

‘Burgers en bedrijven in regie op hun gegevens’

Discussiepaper



November 2015

Leeswijzer

Discussiepaper voor het programma “Burgers en Bedrijven in Regie over hun Gegevens”.

Het doel van dit discussiepaper is het ondersteunen van de bestuurlijke dialoog over ontwikkelingen rondom afsprakenstelsels, waarbij burgers en bedrijven hun persoonlijke gegevens kunnen gebruiken in dienstverleningsprocessen van andere organisaties dan waar het gegeven van afkomstig is. Dit principe heeft gevolgen voor de rol, processen en organisatie van overheidsorganisaties en de Generieke Digitale Infrastructuur.

In dit stuk wordt ook een doorkijk gegeven hoe deze ontwikkeling zich kunnen verhouden tot de huidige eOverheidsbouwstenen. Deze perspectieven zijn bedoeld ter inspiratie en discussie. Daartoe kunnen ze afwijkend zijn van bestaande visies en ontwikkeling. Dit discussiepaper vertegenwoordigt niet de positie of het standpunt van betrokken overheidspartijen.

Het programma Regie op Gegevens loopt tot juni 2016. De bedoeling is dat dit stuk wordt doorontwikkeld naar een overheidsvisie ten aanzien van het gebruik van afsprakenstelsels voor het delen van gegevens door burgers en bedrijven. Input hiervoor zijn onder meer de bestuurlijke dialoog, gesprekken met mensen van binnen en buiten de overheid, experimenten met Qiy en TrustTester van TNO en de beantwoording van een aantal beleidsvraagstukken ten aanzien van o.a. beveiliging, privacy en open standaarden.

November 2015

Voor meer informatie over dit stuk, suggesties of vragen kun u contact opnemen met Petra Mettau
p.mettau@minfin.nl

Inhoudsopgave

Samenvatting	4
1. Inleiding.....	5
2. Het wat en waarom van Persoonlijk Data Management (PDM)	6
2.1. Hoe verhoudt Persoonlijk Data Management zich tot Big Data en Open Data?	7
3. Wat is het nut van Persoonlijk Data Management?.....	8
3.1. Perspectief Persoonlijk Data Management voor personen.....	9
3.2. Perspectief Persoonlijk Data Management voor ondernemers	9
3.3. Economisch potentieel van Persoonlijk Data Management.....	9
3.4. Impact Persoonlijk Data Management voor overheid.....	10
4. Wat is er nodig om tot Persoonlijk Data Management te komen?	11
4.1. Waarom wordt er gekozen voor een infrastructurele oplossing?.....	12
4.2. Hoe werkt het principe van ‘toestemming’ geven voor gegevensuitwisseling?	13
5. Welke infrastructuren / afsprakenstelsels zijn er nu?.....	14
6. Hoe werkt het delen van gegevens in de praktijk?	15
6.1. Welke rollen kan de overheid hebben bij PDM en afsprakenstelsels?	16
7. Hoe verhoudt deze ontwikkeling zich tot de eOverheids bouwstenen?	17
8. Hoe helpt PDM om privacy te managen?.....	21
9. Maar, wat, als	22
10. Wat zijn de volgende stappen?	24

Dit discussiepaper van het programma 'Burgers en bedrijven in regie op hun gegevens' (ROG), geeft een overzicht van de nationale en internationale ontwikkelingen waarbij de burger (of een ondernemer) mogelijkheden heeft om gegevens, die over hem gaan, in te zien en te gebruiken op een veilige en betrouwbare manier

Dit concept van Persoonlijk Data Management is gebaseerd op het verbeteren van de digitale zelfbeschikking van individuen over hun gegevens op een manier die enerzijds het privacy verlies minimaliseert en anderzijds de maatschappelijke baten maximaliseert. Het is in feite een omkering van het door organisaties zelf verzamelen van data die al zijn vastgelegd, bijvoorbeeld in een basisregistratie. Bij Persoonlijk Data Management wordt de burger in staat gesteld om op een eenvoudige en overzichtelijke manier zelf gegevens uit een bron aan te leveren aan een derde partij.

In Nederland zijn twee afsprakenstelsel in ontwikkeling waarmee burgers en ondernemers de mogelijkheid krijgen om regie te hebben over eigen persoonlijke- of bedrijfsgegevens. Het Qiy afsprakenstelsel wordt in samenwerking met internationale private en publieke organisaties ontwikkeld en is beschikbaar om diensten op aan te bieden. TNO ontwikkelt met private en publieke partijen TrustTester, een validatieservice waarbij een bewering van een burger wordt getoetst bij een bron, zonder dat daar gegevens worden uitgewisseld.

Voor de overheid is een aantal rollen te onderscheiden bij het totstandkomen, gebruiken en beheren van een afsprakenstelsel. De overheid kan persoonlijke gegevens, bijvoorbeeld uit basisregistraties, ontsluiten voor de burger. Ook kan de overheid diensten aanbieden waarbij gegevens van bijvoorbeeld burgers, private of publieke organisaties nodig zijn. De overheid kan ook participeren bij het totstandkomen van een afsprakenstelsel, het invullen van bepaalde dienstverleningsrollen of in de toezichtfunctie. Per stelsel kan de rol van de overheid verschillend zijn. Voorzien wordt dat er meerdere stelsels naast elkaar kunnen bestaan.

Persoonlijk Data Management (PDM) zal op termijn een plaats moeten krijgen in het landschap van de eOverheid. De wijze waarop zal de komende jaren uitkristalliseren. Denk daarbij aan (de manier van) ontsluiten van (basis)registraties, het faciliteren van inzage- en correctierecht door middel van afsprakenstelsels, de rol en functie van MijnOverheid bij het ontsluiten van persoonlijke gegevens, het gebruik maken van contactgegevens die de burger zelf vastlegt en ontsluit voor de overheid, het bieden van waarborgen ten aanzien van diensten die door derden worden aangeboden en waar overheidsgegevens voor gevraagd worden.

Tot slot: inherent aan het ontwikkelen van dit type afsprakenstelsels is dat er een nieuwe innovatiedynamiek ontstaat die gekenmerkt wordt door ecosystemen van co-creërende spelers: groot en klein, publiek en privaat. Dat betekent dat de overheid niet alleen een potentiële gebruiker is, maar ook een rol of diverse rollen kan oppakken bij het tot stand komen van stelsels. Dit discussiepaper geeft inzicht in verschillende aspecten van Persoonlijk Data Management om binnen de overheid een bestuurlijke dialoog te ondersteunen over de rol en mogelijkheden voor de overheid bij het ontwikkelen, implementeren en gebruiken van afsprakenstelsels voor regie op gegevens door burgers en bedrijven.

Dit discussiepaper van het programma 'Burgers en bedrijven in regie op hun gegevens' (ROG), geeft een overzicht van de nationale en internationale ontwikkelingen waarbij de burger (of een ondernemer) mogelijkheden heeft om gegevens, die over hem gaan, in te zien en te gebruiken op een veilige en betrouwbare manier.

Deze ontwikkeling is een omkering van het huidige denken over gegevensuitwisseling tussen (overheids)organisaties, waarbij in feite gegevens over een burger¹ worden uitgewisseld, vaak zonder dat deze daar op dat moment van af weet. De omkering ontstaat doordat de burger centraal staat in het uitwisselen van gegevens die over hem gaan. Hij is zelf de regisseur. Hij heeft toegang tot zijn (gevalideerde) persoonlijke gegevens en kan deze al dan niet ter beschikking stellen aan, gebruiken voor een dienst van een andere organisatie of voor een wettelijke verplichting.

Persoonlijke gegevens zijn voor het individu steeds meer een 'middel' dat hij wil inzetten in het maatschappelijk verkeer, net zoals geld een betaalmiddel is. Hij heeft toegang tot het geld dat hij 'bezit' en kan zelf bepalen waar hij het aan uitgeeft. Op deze wijze heeft de burger ook recht op toegang en controle over 'zijn' data. In dit stuk worden onder 'persoonlijke gegevens' die gegevens verstaan waar het individu zelf toegang toe en regie over heeft. Dit betekent niet dat de betreffende persoon deze gegevens zelf altijd kan veranderen, zonder toestemming van degene die ze beheert. Net zo als met geld, kan je niet een extra 'nul' achter het gegeven 'spaarsaldo' op de bank zetten.

De laatste jaren is in binnen- en buitenland een aantal concepten ontstaan om de burger de regie over zijn eigen gegevens te geven. In dit discussiestuk duiden we de modellen en concepten die hieraan ten grondslag liggen. Hiervoor introduceren we het begrip Persoonlijk Data Management (PDM). Drie principes die aan de basis liggen van PDM, zijn:

- 1) Regie op gegevens: het recht van individuen om hun eigen data, die hen betreft, die door anderen verzameld en beheerd wordt, te (laten) managen. Het individu is zich daarbij bewust van de keuzes, en de impact die de keuzes hebben, om persoonlijke gegevens ter beschikking te stellen. Individuen zijn geen passieve dataproducten, maar worden in staat gesteld om in de online en offline wereld hun zaken te regelen en wanneer nodig daarbij zelf gebruik te maken van hun persoonlijke gegevens. Ook wanneer die gegevens bij een andere instantie zijn opgeslagen, zoals je geboortedatum bij de GBA.
- 2) Beschikbare data: Individuen hebben toegang tot de data die bij anderen over hen wordt vastgelegd en beheerd. Deze data is technisch makkelijk te ontsluiten, maar kent vaak juridisch nog de nodige vraagstukken. Het gebruik van deze data gebeurt met een beveiligde en betrouwbare infrastructuur.
- 3) Open infrastructuur: Voor het ontsluiten van de individuele, vaak persoonsgebonden gegevens, is een open infrastructuur beschikbaar waarbinnen meerdere aanbieders acteren. Deze infrastructuur staat de gebruikers toe om van meerdere aanbieders gebruik te maken, zodat er geen 'vendor lock-in' ontstaat.

