwe manier van gegevensuitwisselingen enerzijds en de inbedding van de nodige waarborgen anderzijds.

Dit is een eerste stap om de juridische kaders voor regie op gegevens inzichtelijk te krijgen. Het advies biedt ruimte om experimenten in te richten, ons daarmee te oriënteren op de toekomstige mogelijkheden, en met elkaar op zoek te gaan naar oplossingsrichtingen.

De uitkomsten van dit onderzoek zullen ook meegenomen worden in de verdere uitwerking van het kader voor regie op gegevens.

Douwe Leguit

Programmamanager Regie op Gegevens

1 Inleiding

1.1 Door digitalisering van de samenleving zijn er steeds meer gegevens van burgers en bedrijven beschikbaar, zonder dat voor hen altijd duidelijk is wie, waarom, welke gegevens verwerkt en hoe dat wordt gedaan. De positie van burgers en bedrijven kan worden verbeterd en versterkt door hen meer regie op hun gegevens te geven. Voorts kan daarmee dienstverlening worden verbeterd en innovatiekracht worden versterkt.

1.2 Er zijn diverse initiatieven om burgers en bedrijven meer regie op hun gegevens te geven met behulp van systemen voor regie op gegevens (hierna: RoG). Binnen het programma 'Burgers en bedrijven in regie op hun gegevens' wordt onderzocht wat nodig is om tot werkbare afspraken en structuren te komen voor RoG. U hebt ons in dat kader gevraagd te adviseren over de juridische kaders. Het gaat u in het bijzonder om de verhouding tussen RoG en de Algemene verordening gegevensbescherming (hierna: AVG[1]), nu gegevens van burgers veelal persoonsgegevens betreffen. Op de verwerking van persoonsgegevens is de AVG van toepassing. U treft ons advies hieronder aan.

1.3 Dit advies is bedoeld voor bestuurders en organisaties die experimenteren met initiatieven voor (meer) regie op gegevens. Bij ieder experiment worden andere uitgangspunten gehanteerd en zijn er andere gevolgen voor het ecosysteem van gegevensuitwisselingen. In dit advies beogen wij de algemene juridische kaders te geven, zodat aan de voorkant, per geval, kan worden toegewerkt naar een ecosysteem waarin het juiste evenwicht wordt gevonden tussen een nieuwe manier van gegevensuitwisselingen enerzijds en de inbedding van de nodige waarborgen anderzijds.

1.4 Daarbij merken wij op dat dit advies een levend document is. Het advies zal moeten worden aangepast naar gelang inzichten rondom (de techniek voor) regie op gegevens veranderen. Per techniek moet vervolgens worden gekeken wat de gevolgen van die techniek zijn voor de bescherming van persoonsgegevens en hoe de techniek zich ook overigens verhoudt tot het recht.

1 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

2 Achtergrond AVG en regie op gegevens: regie op wat?

2.1 Alvorens in te gaan op de verhouding tussen de AVG en regie op gegevens, moet allereerst scherp zijn waar burgers en bedrijven precies regie op moeten krijgen. Neemt men tot uitgangspunt dat burgers en bedrijven, conform de naam van het programma, regie op *gegevens* moeten krijgen, dan is de voorvraag om welk soort gegevens het gaat. Er moet in ieder geval onderscheid worden gemaakt tussen de verwerking van persoonsgegevens, waarop de AVG van toepassing is, en de verwerking van andere gegevens[2].

PERSOONSGEGEVENS zijn: "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon" (zie artikel 4, aanhef en onder 1, AVG).

De AVG kent daarbij ook bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens en genetische gegevens:

GEGEVENS OVER GEZONDHEID betreffen "persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven" (artikel 4, aanhef en onder 15, AVG).

GENETISCHE GEGEVENS betreffen "persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon" (artikel 4, aanhef en onder 13, AVG).

VERWERKING is "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens" (artikel 4, aanhef en onder 2, AVG).

Gegevens over een bedrijf (hierna ook: bedrijfsgegevens) zijn, als deze niet herleidbaar zijn tot een identificeerbaar persoon, geen persoonsgegevens. Op de verwerking van bedrijfsgegevens is de AVG dan ook niet van toepassing.

2.2 Aandachtspunt bij het persoonsgegevensbegrip is voorts dat persoonsgegevens de *gegevens* over een persoon als zodanig betreffen, en niet ook de *drager* van de gegevens, zoals een document, of geattesteerde beweringen over een persoon.

2 In het vervolg van dit advies zal daarom steeds onderscheid worden gemaakt tussen persoonsgegevens en (andere) gegevens.

"Wanneer het gaat over de informatie van de persoon hebben we het zowel over 1) persoonsgegevens zoals benoemd in de AVG; 2) de drager van deze gegevens zoals een uittreksel of diploma, en; 3) beweringen die door een persoon worden gedaan en kunnen worden geattesteerd door een (bevoegde) instantie of andere persoon. Deze informatie kan afkomstig zijn van en geleverd worden aan zowel publieke als private partijen."[3]

2.3 Dat onderscheid wordt met name relevant als men de in de AVG opgenomen rechten van de betrokkene als grondslag neemt voor het voeren van regie op persoonsgegevens. De AVG kent aan een betrokkene het recht toe op inzage in de hem betreffende persoonsgegevens. Daarnaast heeft de betrokkene recht op overdraagbaarheid van de hem betreffende persoonsgegevens, maar slechts voorzover de verwerking is gebaseerd op ondubbelzinnige toestemming of een overeenkomst. De betrokkene zal het recht op overdraagbaarheid vaak niet kunnen inroepen ten aanzien van gegevens in overheidsregistraties. De verwerking van gegevens in overheidsregistraties vindt namelijk in zijn algemeenheid plaats op grond van een wettelijke plicht of publieke taak.

