Het landschap van Persoonlijk Data-Management

Oplossingen, concepten en afsprakenstelsels in samenhang

AUTEURS	Marlies Rikken, Wil Janssen, Ines Duits, InnoValor
REVIEW	Bob Hulsebosch, InnoValor
PROJECT	Digital We 2019
REFERENTIE	
DATUM / VERSIE	23/1/20, versie 1.4. Definitief
TOEGANGSRECHTEN	Publiek
EMAIL	marlies.rikken@innovalor.nl

Inhoud

Managementsamenvatting

Naarmate het belang van persoonlijke gegevens in de samenleving groeit, wordt het steeds urgenter om ervoor te zorgen dat individuen – inwoners, consumenten, burgers – in staat zijn toegang krijgen tot hun persoonlijke gegevens, deze kunnen hergebruiken en benutten. Dit is waar persoonlijk data management (of personal data sharing) oplossingen een rol hebben: de PDM oplossing is een intermediair tussen databronnen en diensten die data gebruiken. Het vertrouwen dat het individu stelt in de PDM-oplossing is daarbij van groot belang. Dit vertrouwen kan worden versterkt door het maken en gebruiken van een afsprakenstelsel waarin de regels en afspraken rondom gegevensuitwisseling en de onderlinge verantwoordelijkheden worden vastgelegd, zoals MedMij in de zorg of eHerkenning rond identiteiten.

Persoonlijk data management (PDM) heeft al een lange historie in Nederland en daarbuiten. Een doorbraak is echter tot nu toe uitgebleven. Tegelijk zien we de laatste paar jaar een explosie aan initiatieven. In de veelheid aan oplossingen, samenwerkingsverbanden, technologieën en standaarden kun je makkelijk verdwalen, zelfs als kenner, laat staan als geïnteresseerde nieuwkomer in het veld. Dit rapport helpt de weg weer te vinden in dit landschap, door zaken te ordenen en te duiden, zonder te oordelen.

Basisrollen

De basis van PDM omvat vier rollen: de persoon, de operator die controle over persoonlijke data biedt aan de persoon (ook wel PDM-dienst genoemd), data-aanbieders (ook wel bronnen of leveranciers genoemd) en data afnemers (ook wel *relying parties* genoemd). De persoon is een individu die zeggenschap heeft over het delen van zijn over haar data, voor eigen doeleinden, en heeft een relatie met de andere drie rollen. Een data-aanbieder verzamelt en verwerkt persoonlijke data die de andere rollen (inclusief de persoon) willen inzien of gebruiken. Een data-afnemer kan geautoriseerd worden om persoonlijke data van een of meerdere aanbieders te gebruiken. Een operator maakt het mogelijk voor het individu om veilig persoonlijke data in te zien, gebruiken en te managen. Daarnaast maakt de operator het mogelijk om de uitwisseling van persoonlijke data met en tussen data aanbieders en afnemers te controleren. Buiten deze rollen is kan er nog een rol of entiteit zijn die het beheer van de afspraken en toezicht op het systeem regelt (governance).

In de praktijk lopen deze rollen door elkaar. Vaak zijn data-aanbieders ook data-gebruikers en veel PDM-diensten combineren de operator rol met aanvullende opslag van data, waarmee ze ook bron kunnen zijn, al is het dan niet altijd de authentieke bron. Ook leveren ze soms afgeleide attributen, zoals “ik ben ouder dan 18” op basis van de geboortedatum.

Onderzoeksmodel

Om tot meer overzicht en inzicht te komen in dit landschap maken we aan de hand van ons PDM referentiemodel een analyse van PDM-initiatieven. Dit referentiemodel omschrijft de functionaliteiten die nodig zijn om PDM te laten werken. Functionaliteit kan verdeeld zijn of zelfs overlappen tussen de verschillende rollen in het ecosysteem: niet alles ligt bij de operator en sommige functies liggen bij alle rollen (zoals logging). Voor afsprakenstelsels geldt in de regel: ze stellen eisen aan de invulling van de functionaliteiten (opslag van data zal een afsprakenstelsel niet aanbieden, maar ze zal er wel eisen aan stellen). Deze analyse moet duiden welk onderscheid er is tussen de verschillende initiatieven.