In deze discussiepaper gaan we in op vraagstukken rond PDM. Daarnaast beschrijft een aantal hoofdstukken de achtergrond van PDM, internationale en nationale ontwikkelingen, de rol van de overheid en de verhouding met de huidige eOverheidsbouwstenen.

¹ In de loop van dit stuk wordt meer over burgers dan over bedrijven in regie over hun gegevens gesproken. Onderdeel van het programma Regie op Gegevens is echter ook, in samenwerking met EZ, te kijken naar de mogelijkheden van PDM voor bedrijven.

Het doel van PDM is om individuen te voorzien van toegang tot persoonlijke gegevens en het kunnen gebruiken van die gegevens wanneer zij dat willen. Hierbij is het noodzakelijk dat organisaties die persoonlijke gegevens beheren, deze beschikbaar stellen (voor dienstverlening) aan het betreffende individu. Beschikbaar stellen hoeft niet te leiden tot het daadwerkelijk verstrekken van informatie, het kan ook gebruikt worden om een gegeven te valideren. Ook kan een burger eenvoudig een derde toegang tot bepaalde, specifieke gegevens verschaffen. Het gaat daarbij om allerlei verschillende gegevens, bijvoorbeeld gegevens uit de basisregistraties van de overheid, gezondheidsgegevens, gegevens van de persoon of ondernemer zelf of gegevens van private organisaties. Denk ook aan data over telecommunicatie, verkeer, financiën of over gegevens die zijn gecreëerd door het internet- of wifigebruik van de betreffende persoon. De beherende partij kan dus zowel een overheidsinstantie zijn als een private partij.

Persoonlijk Data Management verandert de wijze waarop organisaties gegevens over burgers en ondernemers verkrijgen. Dit concept vertrekt vanuit het principe dat de burger of ondernemer centraal staat en daarin een actieve rol heeft (van 'citizen centric' naar 'citizen-driven'). PDM is een manier van gegevensuitwisseling die principes van digitale dienstverlening zoals transparantie, inzage en correctie, digitale zelfbeschikking, privacy, dataminimalisatie, kwaliteitsverbetering van gegevens en zelfredzaamheid van de burger kan versterken. Daarmee is PDM tevens een uitwerking van de beginsels 'privacy by design' en 'security by design'.

De waarde van persoonlijke gegevens voor de verschillende stakeholders is groot. Volgens het World Economic Forum² wordt persoonlijke data een nieuwe economische activa, een waardevolle bron voor de economie van de 21^{ste} eeuw die alle aspecten van de samenleving zal raken. Het huidige exponentieel groeiende gebruik van persoonlijke gegevens wordt steeds vaak in verband gebracht met de deflatie van privacy.

Momenteel hebben individuen weinig of geen controle over hoe gegevens gemaakt en gebruikt worden door ondernemingen, overheidsorganisaties of informatiemakelaars. Het concept van PDM is gebaseerd op het verbeteren van de digitale zelfbeschikking van individuen over hun gegevens op een manier die enerzijds het privacy verlies minimaliseert en anderzijds de maatschappelijke baten maximaliseert.

Persoonlijk Data Management is een nieuwe ontwikkeling die het, door dit Kabinet omarmde, principe van eenmalige gegevensverstrekking ondersteunt, doordat vooraf gevalideerde gegevens uit de bron aangeleverd worden met medeweten of expliciete goedkeuring van de persoon die het aangaat. Dit is een wijziging ten opzichte van de huidige situatie, waarbij (overheids)organisaties onderling de betreffende informatie uitwisselen en verzamelen, voordat ze deze informatie aan de burger presenteren. In de nieuwe situatie is er een infrastructuur beschikbaar die de betreffende informatie direct uit de bron inleest en op het scherm van de burger presenteert. Al dan niet in de vorm van een applicatie om een dienst aan te vragen of aan een

Er bestaan verschillende rechten ten aanzien van persoonsgevoelige gegevens. Bij regie over gegevens gaat het minimaal over het recht op toegang en gebruik van persoonlijke gegevens.

- Recht om te weten welke persoonlijke gegevens er van je bestaan
- Recht van inzage in je actuele persoonlijke gegevens
- Recht van correctie van onjuiste persoonlijke gegevens
- Recht op transparantie zodat je weet door wie de gegevens worden gebruikt
- **Recht op toegang tot je persoonlijke gegevens en deze vrij te mogen gebruiken**
- Recht om je persoonlijke gegevens te delen of te verkopen
- Recht om persoonlijke gegevens te (laten) verwijderen

² <http://www.weforum.org/projects/rethinking-personal-data>

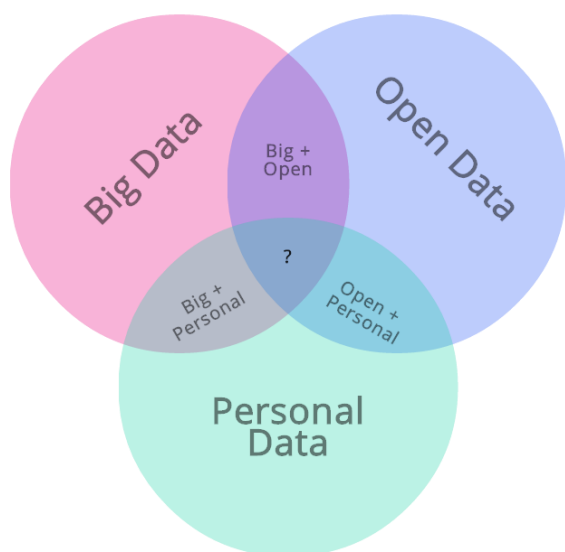
2.1. Hoe verhoudt Persoonlijk Data Management zich tot Big Data en Open Data?

De toename van data analytics en het gebruik van Big Data leidt tot vraagstukken rond privacy, ethisch gebruik en de invloed van het gebruik van algoritmes op besluitvorming, integriteit en transparantie. Big Data en PDM zijn twee complementaire ontwikkelingen.

Waar Big Data de mogelijkheden benadrukt van het potentieel om grote hoeveelheden (open) data te combineren en te analyseren, (vaak) vanuit het perspectief van organisaties, focust PDM zich op de waarde van het individueel gebruik van (besloten) gegevens. Beide concepten hebben belang bij het accountable en transparant zijn over hoe data wordt verzameld en gebruikt. Het accountable en transparant zijn geldt ook voor de algoritmes die worden gebruikt en de werking van zelflerende systemen.

Open Data zijn datasets van overheidsinformatie die openbaar gepubliceerd worden door publieke partijen voor hergebruik door anderen. Het is data waar geen restricties in verband met privacy, veiligheid of anderszins op rusten, welke in een machine leesbare structuur is opgebouwd en daarnaast beschikbaar is in een open formaat. Open Data is juridisch en technisch beschikbaar voor iedereen om te gebruiken.

Bij persoonlijke data gaat het om persoonlijke gegevens die juist wel persoonsgerelateerd (privacygevoelig) zijn. Deze gegevens zijn vervolgens technisch en juridisch beschikbaar voor de betreffende burger/bedrijf om in te zien, te gebruiken en te distribueren zoals hij dat zelf wil binnen de gestelde voorwaarden.



Figuur 1 – schematische weergave Big, Open en Personal Data³

³ <https://github.com/theodi/data-definitions/blob/gh-pages/img/venn.png>

3. Wat is het nut van Persoonlijk Data Management? FS-20151216.06A

In de huidige situatie geven personen juridisch toestemming aan private organisaties voor het gebruik van hun gegevens. Dit gebeurt door het accepteren van, vaak uitgebreide en ingewikkelde, algemene gebruikersvoorwaarden, meestal zonder deze voorwaarden gelezen te hebben. Hierdoor verzamelen organisaties veel informatie over personen, waarbij het vaak onduidelijk is waarom die informatie nodig is. Daarnaast kunnen veel diensten niet worden afgenomen wanneer je niet accoord wilt gaan met het afstaan van persoonlijke gegevens. Denk aan de apps die vragen om toegang tot je persoonlijke adresboek, terwijl het alleen maar een app is waarmee je wilt bijhouden wat je favoriete recepten zijn of wat vandaag de afstand is die je hebt gefietst.

De manier waarop infrastructuur voor Persoonlijk Data Management momenteel worden ontwikkeld, combineren digitale zelfbeschikking en de behoefte van bedrijven aan klantgegevens. Individuen kunnen zelf informatie verzamelen over zichzelf uit verschillende bronnen. Met deze informatie kan iemand vervolgens op zoek naar een dienst of service. Daarbij kan hij, indien mogelijk, deze zoektocht anoniem laten plaatsvinden en zich pas kenbaar maken wanneer hij gekozen heeft om een dienst af te nemen.

Het uitgangspunt dat personen toegang en regie over hun persoonlijke gegevens zouden moeten hebben, is grotendeels ontwikkeld vanuit de wetenschap en door private initiatieven. Vaak door middel van 'Working Groups' waar iedereen aan mee kan werken die er in is geïnteresseerd.