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 (hierna: 'Wgbo'). 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.

2.4 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 (zoals een bestuursorgaan of bedrijf) worden verwerkt, en omvat niet ook een recht op de documenten/dragers van die persoonsgegevens of op geattesteerde beweringen.[4]

2.5 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.[5]

2.6 Verder hebben betrokkenen recht op een kopie *van de persoonsgegevens* die worden verwerkt.[6] 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.

Vgl. ook de website van de Autoriteit Persoonsgegevens:[7]

"KOPIE PERSOONSGEGEVENS
De organisatie moet u een kopie van uw persoonsgegevens geven wanneer u een inzageverzoek doet. De organisatie kan dit

3 Vgl. ***Paper*** over de designathon van 24 oktober 2018.
4 Artikel 15, eerste en tweede lid, AVG.
5 Idem.
6 Artikel 15, derde lid, AVG.
7 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/recht-op-inzage.

op verschillende manieren doen. Bijvoorbeeld door u kopieën te geven van alle documenten waarin uw persoonsgegevens voorkomen.

COMPLEET OVERZICHT
Maar de organisatie kan er ook voor kiezen om alleen uw persoonsgegevens te kopiëren in plaats van de volledige documenten. Om vervolgens deze bij elkaar te zetten in een compleet overzicht. (...)"

2.7 Een stelsel van regie op gegevens gaat mogelijk **WEL** uit van regie op de drager van gegevens en/of op geattesteerde beweringen, althans het enkel hebben van een kopie van persoonsgegevens kan onvoldoende zijn om het stelsel te laten werken. Veelal zal een dienstverlener niet of niet alleen over persoonsgegevens willen beschikken om een dienst te leveren, maar zeker willen zijn dat een bepaalde bewering over de betrokkene waar is, bijvoorbeeld door verkrijging van een gewaarmerkt document of door attestatie van een bewering.

2.8 In aanvulling op het inzagerecht zal het daarom mogelijk moeten zijn om aan persoonsgegevens en/of documenten een bepaalde waarde toe te kennen die een dienstverlener het vertrouwen geeft dat de betrokkene over de gevraagde kwalificatie beschikt. Hier kan een rol zijn weggelegd voor vertrouwensdiensten.

Ter vergelijking wijzen wij op de eIDAS-verordening, die een kader bevat voor het gebruik van vertrouwensdiensten bij (onder meer) interlidstatelijke dienstverlening.[8]

2.9 Een andere belangrijke vraag in dat kader is van wie persoonsgegevens, neergelegd in documenten, zijn. Is het standpunt dat die persoonsgegevens van de burger zijn, en de burger met andere woorden rechthebbende is op de persoonsgegevens, dan resulteert dat in een andere uitgangspositie dan wanneer de bron en/of dienstverlener rechthebbenden zijn op die persoonsgegevens. Gaat het om officiële documenten, zoals identiteitsgegevens of gewaarmerkte uittreksels, dan wordt veelal tot uitgangspunt genomen dat de bron rechthebbende is op die gegevens.

Wij nemen als voorbeeld een diploma, 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 situaties denkbaar waarin een dienstverlener niet zozeer persoonsgegevens wil ontvangen om een dienst te leveren, maar er alleen zeker van wil zijn dat de afnemer van de dienst is afgestudeerd in een bepaalde richting; of
- De diploma (het *document*) als drager van de informatie dat persoon X is afgestudeerd.

8 Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

Hier kan ook het databankenrecht een rol spelen, dat het intellectuele eigendom van databanken regelt.

2.10 Wij zien grosso modo drie modellen met betrekking tot het voeren van regie op gegevens, te weten regie door middel van het attesteren van: 1) beweringen, 2) kopieën van documenten en 3) van originele documenten. Ieder van deze modellen roept eigen vragen op over de technische inrichting, de in te regelen *governance* en de juridische kaders, bijvoorbeeld ten aanzien van aansprakelijkheid voor de verstrekking van foutieve informatie. Het valt buiten de reikwijdte van dit AVG-advies om al deze aspecten te bespreken. Wij volstaan op deze plek met een verwijzing naar een overzicht met de drie voornoemde modellen (**bijlage 1**) en adviseren graag in een vervolgadvies over de (juridische) mogelijkheden van deze modellen.

Deelconclusie

2.11 De AVG en de daarin opgenomen rechten van de betrokkene zijn ten behoeve van het vrije verkeer van *persoonsgegevens* in het leven geroepen. De AVG beoogt het vrije verkeer van persoonsgegevens te bevorderen en tegelijkertijd het recht op bescherming van persoonsgegevens te waarborgen (vgl. overweging 10 AVG). Doordat de rechten van de betrokkene zijn beperkt tot persoonsgegevens, zien wij niet dat de rechten van de betrokkene in de AVG **ZELFSTANDIG** een grondslag kunnen bieden voor (een afsprakenstelsel voor) regie op gegevens. Dit gaat immers over meer dan het sec uitwisselen van persoonsgegevens. Datzelfde geldt voor de in artikel 6 van de AVG opgesomde grondslagen, nu dat slechts grondslagen zijn voor het verwerken van persoonsgegevens.