Dit onderzoek heeft gelopen van april tot december 2019. In april zijn we gestart met het opzetten van het referentiemodel aan de hand van literatuuronderzoek en een analyse van een aantal bestaande oplossingen. In totaal zijn er 29 vragenlijsten verzonden, waarvan er 15 ingevuld retour zijn gekomen. Slechts één initiatief heeft aangegeven niet mee te willen werken, vanwege beëindiging van het initiatief.

Bevindingen

Vanuit het overzicht van initiatieven en operators ontstaat niet direct een kristalhelder beeld. We zien een grote diversiteit aan operators, in verschillende stadia van volwassenheid. De rol van afsprakenstelsels is nog beperkt, maar lijkt groeiend. Ook de programma’s in het speelveld die we hebben besproken zijn divers en maar beperkt samenhangend. Voor betrokkenen is het moeilijk overzicht te krijgen en samenwerking te realiseren.

- Een aantal operators is de pilotfase al ontstegen, al is de schaal waarop ze worden gebruikt nog beperkt. Alle operators in het landschap staan nu nog los van elkaar; interoperabiliteit is nog geen aandachtspunt bij de operators. In de rest van Europa is de situatie niet veel anders: we zien een aantal opkomende operators met meerdere pilots.
- Een belangrijk onderscheid tussen oplossingen zit in de benadering van data: daarbij kan de operator alleen data doorgeven, data opslaan/aggregeren, afgeleide informatie afgeven of zelfs ondertekenen. Een voordeel van alleen doorgeven (en dus niet opslaan) is dat de operator geen verwerker is van de data. Dit is een vorm van privacy-by-design en data minimalisatie. Aan de andere kant, als data wordt opgeslagen en via de operator wordt gedeeld, beperkt de ontkoppeling van leverancier en afnemer ook de hoeveelheid informatie die nieuw in de transactie ontstaat.
- Net zoals persoonlijke data kan worden opgeslagen in de operator, kopiëren (cachen) sommige operators ook de identiteit. Deze kunnen daarmee als inlogmiddel gaan functioneren.
- De scheidslijn tussen authenticatiestelsel en een PDM-oplossing met operatorrol is een dunne: een authenticatiestelsel kun je zien een specifieke implementatie van een PDM-stelsel met de focus op geverifieerde identiteitsgegevens en niet zozeer informatie die aan mijn identiteit gekoppeld is (zoals een diploma of een medisch dossier).
- Een laatste onderscheidend element is het toepassingsgebied. We zien zowel smalle operators als generieke operators ontstaan. Veel van de early movers waren generiek. De laatste jaren komen daar specifiekere operators bij, gericht op het overheidsdomein, de zorg of financiële sector. Tegelijk komen er ook nog steeds generieke initiatieven bij. De diversiteit groeit.

In het algemeen zijn gebruikscijfers nog maar heel beperkt beschikbaar en is gebruik dus moeilijk te duiden. We kunnen wel zeggen dat er nog geen heldere ‘winnaar’ is en ontwikkeling van PDM nog steeds evolutionair verloopt.

De dimensies generiek/specifiek en opslag lijken samen een aardige omspanning te geven van het veld, met een verdeling over alle vlakken. De meeste operators slaan persoonlijke data zelf op, zowel bij generieke als specifieke oplossingen.

Vervolgstappen

Het is belangrijk het overzicht dat nu begint te ontstaan actueel te houden. Zo blijven we in staat de markt te duiden en goede beslissingen over de inzet van PDM voor data-afnemers en data-leveranciers te nemen. Dit overzicht zal worden gepubliceerd op www.digitalwe.nl en daar ook worden bijgehouden. De vervolgstappen zijn onder meer:

1. Internationale consensusvorming op principes voor PDM: op basis van dit onderzoek wordt in MyData verder gewerkt aan een beschrijving van de MyData operator. Daarbij gaat het niet alleen om een functioneel kader, maar ook om een normatief kader: wanneer voldoet een operator aan de MyData principes?
2. Nationale harmonisatie: we zoeken aansluiting bij initiatieven als het programma Regie op Gegevens om tot een geharmoniseerde terminologie te komen en zo begripsverwarring in het veld zo veel mogelijk te voorkomen.
3. Aanvulling met initiatieven die gerelateerd zijn aan de invulling van PSD2. Dit is nu nog bewust achterwege gelaten. Er komen echter de nodige initiatieven rond open banking die ook in Nederland hun impact hebben.