In de samenleving beginnen de eerste toepassingen te ontstaan. In de media zijn steeds meer nieuwsberichten over het verzamelen van persoonlijke informatie door bedrijven waardoor mensen een beter begrip krijgen hoe organisaties kennis over hen opbouwen en gegevens over hen doorverkopen. De Big Brother Award van Bits of Freedom speelt daar ook op in door aandacht te vragen voor privacy⁴. De vraag is of het nodig is dat het individu zelf bezig moet zijn met het zoeken naar oplossingen. Het internet en smartphones zijn ook ontwikkeld zonder de toets of er wel een individuele behoefte was aan webwinkels of apps.

Het concept van regie op gegevens, of beter; Persoonlijk Data Management, wordt binnen de publieke sector steeds meer herkend als mogelijkheid om een oplossing te bieden voor het toenemende gegevensgebruik, als ook de mede daaruit voortvloeiende privacy vraagstukken, en het uitgangspunt van eenmalige gegevensverstrekking.



Figuur 2 - wat willen burgers met gegevens?

Bron: Nederlanders over persoonlijke data. InnoValor/Newcom Research & Consultancy. September 2015

⁴ <https://www.bof.nl/2015/10/21/achmea-microsoft-en-ronald-plasterk-genomineerd-voor-big-brother-awards/>

De strategische verkenning uit 2014 van SGO9 over Burgers en Bedrijven in Regie op Gegevens geeft aan dat door PDM er efficiënter hergebruik kan plaatsvinden, betere gegevenskwaliteit ontstaat, en het privacy-dilemma kan worden verholpen. Daarnaast biedt het een oplossing voor het vraagstuk van privaat gebruik van overheidsgegevens en kan invulling gegeven worden aan het vraagstuk over inzage- en correctierecht.

3.1. Perspectief Persoonlijk Data Management voor personen

Voor personen ontwikkelt PDM zich tot een makkelijk te gebruiken digitale infrastructuur voor het persoonlijk managen van data, transparantie over beschikbare data, mogelijkheden voor correctie en persoonlijk hergebruik, het verhogen van de privacy en mechanismen die laten zien welke organisaties persoonlijke gegevens gebruiken. De gegevens zullen zowel ingezet kunnen worden in het private als in het publieke domein. Doordat personen inzicht hebben in veel meer persoonlijke gegevens, en doordat deze ook op informatieve wijze gepresenteerd kunnen worden, is er een verhoogd inzicht in eigen gedrag, situatie en mogelijkheden. Als de consument meer mogelijkheden heeft om persoonlijke gegevens te gebruiken in de interactie met bedrijven, wordt zijn positie als consument versterkt. Tot slot ontstaan er andere mechanismen voor het benutten van de intrinsieke economische waarde van de eigen persoonlijke gegevens, wat overigens wel tot maatschappelijke discussies leidt. Zie het kader met het voorbeeld van Achmea. Wat is het standpunt van de overheid wanneer de burger gegevens, die door de overheid worden beheerd, kan inzetten voor aanbiedingen of kortingen van commerciële dienstverleners?

Praktijkvoorbeeld Loonaangifteketen

De Loonaangifteketen is begonnen met een verkenning met TrustTester en de hypothecaire sector voor het valideren van inkomensgegevens die benodigd zijn bij een hypotheekaanvraag. De hypotheekverstrekker heeft inkomensgegevens nodig. De aanvrager geeft op wat haar inkomen is. Via TrustTester wordt aan het UWV gevraagd of het inkomen dat het UWV heeft overeenkomstig het bedrag is dat de burger heeft opgegeven. De burger krijgt dit antwoord en beslist zelf of zij dit gevalideerd doorstuurt naar de hypotheekverstrekker.

3.2. Perspectief Persoonlijk Data Management voor ondernemers

Een ondernemer of bedrijf is ook een gebruiker zijn van 'Persoonlijk' Data Management. Van een ondernemer of bedrijf zijn gegevens bij verschillende bronnen aanwezig, zoals bij de Kamer van Koophandel, overheidsorganisaties, banken, verzekeraars en kredietverstrekkers. Gegevens kunnen hergebruikt worden in transacties met de overheid of private partijen en als instrument in digitaal toezicht. Bij bedrijven speelt privacy op een andere manier. Concurrentiegevoeligheid speelt een grote rol. Bovendien heeft een bedrijf vaak meerdere werknemers die geautoriseerd zijn voor een deel van de bedrijfsgegevens. Voor ZZP'ers zijn bestaande concepten zoals Qiy en TrustTester waarschijnlijk evenzeer van toepassing als voor individuele burgers. Dit uitgangspunt zal meegenomen worden bij de doorontwikkeling van het Ondernemingsdossier naar "Mijn overheid voor bedrijf". Door hergebruik van reeds beschikbare gegevens kan PDM bijdragen aan efficiëntie en lastenverlichting van bedrijven en overheid.

3.3. Economisch potentieel van Persoonlijk Data Management

PDM is gebaseerd op open standaarden en ondersteunt interoperabiliteit en het gemakkelijk uitwisselen van gegevens. Dit verlaagt de toetredingsdrempel voor nieuwe bedrijven. Organisaties die zich nu oriënteren op PDM, zien nieuwe businessmodellen en dienstverleningsconcepten ontstaan. PDM kan leiden tot het vergroten van het consumentenvertrouwen in bedrijven die met persoonsgevoelige data werken. Aan de dienstenkant

zullen dienstverleners betere, goedkopere en meer op de consument toegespitste producten kunnen leveren, doordat ze direct kunnen beschikken over gevalideerde gegevens die nodig zijn voor hun dienstverlening.

Hergebruik van gegevens uit vertrouwde bronnen leidt tot lagere kosten voor controle en validatie. De transactiekosten voor het verkrijgen van betrouwbare data kunnen lager worden, doordat niet meer aparte gegevensmakelaars hoeven te worden ingeschakeld. Er kan direct gebruik gemaakt worden van de diverse infrastructuren voor het verkrijgen van benodigde gegevens, die door de klant zelf worden aangeleverd. Nieuwe vormen van marktonderzoek en Customer Relationship Management zullen ontstaan. Individuen zullen hun gegevens (anoniem) ter beschikking stellen aan door hen geselecteerde bedrijven of bedrijfstakken om tot een aanbieding te komen. De klantrelatie kan daardoor veranderen in een meer door het individu gestuurde relatie.

Praktijkvoorbeeld Achmea

Achmea biedt premiekorting bij het delen van privé gegevens. De verzekeraar geeft klanten die een meetkastje installeren in hun auto of huis en de gegevens delen met de verzekeraar, maandelijks korting op de premie. In het PDM concept is het de persoon zelf die een meetkastje aanschafft en kan beschikken over de informatie. Vervolgens kan hij zelf beslissen de informatie met een organisatie, al dan niet anoniem, te delen om te komen tot een beter passende verzekering of premie.

3.4. Impact Persoonlijk Data Management voor overheid

De overheid kan met PDM een ontwikkeling stimuleren waarbij privacy en innovatie nieuwe mogelijkheden krijgen. Enerzijds door bronnen te ontsluiten voor de burger of de ondernemer. Anderzijds kan de overheid PDM gebruiken om zelf, via de burger of ondernemer, sneller geverifieerde informatie te verkrijgen, bijvoorbeeld bij het aanvragen van een huurtoeslag, een vergunning of de aanvraag voor een uitkering. Daarmee is PDM in potentie een belangrijke nieuwe bouwsteen binnen het stelsel van eOverheid dienstverlening.

Een aantal afsprakenstelsels en protocollen die PDM ondersteunen, hebben als uitgangspunt dat ze voldoen aan (toekomstige) EU data wetgeving. Hierdoor biedt PDM de perspectief voor het dilemma dat kan ontstaan tussen hergebruik van gegevens en de privacy regelgeving.

Behalve het ontsluiten van gegevens of het aanbieden van diensten is er nog een aantal vraagstukken bij toepassing van PDM ten aanzien van het ter beschikking stellen en (her)gebruik van persoonlijke gegevens door de overheid en bedrijfsleven, zoals het waarborgen van de privacy en de zelfredzaamheid van de burger. Deze vraagstukken kunnen aanleiding geven tot politiek-bestuurlijke vraagstukken. De rol van de overheid is om tijdig deze vraagstukken te agenderen.

PDM gaat uit van vertrouwen en hanteert daarbij 'trust frameworks' als basis voor een digitale infrastructuur die gericht zijn op het mogelijk maken van 'trust'. De wijze waarop een afsprakenstelsel wordt ingericht, de toegang wordt geregeld en er toezicht wordt gehouden, vraagt om meedenken door de overheid. Wanneer de overheid een bepaald stelsel wil gebruiken voor de eigen dienstverlening, komt ook het implementatievraagstuk ter sprake. Op welke wijze is de overheid betrokken bij de implementatie en het werkend krijgen van een PDM afsprakenstelsel?

Tot slot kan er sprake zijn van wet- en regelgeving die gemaakt of aangepast moet worden om afsprakenstelsels werkend te krijgen. Bijvoorbeeld ten aanzien van het ontsluiten van overheidsgegevens. Ook zullen er voorzieningen als Idensys nodig zijn om een betroubaar authenticatiemiddel te realiseren.

4. Wat is er nodig om tot Persoonlijk Data Management te komen?

FS-20151216.06A

Om de burger of het bedrijf gebruik te laten maken van persoonlijke gegevens, is een infrastructuur en een bovenliggend afsprakenstelsel nodig welke elders beheerde gegevens ontsluiten en waarmee een persoon deze gegevens zelf kan gebruiken.

Door in te zetten op data interoperabiliteit en portabiliteit, is het voor individuen mogelijk om van service provider (dianstaanbieder) te wisselen zonder dat er persoonlijke gegevens verloren gaan of er een 'vendor lock-in' ontstaat.