Zie **bijlage 2** voor een samenvatting van onze analyse van mogelijke grondslagen voor een afsprakenstelsel in de AVG. Daarin bespreken wij ook hergebruik en het vrije verkeer van gegevens als mogelijke grondslag.

2.12 Evenwel speelt de AVG en de daarin opgenomen rechten van de betrokkene een rol bij regie op gegevens, niet in het minst omdat RoG-toepassingen burgers in een optimale positie kunnen brengen om hun rechten uit de AVG uit te oefenen. Daarnaast zullen bij regie op gegevens *ook* persoonsgegevens worden verwerkt. Voorts biedt de AVG een helder kader voor de kwalificatie van de actoren binnen een stelsel van regie op gegevens, evenals waarborgen dat binnen dat stelsel zorgvuldig wordt omgegaan met informatie (ook als die informatie niet als persoonsgegevens kwalificeert; vgl. bijvoorbeeld de bij randnummer 3.4 hierna opgesomde beginselen).

2.13 Wij bespreken hierna dan ook de huidige persoonsgegevensstromen (hoofdstuk 3) en de persoonsgegevensstromen bij meer regie op gegevens (hoofdstuk 4) in relatie tot de AVG. Daarna gaan wij in op het evenwicht tussen meer regie en behoud van waarborgen (hoofdstuk 5). Wij sluiten af met een conclusie (hoofdstuk 6).

3 Persoonsgegevensstromen op dit moment

3.1 Persoonsgegevens van burgers stromen momenteel vaak rechtstreeks van een bepaalde bron naar een dienstverlener.[9]

3.2 De bron of bronregistratie is de plaats waar een persoonsgegeven voor de eerste keer is vastgelegd, zoals inkomensgegevens van werknemers bij een werknemer of geboorteaktes van inwoners bij een gemeente. De dienstverlener is de persoon of organisatie die voorziet in het leveren van een afgebakende prestatie (dienst) aan haar omgeving, in welk kader de dienstverlener persoonsgegevens over een burger of bedrijf zal willen ontvangen.

3.3 Er bestaat in die gevallen, zo is het uitgangspunt, voor de bron een grondslag om die persoonsgegevens te verstrekken aan de dienstverlener. Dat kan zowel een specifieke grondslag zijn in een bijzondere wet, als een algemene grondslag van de AVG.[10]

3.4 Die grondslagen gaan steeds gepaard met waarborgen voor de betrokken burger (ook wel: de betrokkene) die – in de regel – rusten op de verstrekkende bron en de ontvangende dienstverlener als verwerkingsverantwoordelijken.[11] 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**).[12]

3.5 Ook moet een zogenoemde gegevensbeschermingseffectbeoordeling/**DATA PROTECTION IMPACT ASSESSMENT (DPIA)** worden uitgevoerd door een verwerkingsverantwoordelijke voorafgaand aan een verwerking die een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, zoals bij een structurele verstrekking van gevoelige (zogenoemde bijzondere) persoonsgegevens[13] en moet rekening worden gehouden met de uitgangspunten van gegevensbescherming door ontwerp (*DATA PROTECTION BY DESIGN*) en gegevensbescherming door standaardinstellingen (*DATA PROTECTION BY*

9 Wij spreken hierna steeds over persoonsgegevens van burger en niet ook over gegevens van bedrijven, omdat bedrijfsgegevens veelal geen persoonsgegevens zijn (zie daarover randnummer 2.1 hierboven).
10 Artikel 6 AVG noemt – kort gezegd – als grondslagen: a) de ondubbelzinnige toestemming, b) de uitvoering of totstandkoming van een overeenkomst, c) een 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 van een derde.
11 De verwerkingsverantwoordelijke is een natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4, aanhef en onder 7, AVG). Wij gaan er in het vervolg van dit advies van uit dat de bron en de dienstverlener als verwerkingsverantwoordelijken kwalificeren. Of dat daadwerkelijk steeds het geval is, zal per geval aan de hand van de specifieke feiten en omstandigheden moeten worden bepaald.
12 Zie artikel 5, eerste lid, AVG voor de beginselen inzake de verwerking van persoonsgegevens.
13 Artikel 35 AVG e.v.

default).[14] Tot slot kunnen (of moeten[15]) tussen twee verwerkingsverantwoordelijken, zoals de bron en dienstverlener, **afspraken** worden gemaakt over de verwerking, bijvoorbeeld in een regeling of overeenkomst.