Dit wordt vormgegeven door zogenaamde afsprakenstelsels (trust frameworks). Het iDeal en GSM stelsel zijn de meest aansprekende voorbeelden. Door het internationale GSM afsprakenstelsels kan iedereen met iedereen bellen (ook al heb je beide een andere provider), is nummerportabiliteit mogelijk en kan je van provider veranderen. Het tijdperk van de juffrouw die je moest doorverbinden bij intercontinentale gesprekken ligt al ver achter ons.

Het Rathenau Instituut benoemt deze ontwikkeling als een coöperatief platform. Een platform⁵ is een gemeenschappelijke basis van technologieën, technologische, economische en sociale regels en afspraken (zoals standaarden) waarop meerdere spelers samen kunnen innoveren en aanvullende technologieën, producten en diensten kunnen ontwikkelen.

Platformen kunnen uiterst krachtig zijn en zowel economisch succes als snelle innovaties opleveren, maar ze kunnen ook het risico van machtsconcentratie met zich meebrengen. Het onderscheid tussen een platform en een afsprakenstelsel zit hem dan ook in de wijze waarop de machtsstructuur is ingeregeld: want platformen vaak één eigenaar hebben (Facebook, Google, Apple, Myspace, Twitter) richten afsprakenstelsels zich op een gedeelde macht, waarbij gebruikers van het stelsel medezeggenschap hebben.

Platformen en afsprakenstelsels zijn een universeel mechanisme achter een nieuwe innovatiedynamiek die zich aan het ontwikkelen is als gevolg van digitalisering.

Door te werken met afsprakenstelsels is het mogelijk voor de burger om regie op zijn eigen gegevens uit te voeren die elders worden beheerd, zonder de persoonlijke gegevens ergens in een digitale kluis op te moeten slaan om ze zo van daaruit te kunnen gebruiken. De kracht is juist dat de gegevens bij de bron blijven staan: het saldo van je spaarrekening bij de bank, het loongedeven bij de werkgever of in de polisadministratie, je diploma bij de school of instelling waar je het hebt behaald, authentieke gegevens in de desbetreffende overheidsbasisregistratie, etc. Door de wijze waarop de infrastructuur is opgebouwd, kan de ontvanger van de informatie verzekerd zijn van de betrouwbaarheid en actualiteit van de gegevens. Het is voor de burger niet altijd mogelijk om gegevens uit de bron te wijzigen, wanneer dit wel kan en gebeurt, is dat voor de ontvanger te zien.

Er zullen de komende tijd meerdere afsprakenstelsels voor het delen van persoonlijke gegevens ontstaan. De meeste van deze stelsels die nu in ontwikkeling zijn hebben privacy en dataminimalisatie als basisbeginselen. Een afsprakenstelsel voor PDM kan in beginsel sector onafhankelijk zijn. Sectoren kunnen echter kiezen voor een eigen uitwerking van een (bestaand) afsprakenstelsel. Voor de zorg kan bijvoorbeeld gekozen worden voor een eigen afsprakenstelsel (voor het Persoonlijk GezondheidsDossier). In de onderwijssector zien we

Vendor lock-in is het verschijnsel dat een klant zo zeer afhankelijk raakt van een leverancier dat afscheid nemen of overstappen niet langer mogelijk is zonder grote (financiële) gevolgen. Data lock-in gaat het over de onmogelijkheid om persoonlijke gegevens of andere data die je ergens hebt opgeslagen weer terug te halen. Voorbeelden zijn contact apps die niet te migreren zijn van het ene naar het nadere platform, of een aantal eBook leveranciers waarbij je het gekochte eBook alleen op een bepaalde eReader kan lezen.

⁵ Rathenau Instituut, De kracht van platformen, 2014

ontwikkelingen die gebruik maken van een bepaald afsprakenstelsel (UMA). In de financiële sector wordt geëxperimenteerd met meerdere afsprakenstelsels (Qiy, TrustTester). Voor de overheidsdienstverlening worden, in het kader van het programma Regie op Gegevens, momenteel verkenningen uitgevoerd met Qiy en TrustTester.

4.1. Waarom wordt er gekozen voor een infrastructurele oplossing?

⁶Toegang tot persoonlijke gegevens vraagt in veel gevallen om een technische oplossing. Door een aantal technische vernieuwingen, zoals Application Programming Interface (API), is het mogelijk om op een andere manier dan voorheen gegevens op individueel niveau te ontsluiten, met als doel om deze gegevens te kunnen hergebruiken voor publicatie elders. Programma's kunnen dus via API's toegang krijgen tot gegevens in een bepaalde applicatie. De huidige API economie is een wirwar van API's tussen allerlei verschillende organisaties. Voor elke uitwisseling moet je een nieuwe API afspreken.

Aanbieders van opslag van gegevens, en allerlei daarvan afgeleide diensten, organiseren dit vaak als een platform. Onder de voorwaarden van de platformeigenaar worden gegevens opgeslagen, bewaard en doorverkocht of gebruikt voor doeleinden van derden. Het veranderen van platform is vaak erg lastig. De Amerikaanse bedrijven als Facebook, Google, Apple en LinkedIn zijn hier voorbeelden van. Deze technische oplossing leidt vaak tot een zogenoemde 'data lock-in'.

De nieuwe infrastructuur voor Persoonlijk Data Management gaan uit van dienstverleners die opereren binnen vastgestelde afspraken waarin gebruik wordt gemaakt van een gestructureerde manier van gegevensuitwisseling via API's. Hierbij is er geen dominante partij die de werkwijze reguleert en is er een open stelsel voor meerdere partijen om diensten aan te bieden. Dit kent twee grote voordelen:

- 1) Gegevens blijven staan bij de bron: de persoon of organisatie die de gegevens heeft gemaakt en deze beheert, stelt de gegevens beschikbaar. Daardoor worden er geen kopieën op andere plaatsen bewaard. Kopieën kunnen leiden tot verminderde kwaliteit (vervuiling), bijvoorbeeld doordat gegevens niet actueel zijn. Er zal geen digitale kluis zijn waar van één persoon alle gegevens zijn opgeslagen. Wel zullen er plaatsen komen waar een burger of bedrijf 'zijn' eigen gegevens opslaat, bijvoorbeeld een kluis voor al je wachtwoorden of een clouddienst voor je foto's of documenten. Bedrijven hebben bijvoorbeeld hun bedrijfsadministratie, dat is ook een soort digitale kluis.
- 2) Het voorkomt een 'vendor en data lock-in'. Doordat gegevens gestructureerd langs een afsprakenstelsel opgevraagd kunnen worden, zonder dat daar een (technisch) platform aan ten grondslag ligt, maakt het mogelijk om te kunnen wisselen van aanbieder zonder dat daarbij direct alle 'eigen' data verloren gaat. Het ecosysteem wordt niet door één partij bepaald.



Figuur 3 - Gebaseerd op MyData⁶

⁶ https://www.lvm.fi/docs/en/3759139_DLFE-27119.pdf

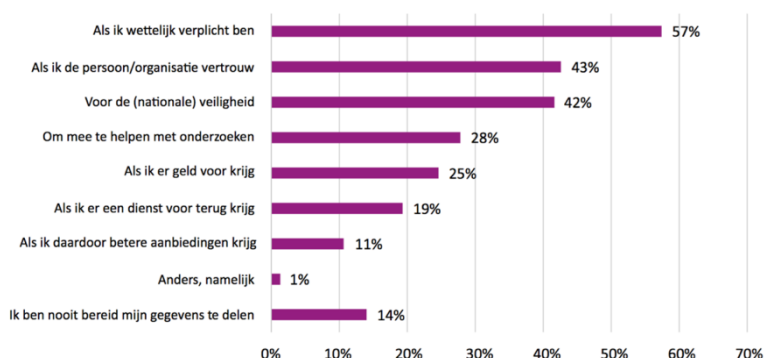
4.2. Hoe werkt het principe van 'toestemming' geven voor gegevensuitwisseling?

FS-20151216.06A

Bij PDM is het principe dat het individu 'toestemming' geeft voor een specifieke gegevensuitwisseling cruciaal. Deze toestemming is ingebouwd in de afspraken en infrastructuur, op een andere, aanvullende wijze dan in de huidige manier van gegevensuitwisseling. Denk daarbij aan delegatie (toestemming aan organisatie A om gegevens te sturen naar organisatie B) of doeluitbreiding (organisatie A mag het gegeven om een andere reden dan waarvoor het verkregen is, doorsturen naar organisatie B).

Bij de ontwikkeling van PDM infrastructuur blijft voor de overheid het uitgangspunt dat informatie waar een juridische basis voor is, zonder toestemming van de betreffende burger kan worden verkregen. Protocollen zoals Qiy en UMA (User Managed Access) erkennen dit uitgangspunt en hebben dit geïntegreerd in hun standaarden. Tevens voldoet dit protocol ook aan de toekomstige EU data protectie richtlijn.

PDM betekent niet dat er altijd toestemming nodig is voor gegevensdeling. PDM biedt wel de mogelijkheid om transparant te zijn en personen op de hoogte te kunnen brengen van het gebruik van gegevens die op hen betrekking hebben. Ook wanneer gegevens op basis van een wettelijke grondslag direct verkregen kunnen worden uit een externe databron, kan het mechanisme van PDM gebruikt worden: bij een wettelijke verplichting kan het gegevens wel via de burger aangeleverd worden, die kan dan de toegang niet weigeren. Zo wordt transparantie geborgd.



Figuur 4 - Wanneer willen burgers gegevens delen?

Bron: Nederlanders over persoonlijke data. InnoValor/Newcom Research & Consultancy. September 2015

Wereldwijd ontstaan verschillende oplossingen die inzetten op het versterken van de positie van het individu wanneer het gaat om het delen van persoonlijke gegevens. In Nederland is het Qiy afsprakenstelsel in januari 2015 met een eerste versie live gegaan. Het Nederlandse Qiy afsprakenstelsel is een privaat initiatief geborgd door de onafhankelijke en non-profit Qiy Foundation. In Amerika is het Kantara initiatief gestart met het ontwikkelen van het User Managed Access (UMA) protocol. Dit protocol wordt, samen met het Qiy Afsprakenstelsel, onder andere onderzocht door het Finse MyData initiatief dat in 2015 is gestart als een samenwerkingsverband tussen overheid, wetenschap en bedrijfsleven. Sinds 2011 heeft de Engelse overheid, in samenwerking met verschillende organisaties, MiData gestart en heeft in 2015 aangekondigd in samenwerking een financieel dashboard voor burgers te willen ontwikkelen. Tot slot is er Respect Network, dat zich vooral richt op het veilig, en met bescherming van de privacy, kunnen gebruiken van persoonlijke data op het Internet.

Daarnaast zijn er initiatieven zoals TrustTester van TNO. TrustTester richt zich op een validatieservice met bescherming van de privacy. Hierbij worden geen gegevens uitgewisseld, maar wordt een bewering van een burger, met zijn toestemming, getoetst bij een vertrouwde bron. De bron valideert of de informatie overeenkomt met de verstrekte informatie aan de afnemer, zonder dat de bron kan leren wie de afnemende partij is of voor welk doel de validatie dient. De burger geeft vervolgens zijn expliciete toestemming om het validatieresultaat (en dus niet het gegeven zelf) te verstrekken. Bijvoorbeeld een bewering over het inkomen bij het online aanvragen van een hypotheek kan door een burger worden gevalideerd bij de Loonaangifteketen. De potentie van TrustTester is aanzienlijk: zo kan de overheid persoonsgegevens van burgers valideren voor commerciële bedrijven, en vice versa, zonder te leren voor welke partij of voor welk doel dit gebeurt. Dit kan de betrouwbare digitalisering van processen helpen en kostenbesparingen opleveren.

Praktijkvoorbeeld Kennisnet

Kennisnet doet onderzoek naar de UMA-standaard. Gegevens van en over leerlingen en studenten zijn over meerdere partijen verspreid die in diverse onderwijsprocessen met elkaar samenwerken. Tussen deze partijen worden persoonsgegevens, waaronder ook leerresultaten, uitgewisseld over leerlingen/studenten en docenten. Momenteel is er geen transparantie in deze gegevensstromen en hebben de gegevenseigenaren geen of beperkt zeggenschap over het gebruik hiervan en hebben zij vrijwel geen inzage in het daadwerkelijk gebruik.

De verschillende stelsels vullen elkaar soms aan of maken bewust keuzes in het ontwikkelen van onderdelen van een stelsel. Zo wordt het UMA protocol en het Qiy afsprakenstelsel ingezet in pilots bij het Finse MyData initiatief. Een validatieservice als TrustTester kan een onderdeel zijn van een breder afsprakenstelsel als Qiy of MyData.

Overigens zijn er andere technologische ontwikkelingen die gerelateerd zijn aan het ontstaan van afsprakenstelsels of infrastructuren voor het delen van persoonlijke gegevens. Bijvoorbeeld de Blockchain ontwikkeling (de onderliggende techniek van de Bitcoins). Blockchain is een manier om veilig transacties te doen zonder een centraal systeem zoals een bank, een notaris of een overheid. Een andere ontwikkeling is die van een Uniform Economisch Transactie Protocol (UETP). Een set van open source afspraken om transacties te kwalificeren. Door informatie van transacties in UETP te bundelen via een soort beveiligde 'group chat', beschikken alle partijen die bij de transactie betrokken zijn automatisch over de data die voor hen relevant zijn. Waarbij er automatisch uitsluiting is van toegang tot data die voor partij(en) in de keten niet relevant zijn. Tot slot ontstaat door voortschrijdende technologie extra mogelijkheden om de privacy van burgers te beschermen. Zo is het mogelijk om zonder kennis te nemen van de data zelf berekeningen uit te voeren op data, zelfs als die verspreid is over meerdere partijen. Hiermee kunnen extra waarborgen voor de burger worden geboden. Een concreet voorbeeld van een dergelijke toepassing is het Enigma initiatief bij het Massachusetts Institute of Technology⁷. Randvoorwaarden hiervoor kunnen binnen publiek/private afspraken stelsels worden vastgelegd.

⁷ <http://enigma.media.mit.edu/>

6. Hoe werkt het delen van gegevens in de praktijk? FS-20151216.06A

Zoals in het vorige hoofdstuk is aangegeven, zijn er verschillende afsprakenstelsels en infrastructuren in ontwikkeling. In hoofdlijnen zijn veel van deze ontwikkelingen gebaseerd op de volgende werkwijze en onderverdeling in rollen:

De burger opent een account waarmee hij de toegang en het gebruik van zijn persoonlijke gegevens kan regelen. Er zijn meerdere account aanbieders en als individu kun je van aanbieder wisselen. Dit account, dat ook wel een domein of 'node' wordt genoemd, geeft de burger een omgeving voor het toegang krijgen tot gegevens en het toestemming geven aan andere partijen om gegevens te gebruiken. Het account is een soort basis voor de burger. In de praktijk zal hij vaak bij reeds bekende diensten of applicaties (die ook aangesloten/gecertificeerd zijn door het betreffende afsprakenstelsel) de vraag krijgen of hij toestemming wil geven om, via de PDM infrastructuur, de persoonlijke gegevens uit de verschillende bronnen vooraf in te willen vullen in de applicatie. Vervolgens kan hij bekijken of hij het eens is, eventueel data wijzigen (de ontvanger ziet of het gegeven uit een bron komt of door de burger is bewerkt) voordat hij de digitale dienst ondertekent en instuurt.

Organisaties kunnen persoonlijke data naar de burger of de ondernemer ontsluiten via de infrastructuur van het afsprakenstelsel. Daarmee geven zij de grondstof, het persoonlijke gegeven van de burger, vrij voor gebruik door die burger.

Deze organisaties, of anderen, kunnen diensten aanbieden waarbij deze gegevens noodzakelijk zijn. Bijvoorbeeld een hypotheekverstrekker die inkomensgegevens van de werkgever, UWV of Belastingdienst nodig heeft.

Praktijkvoorbeeld ABNAMRO en ING

ABNAMRO en ING hebben een pilot uitgevoerd met Qiy voor het hypotheekaanvraag proces. Het aanvragen van een hypotheek is een papieren proces waarbij de burger allerlei documenten aanlevert. Door dit te doen op basis van het Qiy Afsprakenstelsel, wanneer daar verschillende databronnen gebruik van maken, kan gebruik worden gemaakt van digitale, gecertificeerde informatie. De businesscase voor hypotheekverstrekkers is groot, het gemak voor de burger aantoonbaar. Daarnaast heeft dit neveneffecten voor bijvoorbeeld notarissen die ook sneller de benodigde informatie hebben, die tevens van een hogere kwaliteit en betrouwbaarheid is.

Hierboven zijn drie rollen beschreven die nodig zijn om tot diensten en producten te komen op basis van persoonlijke gegevens, die ter beschikking worden gesteld door de burger zelf.

Daarnaast is er een organisatie nodig die het afsprakenstelsel beheert. Die zal vaak ook een spelverdeler aanwijzen. Dat is de organisatie die zorgt dat de regels van het afsprakenstelsel worden toegepast. Een voorbeeld van een spelverdeler is SIDN, die alle .nl-domeinnamen registreert en beheert. Terwijl het ICANN de internationale organisatie is die het afsprakenstelsel rondom domeinnamen beheert. De spelverdeler kan, op basis van de afspraken, organisaties certificeren die accounts voor burgers afgeven, de infrastructuur leveren, gegevens ontsluiten of diensten aanbieden waarvoor de burger data moet aanleveren. Bij veel stelsels wordt voorzien dat een organisatie niet zomaar een dienst kan aanbieden waarbij persoonsgegevens moeten worden ingezet, deze organisatie zal zich eerst moeten inschrijven en akkoord moeten gaan met de afspraken van het stelsel, bijvoorbeeld ten aanzien van privacy en dataminimalisatie.

Tot slot is er een toezichtfunctie nodig om toezicht te houden op het functioneren van het stelsel en de actoren die daarbinnen opereren.

De overheid kan verschillende rollen hebben:

- Gebruiker van het afsprakenstelsel (data ontsluiten en diensten aanbieden)
- Faciliteren van onderdelen van het afsprakenstelsel
- Toezicht houden op het afsprakenstelsel
- Innovator en stimulator voor totstandkoming van afsprakenstelsels voor PDM

Gebruiker

In de dagelijkse praktijk kan de overheid data ontsluiten naar de burger of de ondernemer, zoals data uit de basisregistraties. Ook kan de overheid diensten aanbieden waarvoor de burger gegevens moet aanleveren zoals voor het aanvragen van een toeslag, het melden van een adreswijziging, het aanmelden op een nieuwe school of het aanvragen van studiefinanciering. In de praktijk zijn het vooral kennisproducten en diensten waar anders meerdere dienstverleners voor nodig zijn, die innovatie, efficiency en dienstverlening stimuleren. Een voorbeeld is een financieel dashboard waar je inzicht krijgt in je financiële positie en op basis daarvan advies kan vragen over producten of diensten.