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

3.7 Tegelijkertijd heeft de burger weinig tot geen zicht op de verwerking c.q. uitwisseling van persoonsgegevens tussen de bron en de dienstverlener. Aan de voorkant zal de burger worden geïnformeerd over de verwerking van zijn persoonsgegevens op het moment dat deze bij hemzelf of bij een ander worden verzameld, maar in de AVG is niet geregeld dat de betrokkene zicht heeft op de individuele verwerkingen die nadien plaatsvinden.[16] In de situatie waarin ondubbelzinnige toestemming de grondslag voor de verwerking van persoonsgegevens is, wordt de betrokkene over de specifieke verwerking geïnformeerd alvorens hij toestemming geeft.[17] Toestemming kan echter alleen als grondslag dienen voor een verwerking als de toestemming vrijelijk is gegeven. Van 'vrijelijke toestemming' is geen sprake bij een duidelijke wanverhouding tussen de betrokkene en de verantwoordelijke. Dat kan zich voordoen bij de relatie werkgever-werknemer of de relatie overheid-burger.[18] Wil de burger in andere situaties zicht hebben op de persoonsgegevens die de bron en dienstverlener uitwisselen, dan moet de burger gebruikmaken van de rechten die in de AVG aan betrokkenen zijn toegekend. De burger zal die rechten actief moeten uitoefenen, teneinde concrete informatie over de verwerking van persoonsgegevens te verkrijgen.

3.8 Het belangrijkste recht dat de betrokkene heeft is zijn **inzagerecht**. Op grond daarvan heeft een betrokkene het recht om van een verwerkingsverantwoordelijke uitsluitsel te krijgen of over hem betreffende persoonsgegevens worden verwerkt, en, wanneer dat het geval is, om inzage te krijgen in die persoonsgegevens en geïnformeerd te worden over verschillende aspecten van de verwerking (zoals de doeleinden en de (categorieën van) ontvangers).[19]

3.9 Wanneer de grondslag voor de verwerking berust op ondubbelzinnige toestemming[20] of

14 Artikel 25 AVG. Data protection by design betekent dat bij de ontwikkeling van producten en diensten (zoals nieuwe informatiesystemen) al zoveel mogelijk aandacht moet worden besteed aan privacyverhogende maatregelen en aan het uitgangspunt van dataminimalisatie. Data protection by default houdt in dat door middel van standaardinstellingen zo privacyvriendelijk mogelijk wordt gewerkt.
15 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.
16 Artikel 13 en 14 AVG bevatten de informatieplicht.
17 Artikel 6, eerste lid, aanhef en onder a, AVG jo. artikel 4, aanhef en onder 7, AVG.
18 Artikel 4, aanhef en onder 7, AVG jo. artikel 7 AVG.
19 Artikel 15 AVG. Zie daarover ook hoofdstuk 2 van dit advies.
20 Artikel 6, eerste lid, aanhef en onder a, AVG (en voor de verwerking van bijzondere persoonsgegevens: artikel 9, tweede lid, aanhef en onder a, AVG).

op een overeenkomst[21] en de verwerking via geautomatiseerde procedures wordt verricht, kan een betrokkene voorts de hem betreffende persoonsgegevens in een gestructureerd, algemeen gebruikt en machinaal leesbaar formaat verkrijgen door gebruik te maken van zijn recht op overdraagbaarheid van gegevens (ook wel: het **RECHT OP DATAPORTABILITEIT**). Door gebruikmaking van dit recht kan een betrokkene zijn persoonsgegevens doorgeven van de ene dienstverlener aan een andere dienstverlener.[22]

3.10 Daarnaast bestaat er de mogelijkheid van **HERGEBRUIK** van persoonsgegevens. Hergebruik heeft echter (kort gezegd) betrekking op het gebruik van *openbare informatie*,[23] neergelegd in documenten, voor andere (commerciële of niet-commerciële) doeleinden dan het oorspronkelijke doel waarvoor de informatie binnen de *publieke taak* van een instelling is geproduceerd.[24] Het gaat dus niet om een recht van de betrokkene op hergebruik van de hem betreffende persoonsgegevens, maar om hergebruik van openbare overheidsinformatie.

> Voor zover met de term 'hergebruik' wordt gedoeld op het gebruiken van de eigen persoonsgegevens door een betrokkene voor een ander doel dan waarvoor hij de persoonsgegevens aanvankelijk heeft verkregen, wijzen wij op randnummer 5.2 hierna.

Deelconclusie

3.11 Gelet op het bovenstaande vinden op dit moment de uitwisselingen van persoonsgegevens tussen een bron en dienstverlener plaats op basis van een met waarborgen omklede grondslag. Tegelijkertijd heeft de betrokkene weinig zicht op de verstrekkingen. De (zelf) beschikking van de burger is beperkt tot de informatie die hij verkrijgt bij aanvang van een verwerking en eventueel door zijn AVG-rechten te effectueren. Zo kan een burger verzoeken om inzage in zijn persoonsgegevens. In sommige gevallen heeft de betrokkene ook recht op overdraagbaarheid van zijn persoonsgegevens of heeft hij geïnformeerd toestemming kunnen geven voor de verwerking van zijn persoonsgegevens. Uitoefening van deze rechten leidt niet automatisch tot (meer) regie op gegevens.

21 Artikel 6, eerste lid, aanhef en onder b, AVG.
22 Artikel 20 AVG.
23 Dat de voor hergebruik gevraagde informatie openbaar moet zijn, volgt uit artikel 2, eerste lid, aanhef en onder a, Wet hergebruikvan overheidsinformatie (hierna: Who), waarin is bepaald dat de Who niet van toepassing is op informatie die niet openbaar is op grond van de wet (bijvoorbeeld op grond van de Wet openbaarheid van bestuur of de Archiefwet).
24 Artikel 1, aanhef en onder b, Who.

4 Persoonsgegevensstromen bij regie op gegevens

4.1 Burgers meer regie geven op hun (persoons) gegevens geven, impliceert de introductie van een nieuw stelsel voor uitwisselingen van persoonsgegevens. Persoonsgegevens die nu tussen een bron en dienstverlener worden uitgewisseld, zonder dat een burger daar (direct) zicht en grip op heeft, gaan straks via de burger lopen.[25] De meerwaarde van (een afsprakenstelsel voor) regie op gegevens is dat burgers niet alleen vooraf worden geïnformeerd over een verwerking van hun persoonsgegevens, maar constant inzichtelijk is welke persoonsgegevens door wie worden verwerkt.

4.2 Bij experimenten met regie op gegevens zullen partijen zich veelal willen committeren aan initiatieven voor RoG-systemen en dus bereid zijn de burger de gewenste regierol te geven. Bij de doorontwikkeling en implementatie van een dergelijk systeem zal de vraag rijzen of de centrale regiefunctie van de burger juridisch kan worden afgedwongen. Beschikt de burger, met andere woorden, over juridische mogelijkheden om zijn regiefunctie uit te oefenen?

4.3 Die vraag is niet eenvoudig te beantwoorden, omdat een dergelijk stelsel afwijkt van het huidige kader waarbinnen uitwisselingen van persoonsgegevens plaatsvinden en waarop wet- en regelgeving is toegeschreven. Het antwoord zal moeten worden gevonden in de (waarborgen bij de) eerdergenoemde grondslagen voor het verstrekken van persoonsgegevens tussen bron en dienstverlener. Iedere grondslag bevat eigen aandachtspunten.

I Rechten van de betrokkene

4.4 Een grondslag kan allereerst worden gevonden in de rechten die in de AVG aan de betrokkene zijn toekgekend, te weten het inzagerecht en/of het recht op dataportabiliteit. De burger zou dan regie op zijn persoonsgegevens kunnen voeren door met een beroep op deze rechten zijn persoonsgegevens bij de bron op te vragen. Na verkrijging van de persoonsgegevens bij de bron kan de burger vervolgens zelf beslissen wanneer hij welke persoonsgegevens 'doorverstrekt' aan een dienstverlener.

4.5 Wij plaatsen daarbij – zoals reeds toegelicht in hoofdstuk 2 en bijlage 2 – de kanttekening dat de rechten van de betrokkene niet absoluut zijn. In de AVG en de Uitvoeringswet AVG zijn gronden opgenomen die de uitoefening van de rechten van de betrokkene kunnen beperken of de rechten in het geheel buiten toepassing kunnen laten, bijvoorbeeld in verband met het waarborgen van de openbare veiligheid of van toezicht- en inspectietaken.[26] Zouden burgers middels de AVG-rechten regie moeten voeren op hun persoonsgegevens, dan moet rekening worden gehouden met de situatie waarin een bron zich beroept op een van deze gronden en weigert persoonsgegevens te verstrekken aan of via een betrokkene. Daarnaast kan het recht op dataportabiliteit alleen worden geëffectueerd bij automatische verwerkingen van persoonsgegevens die zijn gebaseerd op toestemming of op een overeenkomst (zie randnummer 3.9 hierboven). Bij verwerkingen op grond van andere grondslagen[27] kan een bron niet onder verwijzing naar het recht op

25 Daarbij merken wij op dat er altijd gegevensstromen zullen bestaan die zich buiten het zicht van de burger voltrekken, bijvoorbeeld in de strafrechtelijke keten. Dergelijke verstrekkingen laten wij in dit advies buiten beschouwing.
26 Artikel 23 AVG en artikel 41 Uitvoeringswet AVG.
27 Zie voetnoot 10 voor alle AVG-grondslagen.

dataportabiliteit verplicht worden de burger beschikking te geven over zijn persoonsgegevens.

4.6 Daarnaast is de vraag of het recht op inzage en het recht op dataportabiliteit voldoende basis bieden voor een vorm van RoG waarbij alle persoonsgegevens onder de burger zelf komt te berusten (bijvoorbeeld via een agent of op het *device* van de burger). De genoemde rechten hebben een andere ratio en achtergrond dan het creëren van een verkrijgingsrecht of een opslagrecht voor de burger. Achtergrond van het inzagerecht is dat een betrokkene kan nagaan of de hem betreffende persoonsgegevens bij de bron of dienstverlener juist zijn en rechtmatig worden verwerkt. Zo niet, dan kan de betrokkene verzoeken om rectificatie of wissing dan wel rechtsmiddelen aanwenden tegen de verwerking van zijn persoonsgegevens. Achtergrond van het recht op dataportabiliteit is dat een betrokkene een set persoonsgegevens van een leverancier van een dienst kan doorgeven aan een nieuwe leverancier van diezelfde dienst. In beide gevallen zullen burgers een verzoek doen om hun rechten uit te oefenen. Het structureel en/of op grote schaal verstrekken van persoonsgegevens door een bron aan of via een betrokkene ten behoeve van RoG lijkt oneigenlijk gebruik van deze rechten. Daarvoor zal veelal een stevigere en specifiekere wettelijke basis nodig zijn.