Faciliteren

De overheid kan ook kiezen om onderdelen van het afsprakenstelsel te faciliteren. Denk bijvoorbeeld aan de mogelijkheid om accounts aan te bieden. Uit de eerste onderzoeken blijkt dat burgers een betrouwbare organisatie willen kiezen voor hun account, zoals de overheid of de banken, maar misschien ook wel de ANWB of XS4ALL. Het is denkbaar dat de overheid burgers een account aanbiedt, waarmee de burger door de overheid beheerde gegevens kan inzien en delen. Daarmee ontstaat in feite een andere functionele invulling van "mijn.overheid".

Praktijkvoorbeeld Wijzer in Geldzaken

De stuurgroep van Wijzer in Geldzaken liet een verkenning uitvoeren naar de haalbaarheid van een online omgeving met daarin persoonlijke financiële data van burgers. Om financiële beslissingen te nemen moeten burgers nu vaak veel moeite doen om gegevens vanuit verschillende kanalen bij elkaar te krijgen, met als gevolg dat zij dit achterwege laten. Dit kan leiden tot minder goede financiële beslissingen. Digitale ontwikkelingen bieden kansen om deze situatie te verbeteren. Vragen over privacy en veiligheid komen aan bod, en de potentie van afsprakenstelsels wordt in de verkenning besproken.

Toezicht

De overheid kan ook een rol spelen in het toezicht op een afsprakenstelsel.

Stimulator

Een laatste onderdeel waar de overheid een rol in kan hebben is het tot stand komen van het stelsel. Bij veel afsprakenstelsels is de overheid vanaf het begin een belangrijke initiator of deelnemer. In Nederland zien we dat bij de ontwikkeling van eHerkenning en Idensys. In een aantal landen (Engeland, Finland, Italië) is de overheid, samen met het bedrijfsleven, de initiator van een afsprakenstelsel of infrastructuur voor PDM. De Nederlandse overheid participeert met kennis en deskundigheid en doet ervaring op door middel van verkenningen en pilots. Dit is noodzakelijk om inzicht in de werking van het stelsel te krijgen en tot besluitvorming te kunnen komen of en op welke wijze de overheid gebruik wil en kan maken van een afsprakenstelsel.

In Nederland is rond 2007 een private partij, Qiy, begonnen met de ontwikkeling van dit gedachtegoed. Sinds 2010 zijn alle R&D activiteiten en de aandelen van Qiy BV overgedragen aan de stichting Qiy Foundation om expliciet te maken dat een afsprakenstelsel op onafhankelijke wijze het coöperatieve domein moet kunnen bedienen. Mede door de collaboratie met publieke en private partijen op het vlak van governance en legal affairs is besloten om de commerciële activiteiten te splitsen van de Qiy Foundation en onder te brengen in een aparte BV. Een en ander heeft per 1 januari 2015 geleid tot de afsplitsing van Qiy BV, die is hernoemd naar Digital Me.

Bij TNO is vanaf 2013 de ontwikkeling van een validatieservice onder de naam TrustTester gestart. Beide afsprakenstelsels kennen hun eigen focus.

7. Hoe verhoudt deze ontwikkeling zich tot de eOverheids bouwstenen?

FS-20151216.06A

Persoonlijk Data Management zal op termijn een plaats kunnen krijgen in het landschap van de eOverheid. De wijze waarop zal de komende jaren uitkristalliseren. Wel is een aantal lijnen te schetsen hoe bestaande eOverheidsvoorzieningen met deze ontwikkeling te maken kunnen krijgen.

De huidige eOverheidsvoorzieningen voor burgers zijn gericht op elektronische dienstverlening binnen het overheidsdomein (of private organisaties die een publieke taak uitvoeren). PDM leidt tot uitwisselen van gegevens tussen private en publieke domeinen. Bij bedrijven zijn er eOverheidsvoorzieningen die gericht zijn op het uitwisselen van gegevens tussen het publieke en private domein zoals SBR, e-factureren en eHerkenning.

PDM zal de huidige dienstverleningsconcepten mede veranderen, net zo als de ontwikkeling van mobiele interactie en de opkomst van nieuwe technologieën. Het zal de komende 3 tot 7 jaar echter niet het huidige landschap vervangen. Wel zal in de doorontwikkeling van een aantal eOverheidsvoorzieningen rekening gehouden kunnen (en mogelijk moeten) worden met het gebruik van PDM, mede als gevolg van Europese wet- en regelgeving. Bijvoorbeeld voor onderstaande voorzieningen en services. In de volgende paragrafen schetsen we enerzijds de huidige ontwikkeling en geven daarnaast een of meerdere perspectieven vanuit de ontwikkeling van PDM.

Identificatie en authenticatie

De Nederlandse overheid werkt samen met het bedrijfsleven aan een standaard voor de toegang tot online dienstverlening. Idensys maakt het mogelijk dat burgers, consumenten en ondernemers op termijn beter online zaken kunnen doen met overheid en bedrijfsleven. Idensys is een afsprakenstelsel voor authenticatie en autorisatie en is daarmee complementair op PDM stelsels die zich richten op het uitwisselen van gegevens. In Q1 van 2016 wordt onderzocht hoe Idensys en Qiy zich tot elkaar verhouden.

De identiteit van een persoonlijk account bij een PDM stelsel moet op een goed gekwalificeerde manier vastgesteld kunnen worden, afhankelijk van de gegevens die ontsloten worden of de dienst die wordt afgenomen. De bronhouder moet zekerheid hebben dat de persoonlijke gegevens die hij ontsluit ook daadwerkelijk van de burger zijn waarvoor hij zich uitgeeft (identificatie en authenticatie). Hiervoor kunnen verschillende partijen een rol spelen. Een mogelijkheid die nu verkend wordt, is het valideren van een persoonlijke Qiy node⁸ bij de gemeentelijke balie. Maar ook andere partijen, zoals notarissen, zouden dit kunnen doen.

Praktijkvoorbeeld Boxtel en Rotterdam

De gemeenten Boxtel en Rotterdam hebben een aantal customer journeys gemaakt met Qiy. Daarin hebben ze positief beproeft dat de gemeente de identificatie van een Qiy domein kan uitvoeren aan de balie (Stork4) of via Internet (Stork3). Tevens hebben ze aangetoond dat er vanuit de gemeentelijke administratie een basisset van identificerende gegevens geleverd kan worden aan de burger die deze gegevens vervolgens kan gebruiken in dienstverleningsprocessen van andere partijen. Ook is een aantal diensten gevisualiseerd zoals het aanvragen van een huurwoning, het overdragen van persoonlijke dossiers van gemeente A naar gemeente B bij verhuizing.

Burger service nummer (BSN)

Regelmatig wordt vanuit het bedrijfsleven de vraag gesteld of de BSN wetgeving verruimd kan worden en het BSN als identificerend nummer in het private domein kan worden gebruikt. De vraag is of dit nog nodig is, wanneer er met Idensys en een PDM stelsel gegevens kunnen worden uitgewisseld. Via een infrastructurele toegangsfunctionaliteit kan dan toegang tot gegevens worden gegeven door de burger zelf. In het ontwerp van Idensys zijn daarvoor pseudo-id's benoemd: een door een authenticatiedienst gegenereerd betekenisloos identificeren nummer van een persoon. In een koppelregister wordt de pseudo-id van een persoon gekoppeld

⁸ Binnen het Qiy Afsprakenstelsel spreekt met over een 'persoonlijk domein' of een 'node' om hiermee het individu op een interoperabele manier deel uit te laten maken van de digitale infrastructuur.

aan het administratieve nummer waaronder de persoon bekend is bij de dienstverleners. Om dat een sector kan gebruik worden gemaakt van een sectoraal nummer, bijvoorbeeld het BSN binnen de overheid.

Ontsluiten persoonlijke gegevens

Elke overheidsorganisatie kan afzonderlijk gegevens uit de bron ontsluiten. Op MijnOverheid/Persoonlijke Gegevens wordt voor een aantal veelgebruikte (authentieke) gegevens een inzagemogelijkheid gegeven. De ontsluiting vanuit de verschillende overheidsorganisaties is nu nog divers. Het streven van MijnOverheid is om dit te standaardiseren, in ieder geval voor de meest gebruikte bronnen. De service Persoonlijke Gegevens van MijnOverheid kan zich vanuit PDM op een aantal manieren ontwikkelen. MijnOverheid ontsluit een aantal veelgebruikte gegevens naar afsprakenstelsels waarover besloten is dat de overheid daar gegevens naar toe ontsluit. Het is aan de verschillende overheidsorganisaties om zelf extra gegevens te ontsluiten. Een andere optie is dat MijnOverheid geen gegevens meer ontsluit, dat doen de overheidsorganisaties zelf. MijnOverheid kan dan een webservice of applicatie bieden binnen een afsprakenstelsel om overzichtelijk een aantal overheidsgegevens te presenteren.

MijnOverheid

De website mijn.overheid.nl biedt op dit moment drie services. Een overzicht van een aantal persoonlijke gegevens, de berichtenbox voor burgers en een overzicht met lopende zaken. MijnOverheid biedt een landingsplaats voor de burger, maar het is technisch gezien ook een landingsplaats voor deze drie services. In de toekomst zullen deze services mogelijk ook aanroepbaar kunnen zijn op andere plekken, bijvoorbeeld een berichtenbox app.

Datzelfde kan ook mogelijk zijn voor het ontsluiten en delen van de persoonlijke gegevens. Bijvoorbeeld door middel van een PDM afsprakenstelsel. En wellicht wil de burger een overzicht van lopende zaken geïntegreerd hebben in zijn geïntegreerde digitale agenda of notificatie voorziening. Wanneer de burger ook ZZP'er is, kan hij voorzieningen uit het bedrijvendomein van de overheid integreren. MijnOverheid wordt dan een onderdeel die deze voorzieningen ontwikkelt en ter beschikking stelt. Daarnaast is het een plaats op Internet waar ik als burger weet dat dat de locatie is om eventuele instellingen te veranderen.