4.7 Bovendien hebben genoemde rechten – als gezegd – alleen betrekking op de *persoonsgegevens* die de verwerkingsverantwoordelijke (zoals de bron) verwerkt en niet op documenten als zodanig en/of op geattesteerde beweringen, noch op andere gegevens dan persoonsgegevens.

II Een overeenkomst

4.8 Daarnaast zou een overeenkomst kunnen worden gesloten die als grondslag dient voor het verwerken van persoonsgegevens via de burger.[28] Een dergelijke overeenkomst zal – gelet op de formulering van deze grondslag in de AVG – in ieder geval met de betrokkene zelf moeten worden gesloten. Verder bevat de AVG geen nadere eisen met wie een overeenkomst moet worden gesloten. Lastig voorstelbaar is dat een overeenkomst tussen een burger en een dienstverlener een bron kan verplichten persoonsgegevens te leveren, nu overeenkomsten in de regel alleen contractspartijen binden. Een driepartijencontract zou daarom als basis kunnen dienen.

4.9 Wij merken daarbij op dat de overeenkomst als verwerkingsgrondslag doorgaans betekent dat uit hetgeen waarover gecontracteerd is, volgt dat voor de uitvoering van die overeenkomst noodzakelijkerwijs persoonsgegevens moeten worden verwerkt (denk aan de noodzakelijkheid om adresgegevens te verwerken als gevolg van het sluiten van een overeenkomst over de bezorging van een pizza). Vraag is of men middels algemene afspraken een grondslag kan creëren voor een stelsel van regie op gegevens en hoe zich dat verhoudt tot het beginsel van doelbinding en de regels omtrent verdere verwerking van persoonsgegevens.

> Vgl. overweging 44 AVG: “Een verwerking die noodzakelijk is **IN HET KADER VAN** een overeenkomst of een voorgenomen overeenkomst, dient rechtmatig te zijn.”

28 Artikel 6, eerste lid, aanhef en onder b, AVG.

4.10 Daarnaast is de vraag hoe vrij een burger staat om het sluiten van een overeenkomst te weigeren omdat hij geen persoonsgegevens wil delen, als dat betekent dat hij daarmee geen aanspraak meer kan maken op het product of de dienst die hij geleverd wil krijgen. Aan de voorkant moet rekening worden gehouden met deze mogelijk kwetsbare positie van burgers.

III Ondubbelzinnige toestemming

4.11 Tot slot zou de ondubbelzinnige toestemming van de betrokkene ten grondslag kunnen worden gelegd aan het verwerken van persoonsgegevens binnen een systeem voor RoG.[29] Idee is dan dat de burger uitwisselingen van persoonsgegevens tussen bron en dienstverlener goed- of afkeurt door al dan niet zijn toestemming te geven. Een bron of dienstverlener zou dan om een *go* van de burger vragen om bepaalde persoonsgegevens uit te wisselen. Aandachtspunt daarbij is dat toestemming alleen als grondslag voor een verwerking kan dienen als sprake is van een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting.[30] Als sprake is van een wanverhouding tussen de toestemmingvrager- en gever kan de toestemming niet als grondslag dienen (zie randnummer 3.7 hierboven). Daarnaast heeft een betrokkene het recht te allen tijde zijn toestemming in te trekken. Vanaf het moment van intrekken vervalt de grondslag voor de betreffende verwerking.[31]

4.12 Voor de hand ligt dat dat de bron die de persoonsgegevens heeft, toestemming vraagt van de betrokkene en vastlegt dat de toestemming is verkregen.[32] Ook een dienstverlener kan de toestemming van de burger vragen. De bron moet zich dan wel voldoende comfortabel voelen om op basis van die toestemming persoonsgegevens uit te wisselen. Dat vergt mogelijk het maken van afspraken.

Deelconclusie

4.13 Gelet op het bovenstaande zijn er verschillende banden waarover een centrale positie voor de burger in een nieuw systeem van persoonsgegevensstromen kan worden bereikt, met ieder eigen aandachtspunten.

29 Artikel 6, eerste lid, aanhef en onder a, AVG.
30 Artikel 4, aanhef en onder 11, AVG.
31 Artikel 7, derde lid, AVG.
32 Op grond van artikel 7, eerste lid, AVG moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven. Gelet daarop verdient het aanbeveling dat de bron de toestemming documenteert.

5 Evenwicht tussen meer regie en behoud van waarborgen

5.1 Met een nieuwe stelsel voor persoonsgegevensstromen – waarin regie van de burger centraal staat – wordt getornd aan het huidige gesloten ecosysteem van grondslagen, doelbinding en andere waarborgen zoals omschreven in hoofdstuk 3. De vraag is hoe de leemten die ontstaan, kunnen worden opgevuld. Per RoG-initiatief zal men moeten nagaan of tegemoet kan worden gekomen aan (de ratio achter) de huidige waarborgen.

De basis voor regie op persoonsgegevens, doelbinding en dataminimalisatie

5.2 De inrichting van het systeem en bijbehorende grondslag is bepalend voor de vraag of en zo ja, hoe het stelselevenwicht kan worden teruggebracht. Kiest men bijvoorbeeld het inzagerecht (of het recht op dataportabiliteit) als grondslag voor het verwerken van persoonsgegevens via een systeem van RoG, dan kan de burger gewoonweg zijn eigen persoonsgegevens verzamelen bij de bron, zonder dat de bron zich ervan hoeft te vergewissen waarom de burger zijn persoonsgegevens opvraagt en wat de burger (dan wel de dienstverlener die de persoonsgegevens via de burger ontvangt) met die persoonsgegevens gaat doen. Een burger heeft simpelweg een recht op inzage in de hem betreffende persoonsgegevens, ongeacht het oogmerk waarvoor hij zijn persoonsgegevens vraagt. Verder staat het de burger vrij te doen met zijn persoonsgegevens wat hij wil. Aandachtspunt is wel dat de burger alleen recht heeft op zijn persoonsgegevens met het oog op controle van de juistheid en rechtmatigheid daarvan en niet ook op de documenten waarin de persoonsgegevens voorkomen.

5.3 Tegelijkertijd zal de burger moeten worden beschermd tegen bepaalde doorverstrekkingen, bijvoorbeeld het te makkelijk verstrekken van persoonsgegevens in ruil voor producten of diensten. Mogelijk moet daarvoor een extra waarborg worden ingebouwd in een afsprakenstelsel voor regie op gegevens.

5.4 Als de grondslag voor het nieuwe stelsel wordt gevonden in een overeenkomst, dan zal de bron wel voor iedere verstrekking moeten nagaan of de verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van de overeenkomst. Is het haakje de toestemming van de burger, dan zal de bron alleen persoonsgegevens mogen verstrekken als de burger vrije, specifieke en geïnformeerde toestemming heeft gegeven. In beide gevallen is er dan dus een limitering van de hoeveelheid persoonsgegevens die van de bron, via de burger, naar de dienstverlener kunnen vloeien.

5.5 Een andere vraag is of de bron zich er ook van moet vergewissen dat de ontvangende partij – de burger of de dienstverlener – de persoonsgegevens wel conform de AVG zal gaan verder verwerken. Bij randnummer 5.2 is reeds toegelicht dat dat bij gebruikmaking van de rechten van de betrokkene niet het geval is. Ook bij de uitvoering van een overeenkomst of bij toestemming draagt de bron in beginsel geen verantwoordelijkheid voor de wijze waarop een ontvanger (de burger of de dienstverlener) met de persoonsgegevens omgaat, nadat de bron de persoonsgegevens rechtmatig heeft verstrekt. Dat geldt zowel als de bron op verzoek van de burger of dienstverlener persoonsgegevens verstrekt als wanneer de bron op eigen initiatief persoonsgegevens verstrekt.

5.6 Dat doet niet af aan het feit dat zowel de bron als de ontvanger gebonden zijn aan het doeleinde of de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verkregen. Voor een verdere verwerking die onverenigbaar is met het aanvankelijke doel, is in beginsel de toestemming van de betrokkene vereist.[33]

De basis voor regie op persoonsgegevens en de juistheid, opslagbeperking en beveiliging

5.7 Een andere vraag is wie zorgdraagt voor de juistheid, opslagbeperking en beveiliging van de persoonsgegevens. Tot het moment van verstrekking is de bron verantwoordelijk voor de kwaliteit en veiligheid van de persoonsgegevens. Zodra de dienstverlener persoonsgegevens ontvangt, is ook hij verantwoordelijk voor de kwaliteit en veiligheid van de persoonsgegevens. Voorstelbaar is dat afspraken worden gemaakt tussen de bron en dienstverlener over bewaartermijnen en veiligheidsmaatregelen, zodat persoonsgegevens veilig kunnen worden uitgewisseld.

5.8 Als persoonsgegevens via de rechten van de betrokkene bij een dienstverlener terechtkomen, is het aan de burger om al dan niet zorg te dragen voor de kwaliteit en veiligheid van zijn persoonsgegevens. Dat brengt het risico mee dat onjuiste of verouderde persoonsgegevens bij een dienstverlener worden aangeleverd. Voorstelbaar is daarom dat de dienstverlener verlangt dat hij persoonsgegevens rechtstreeks van de bron ontvangt of dat de dienstverlener eisen stelt om de authenticiteit en actualiteit van de persoonsgegevens. In dat geval ligt voor de hand dat een andere grondslag, zoals de overeenkomst, wordt gekozen.

33 Artikel 6, vierde lid, AVG.

6 Conclusie

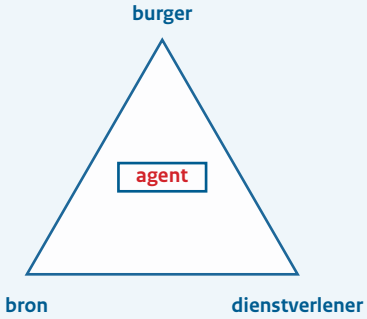
6.1 Tot zover onze notitie, waarin wij hebben geconcludeerd dat:

- Op dit moment het systeem voor persoonsgegevensstromen met bijbehorende grondslagen waarborgen biedt voor de veilige verwerking van persoonsgegevens, maar beperkte inzage- en zelfbeschikkingsmogelijkheden biedt voor burgers (hoofdstuk 3);
- De centrale positie voor de burger in een nieuw systeem van persoonsgegevensstromen mogelijk over verschillende banden kan worden bereikt, met ieder eigen aandachtspunten (hoofdstuk 4); en
- Bij het kiezen van de band waarover een systeem met meer regie wordt vormgegeven, moet worden nagedacht over het behoud van privacyrechtelijke waarborgen (hoofdstuk 5).