Een andere mogelijkheid is dat de MijnOverheid een plaats wordt waar de burger applicaties van de overheid of externe partijen kan vinden die gecertificeerd zijn voor een veilig en betrouwbaar gebruik in een bepaald stelsel. Een soort van appstore voor een PDM stelsel.

Contactgegevens

Contactgegevens zoals email adres of telefoonnummer zijn geen onderdeel van de basisregistratie persoonsgegevens. Overheidsorganisaties hebben soms de behoefte om te beschikken over deze informatie. Momenteel wordt een verkenning uitgevoerd door MijnOverheid waarin wordt onderzocht of het haalbaar en verstandig is dat een burger in MijnOverheid zijn e-mail, telefoon en andere contactgegevens aan kan geven, die door overheidsinstanties kunnen worden gebruikt om de burger te contacteren. De vraag is of dat nodig is wanneer in een PDM een burger altijd een plek heeft, waarschijnlijk op zijn persoonlijk account, om deze gegevens in te vullen en te laten gebruiken door afnemende organisaties.

Verminderen registraties

Wanneer in een PDM omgeving een goede identificatie en authenticatie plaats vindt, kan de burger op een betrouwbare manier informatie uitwisselen. Dusdanig dat de ontvangende partij zeker is van de herkomst van de informatie. Wanneer een burger zijn bankgegevens, zoals zijn rekeningnummer, koppelt aan zijn account en vervolgens een toeslag aanvraagt, kan de burger dit rekeningnummer doorgeven en weet de organisatie dat dit rekeningnummer bij deze burger hoort. Een eigen registratie van een achteraf gevalideerd rekeningnummer / naam rekeninghouder is daarmee in een aantal gevallen niet meer nodig.

Persoonsgebonden content

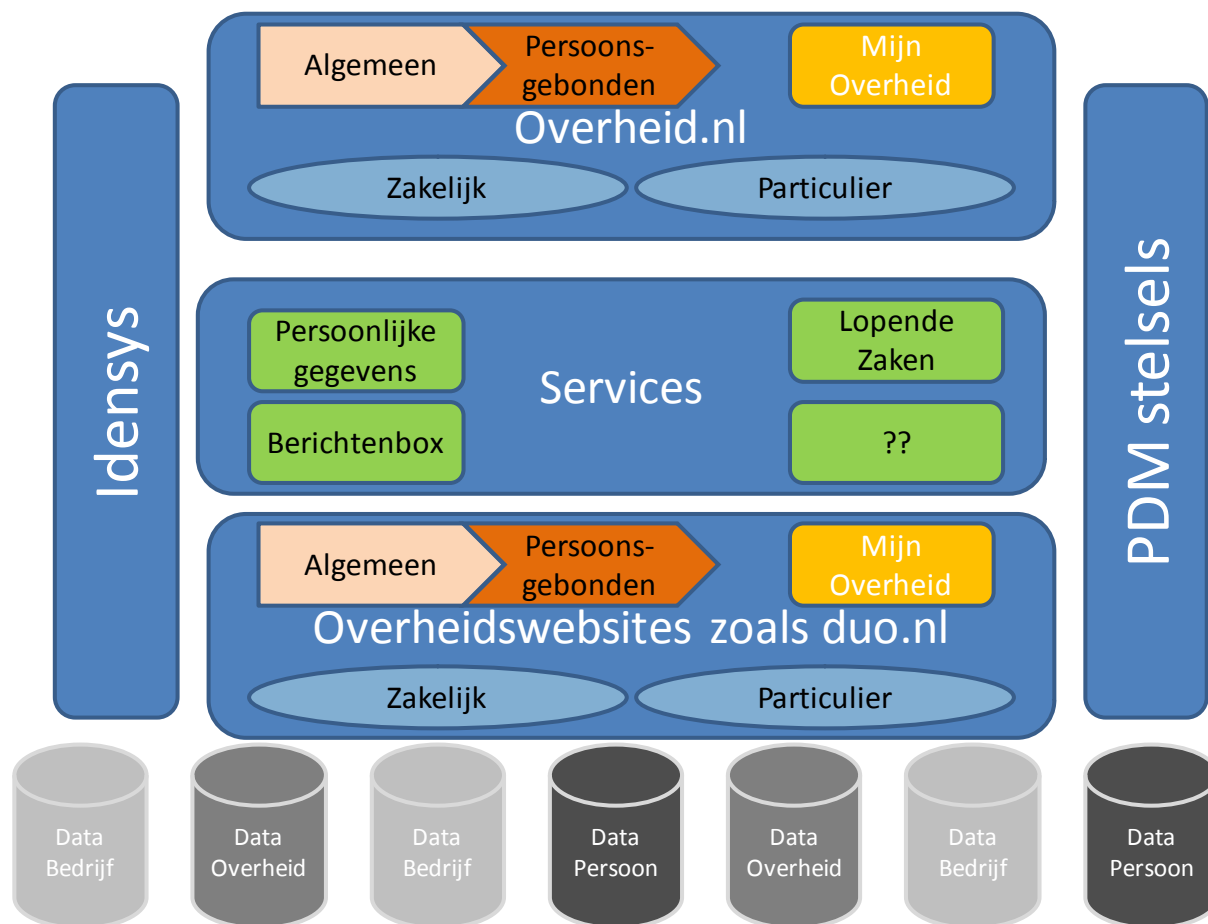
Het onderscheid tussen algemene content en persoonsgevoelige gegevens wordt, vanuit de burger en de ondernemer, steeds meer ervaren als een kunstmatig onderscheid. Al naar gelang de situatie en context van de burger heeft hij informatie nodig. Algemene content wordt daarmee persoonsgerichte content waar

persoonlijke gegevens al dan niet een onderdeel van zijn. Op veel websites is deze ontwikkeling te zien. Daarnaast biedt een bedrijf vaak één website aan waar een persoonlijk domein een onderdeel van is. De meeste overheidsorganisaties doen dat ook. Alleen de overheid in het algemeen nog niet. Deze informatie is nu versnipperd over diverse websites als www.overheid.nl, www.rijksoverheid.nl, mijn.overheid.nl. Er is nu niet één landingsplaats van waaruit de burger zijn zoektocht start. Overheid.nl wil zich wel ontwikkelen tot die ene landingsplaats voor overheidsinformatie. Door ontwikkelingen zoals PDM zal steeds meer informatie worden aangeboden op de plaats waar de burger dat zelf als eerste verwacht. De overheid dient er daarom ook voor te zorgen dat content (algemeen of persoonlijk) op het juiste moment en de juiste locatie veilig en overzichtelijk is te ontsluiten. Een perspectief is dat er één centrale locatie is waar de burger informatie kan vinden en een aantal basis zaken kan regelen zoals het aanvragen van een DigiD en het inkijken van mijn.overheid.nl. Daarnaast kan deze informatie en organisatiespecifieke informatie ontsloten worden in dienstverleningsapplicaties/-systemen die de burger of de ondernemer gebruikt.

Stelsel van overheidsgegevens

Het stelsel van basisregistraties of het stelsel van overheidsgegevens is een ander concept dan PDM. Het stelsel van basisregistraties en het stelsel van overheidsgegevens heeft het uitwisselen van gegevens tussen overheidsorganisaties onderling als onderwerp. In de discussie over het optimaal gebruik van het stelsel van overheidsgegevens zal ook het concept van PDM en het ontsluiten van gegevens naar PDM stelsels een onderwerp zijn.

Hieronder een schets van enkele eOverheidsvoorzieningen inclusief de PDM stelsels. Met als uitgangspunt het gebruik van gegevens uit zowel bestanden van de overheid, bedrijfsleven, de burger en de onderneming zelf.



Figuur 5 - Schets eOverheidsvoorzieningen en PDM

Het blok aan de rechterkant, PDM stelsels, geeft aan dat er een infrastructuur en afspraken zijn om de burger en ondernemer te ondersteunen in zijn regie over zijn gegevens. Aan de linkerkant de authenticatie en autorisatie diensten zoals door Idensys geleverd gaan worden.

Als algemene landingspagina voor overheidsinformatie wordt bovenaan in het middenblok www.overheid.nl gepositioneerd. Daarin kan de burger of de ondernemer zowel algemene informatie vinden als inloggen op zijn persoonlijke pagina (mijn.overheid.nl)

In het middenblok staan een aantal services aangegeven die de burger en ondernemer ondersteunen in zijn contact en interactie met de overheid. Daarin staan de huidige drie onderdelen van “mijn.overheid.nl” genoemd. Deze services kunnen ontsloten worden op andere plaatsen dan nu “mijn.overheid.nl”. Ook bijvoorbeeld via een Qiy stelsel.

In het onderste blok zijn de overheidsspecifieke websites gepositioneerd die bijna allemaal een eigen domein hebben zoals “mijn.duo.nl”.

De verschillende afsprakenstelsels en infrastructuren rondom PDM die op dit moment bestaan of in ontwikkeling zijn, hebben als uitgangspunt het beter beschermen van de privacy. Een mooi voorbeeld zijn de 12 Qiy Principles⁹, waarmee de individuele rechten worden gedefinieerd bij de uitwisseling van persoonsgegevens met andere partijen een op Qiy Principles gebaseerd Qiy Trust Framework. Alle partijen die hun diensten aanbieden binnen dit Qiy Trust Framework moeten zich houden aan deze regels.