Bijlage 1

Model 1

1 Wat zit er in de agent?



in agent **digitale kluis**

Stelling en attestatie

Wat nodig	Ecosysteem	Afsprakenstelsel
ID burger en bron	Centrale authentieke bron	Wanneer attestator trusted?
Trusted attestator		Zero Knowledge Proof

Model 2

2 Wat zit er in de agent?

in agent **digitale kluis**

Kopie document en attestatie

Wat nodig	Ecosysteem	Afsprakenstelsel
ID burger en bron	Centrale authentieke bron	Wanneer kopie trusted?
Trusted kopie en attestator	Decentrale kopie bron	vertrouwensdienst
Grondslag verkrijgen kopie (is niet de AVG en/of eIDAS)		Wanneer attestator trusted?

Model 3

3 Wat zit er in de agent?

in agent **digitale kluis**

Origineel document en authentiek document

Wat nodig	Ecosysteem	Afsprakenstelsel
Bewijs authenticiteit	Decentrale authentieke bron	Wanneer document authentiek
Grondslag verkrijgen authentiek document (is niet de AVG en/of eIDAS)	Centrale authentieke bron	vertrouwensdienst
Koppeling decentraal en centraal ID burger		Koppeling tussen centraal en decentraal

Bijlage 2 De AVG, hergebruik en/of het vrije verkeer van gegevens als zelfstandige grondslag voor een afsprakenstelsel?

1 Recht van inzage van de betrokkene (artikel 15 AVG)

- Geen inzagerecht ten aanzien van andere gegevens dan persoonsgegevens, bijvoorbeeld bedrijfsgegevens.
- Als sprake is van persoonsgegevens, ziet het inzagerecht alleen op de persoonsgegevens en niet ook op de dragers van persoonsgegevens, zoals documenten. Een stelsel van regie op gegevens gaat mogelijk wel uit van regie op de drager van gegevens en/of op geattesteerde beweringen, althans het enkel hebben van een kopie van persoonsgegevens kan onvoldoende zijn om het stelsel te laten werken.
- Inzage kan worden geweigerd (artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG).
- Het structureel en/of op grote schaal verstrekken van persoonsgegevens door een bron aan of via een betrokkene ten behoeve van Regie op Gegevens (RoG) middels het inzagerecht lijkt oneigenlijk gebruik van dit recht. Daarvoor zal veelal een stevigere en specifiekere wettelijke basis nodig zijn.

2 Recht op overdraagbaarheid van gegevens (artikel 20 AVG)

- Ook het recht op dataportabiliteit (“overdraagbaarheid van gegevens”) beperkt zich tot persoonsgegevens, kan worden geweigerd en vormt een te wankele basis voor het structureel en/of op grote schaal verstrekken van persoonsgegevens door een bron aan of via een betrokkene ten behoeve van RoG. De hierboven opgenomen haken en ogen aan het inzagerecht gelden dan ook onverkort voor het recht op dataportabiliteit.
- Daarnaast kan het recht op dataportabiliteit alleen worden ingeroepen bij verwerkingen van persoonsgegevens die berusten op toestemming of een overeenkomst en als die verwerkingen via automatische procedures worden verricht.

3 Overeenkomst (artikel 6, eerste lid, aanhef en onder b, AVG)

- Ziet ook alleen op persoonsgegevens. Zie hierboven.
- Daarnaast roept dit andere vragen op. Kan regie op gegevens bijvoorbeeld contractueel worden afgedwongen? En zo ja, hoe? Wat moet een overeenkomst minimaal bevatten en met wie wordt deze gesloten?

4 Toestemming (artikel 6, eerste lid, aanhef en onder a, AVG)

- Ziet ook alleen op persoonsgegevens. Zie hierboven.
- Er kan sprake zijn van een afhankelijke relatie tussen toestemminggever en toestemmingontvanger. Daarnaast kan toestemming worden ingetrokken.

5 Hergebruik en vrij verkeer van gegevens

- Hergebruik als bedoeld in de Wet hergebruik van overheidsinformatie (Who) heeft wel betrekking op (informatie neergelegd in) documenten, maar ziet alleen op *openbare* overheidsinformatie. Persoonlijke informatie van burgers en concurrentiegevoelige informatie van bedrijven is veelal niet openbaar en openbaarmaking daarvan zal in veel gevallen ook niet wenselijk zijn.

- Er zijn initiatieven vanuit de EU ten behoeve van het vrije verkeer van gegevens. Die initiatieven zien echter op open data en open access en dus op gebruik van naar zijn aard openbare informatie. Vgl. de opmerking hierboven over persoonlijke informatie en bedrijfsgevoelige informatie.

- Ten behoeve van het vrije verkeer van *persoonsgegevens* is de AVG in het leven geroepen. Die beoogt het vrije verkeer van persoonsgegevens te bevorderen en tegelijkertijd het recht op bescherming van persoonsgegevens te waarborgen (vgl. overweging 10 AVG).

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!