1. Qiy Node

Een aan mij verstrekte Qiy Node voldoet aan de spelregels en de open standaard van het Qiy Afsprakenstelsel. Via mijn Qiy Node beheer ik mijn gegevens.

2. Mijn gegevens

Mijn gegevens mogen alleen met mijn toestemming worden gebruikt. Of die zich nu bevinden bij een organisatie of dat ik ze zelf heb gegeven.

3. Informatieplicht

Als een organisatie mijn gegevens wil gebruiken moeten ze me eerst informeren waarom ze dat willen en hoe vaak.

4. Data minimalisatie

Een organisatie mag mij alleen die gegevens vragen die echt nodig zijn voor het beoogde doel, of die gegevens gevalideerd zijn of niet.

5. Waarborgen

Wanneer een organisatie een waarborg vraagt over mij, moet de gevraagde waarborg echt nodig zijn voor het beoogde doel.

6. Keuze termijn ter beschikking stellen

Ik kan besluiten (een deel van) mijn gegevens éénmalig of voor een bepaalde periode ter beschikking te stellen. Ik kan dit besluit altijd wijzigen, tenzij er een contractuele reden is waarom dit niet kan.

7. Anonimiteit

Ik kan mijn gegevens altijd anoniem delen, behalve als dat wettelijk verboden is. In dat laatste geval kan ik kiezen of ik identificerende gegevens wil verstrekken of dat ik de transactie af wil breken.

8. Toegang

Organisaties die deelnemen aan het Qiy Afsprakenstelsel zijn verplicht mij 'toegang' te geven tot mijn gegevens. Dit geldt niet voor anonieme gegevens, maar verder wel voor alle gegevens die over mij gaan, ook als die ontstaan zijn op basis van gegevens die ik ter beschikking heb gesteld.

9. Delen van mijn gegevens

Organisaties mogen mijn gegevens alleen delen met een andere partij wanneer ik daarvoor toestemming heb gegeven. Deze toestemming kan niet 'voor altijd' zijn. De enige uitzondering is dat organisaties dit verplicht zijn vanwege bestaande wet of regelgeving. Dergelijke uitzonderingen moeten te allen tijde traceerbaar zijn.

10. Bescherming gegevens

Iedere partij die deelneemt aan het Qiy Afsprakenstelsel en mijn gegevens gebruikt of erover beschikt, beveiligt deze gegevens volgens de eisen die daar door de Qiy Foundation aan gesteld zijn.

11. Privacy statements

Voor iedere organisatie die via het Qiy Afsprakenstelsel met mijn gegevens te maken heeft, hebben deze Qiy Principles voorrang boven hun eigen privacy statements.

12. Klachten & geschillen

Als er een klacht is spreek ik eerst de direct betrokken organisatie aan. Dat kan ik doen via hun website. Als dat geen goed resultaat oplevert, mag ik de Geschillencommissie inschakelen.

⁹ <https://digital-me.nl/nl/consumer/qiy-principles/>

Het werken met afsprakenstelsels, zoals bij iDeal en het GSM netwerk, kunnen een krachtig instrument zijn om economische waarde toe te voegen. Ook kunnen ze snelle innovaties opleveren. Maar ze kunnen ook het risico van machtsconcentratie met zich meebrengen. Een afsprakenstelsel is een ecosysteem van cocreërende spelers. De structuur van het platform bepaalt de ruimte die geboden wordt aan een diversiteit van spelers, samenwerkingsrelaties en de vorm van concurrentie. Zo kan een coöperatieve samenwerkingscultuur terug te vinden zijn in het gebruik van open standaarden en open technologie.

Deze elementen brengen tegelijkertijd een aantal uitdagingen met zich mee. Wanneer stelsels in omvang en kracht toenemen, groeit de kans dat concurrentie wordt uitgesloten, gebruikers gevangen worden en overheden in een te afhankelijke positie komen. Dan ontstaan de meer herkenbare gesloten platformen zoals Google, Apple, Facebook en LinkedIn. Vanuit dit oogpunt is het van belang om monopolisering door een afsprakenstelsel tegen te gaan.

PDM afsprakenstelsels worden op dit moment vooral vorm gegeven vanuit de visie om de burger zijn privacy over gegevens terug te geven en de digitale zelfbeschikking te vergroten. Hoe ga je om met ongewilde neveneffecten of risico's? Kan een afsprakenstelsel, in zijn uitwerking tegenovergestelde effecten hebben. Bijvoorbeeld omdat een persoon toch verleid wordt om gegevens te verkopen voor goedkope dienstverlening. Is er impliciete dwang om gegevens ter beschikking te stellen? Op welke wijze probeert een stelsel hierop te anticiperen of dit te voorkomen.

PDM afsprakenstelsels beroepen zich er op dat er geen 'man-in-the-middle-aanval' mogelijk is, waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Persoonlijke data van een burger is minder kwetsbaar omdat het niet op één plek, in een digitale kluis, is opgeslagen maar in een groot aantal verschillende databases. Echter, wanneer het persoonlijke knooppunt van de burger wordt gehackt kan via dit knooppunt bij alle informatie worden gekomen die over de betreffende persoon is opgeslagen. En hoe wordt dit geregeld ten aanzien van de opsporing- en veiligheidsdienst? Elke systeem kan, zonder goede afspraken en toezicht, verworden tot een digitale dictatuur.

Wanneer een afsprakenstelsel Europees en internationaal gaat werken, kan dit heel veel voordelen hebben, ook voor het uitwisselen van overheidsinformatie. Echter zal dan een gedegen toezicht moeten bestaan en duidelijkheid wat het betekent wanneer je als individu via deze infrastructuur persoonlijke gegevens uitwisselt. Persoonlijk Data Management valt en staat met vertrouwen.

Er is nog een aantal bezwaren en risico's te benoemen, in dit hoofdstuk worden er slechts een aantal aangestipt. Inherent aan de totstandkoming van afsprakenstelsels is dat organisaties gezamenlijk deze vraagstukken op de agenda zetten en gemeenschappelijk tot antwoorden komen.

Het experimenteren met afsprakenstelsels als Qiy en TrustTester zal nog veel verschillende vraagstukken oproepen die besproken gaan worden. Denk daarbij aan vraagstukken ten aanzien van financiën, implementatie, vertrouwen van de burger, introduceren van en communiceren over een afsprakenstelsel, afwegen van de implementatietermijn en gewenste investeringen in relatie tot gebruik etc.

Het Rathenau instituut geeft tien handelingsopties voor de overheid om platformen¹⁰ of afsprakenstelsels te reguleren. Een aantal daarvan betreft de grote monopolistische platformen. Vijf aanbevelingen zijn van toepassing op de totstandkoming van PDM afsprakenstelsels: FS-20151216.06A

1. Moedig bedrijven aan bij het werk maken van platformen/afsprakenstelsels.
2. Stimuleer standaarden. Probeer als overheid standaarden te zetten of bevorder de totstandkoming daarvan als oplossing voor het kip-ei probleem.
3. Door te investeren in innovaties in voor de samenleving belangrijke domeinen wordt de mogelijkheid gecreëerd om invloed te hebben op de voorwaarden en toegankelijkheid van de kennis.
4. Wees extra kritisch bij bedrijfsovernames en fusies. Toegenomen macht geeft platformen de kans tot monopolisering en uitsluiting van concurrentie.
5. Zorg voor toegang in het intellectueel eigendomsrecht. Hoe meer patenten, hoe meer barrière voor nieuwe toetreders, met name kleine spelers.

¹⁰ Het Rathenau benoemt in het boek 'De kracht van platformen' vier typen van platformen. Het 'coöperatieve platform' komt overeen met de trusted frameworks en afsprakenstelsels waar dit discussie paper over gaat.

10. Wat zijn de volgende stappen?

In 2014 is, in opdracht van SGO9, een strategische verkenning gedaan naar de manier waarop burgers en bedrijven meer regie zouden kunnen krijgen bij het gebruik van persoonlijke gegevens en met name te duiden wat de nieuwe ontwikkelingen zijn naast het gebruik van digitale kluizen. Een van de uitkomsten van het advies om een programma te starten dat met een aantal vraagstukken aan de slag kon gaan rond afsprakenstelsels voor gegevensuitwisseling. En tevens een aantal experimenten op te starten.

De opdracht van het programma Burgers en bedrijven in regie over hun gegevens richt zich op het opdoen van ervaring met afsprakenstelsels en het vaststellen en waar mogelijk beantwoorden van de daaruit voortvloeiende (beleids)vragen. Tevens zorgt het voor het van de grond krijgen en versnellen van experimenten (waaronder verkenningen en pilots) met afsprakenstelsels zoals Qiy, TrustTester en UMA.

Daarnaast start het een bestuurlijke dialoog over een aantal onderwerpen die naar verwachting naar voren zullen komen. Deze discussiepaper is een aanzet om deze bestuurlijke dialoog te faciliteren.

In zijn blog¹¹ heeft de Digicommissaris aangegeven om in de huidige ontwikkeling van stelsels zoals Qiy en TrustTester hierin samen op te trekken. Daarbij zal de bijdrage van de overheid bestaan uit:

- Actieve bijdrage aan de verdere ontwikkeling van het publiek/private afsprakenstelsel.
- Uitsluitel geven aan Qiy Foundation en andere partijen welke rol en positie de overheid in een dergelijk afsprakenstelsel wil.
- Actief participeren in pilots om ervaring op te doen en vragen scherp te krijgen.

Besluitvorming en afstemming over dit traject zal, ook gezien het overheidsbrede karakter, in de governance van de Digicommissaris plaatsvinden.

¹¹ <https://www.digicommissaris.nl/blog-item/qiy>