Ook op technologisch vlak is er een aantal zaken om rekening mee te houden. Onder meer de ontwikkeling van Self Sovereign Identities is eentje die veel aandacht krijgt, met name in de blockchainhoek. Feitelijk kan dit worden gezien als een nieuwe generatie identiteitstechnologieën die een aantal manco’s van user centric identiteiten en gefedereerde identiteiten wegneemt.

Tenslotte is het belangrijk juist naar het speelveld te kijken: dynamiek daar wordt deels bepaald door de markt, deels door technologie en deels door de politiek. Juist het politieke aspect is een moeilijk te voorspellen dimensie. Volgen, voorlichten en informeren is daar minimaal noodzakelijk.

Dit werk is gedaan in het kader het project Digital We. In Digital We gaan we op zoek naar de betekenis van de digital enterprise voor organisaties. Het is een co-innovatieproject gefaciliteerd door InnoValor. Het consortium bestaat uit APG, De Volksbank, de i4Sociaal gemeenten en Dimpact, RVO, Kadaster, DUO en InnoValor.

Rechten op dit materiaal zijn voorbehouden aan de Digital We deelnemers.

1 Persoonlijk data management in context

Naarmate het belang van persoonlijke gegevens in de samenleving groei, wordt het steeds urgenter om ervoor te zorgen dat individuen in staat zijn toegang krijgen tot hun persoonlijke gegevens, deze kunnen hergebruiken en benutten. Dit is heel anders dan in de begindagen van het Internet, waar Internet pioniers jouw data voor je beheerden, inclusief een identiteit, in ruil voor jouw data. Een dergelijke bundeling van services remt echter de concurrentie, vermindert de kracht van de markt en remt innovatie op het vlak van verantwoord gebruik van persoonlijke data. Een dergelijk platformmodel zonder de mogelijkheid om verschillende diensten, service providers te kiezen is er geen betekenisvolle instemming voor gebruik en heeft het individu geen macht om de markt te beïnvloeden.

Dit is waar persoonlijk data management oplossingen (Personal information management services, of Personal Data Store) hun rol hebben: de PDM oplossing speelt de rol van een intermediair tussen gegevensbronnen en gegevens die diensten gebruiken binnen een afsprakenstelsel of ecosysteem, waarbij het individu vertrouwen stelt in de PDM oplossing. Het moet vertrouwen creëren en een data-gedreven markt faciliteren waar individuen zowel worden beschermd als gemachtigd om de gegevens te gebruiken die organisaties over hen bewaren.

Figuur 1. Internetpioniers als centrale spil in data [bron:MyData Master Presentation]

De thematiek is niet nieuw. Persoonlijk data management heeft al een lange historie in Nederland en daarbuiten. Project VRM startte in 2006,[1] de basis voor MijnOverheid werd meer dan 12 jaar geleden gelegd, Qiy is gestart in 2007, hetzelfde jaar dat Mydex in het Verenigd Koninkrijk werd opgericht. Sinds die tijd is er veel gebeurd, maar een echte doorbraak is uitgebleven. MijnOverheid is ver weg gebleven van de oorspronkelijke ambities, met Qiy hebben enkele pilots gelopen, maar opschaling ontbreekt. Wat wel werkt tot nu toe zijn smalle toepassingen als het pensioenoverzicht, maar PDM-diensten in de breedte missen nog. Tegelijk zien we de laatste paar jaar een explosie aan initiatieven, met name vanuit verschillende toepassingen. Op het generieke vlak timmert IRMA flink aan de weg.

Zo snel als initiatieven ontstaan, zo snel verdwijnen sommigen ook weer. De poliskluis van de verzekeraars (MijnVerzekeringenOpEenRij.nl) werd in mei van dit jaar alweer opgeheven. Only Once, via crowdsourcing gestart en gelanceerd in 2015, lijkt gestopt. OpenPDS van MIT in de VS kende een mooie start, maar is stilgevallen. CV monitor is verdwenen, tevens is Tippiq stilgelegd en MyDex in UK heeft nog steeds niet de weg naar brede adoptie.

Verschillende programma's werken aan de thematiek van persoonlijk data management. Bij de overheid loopt al enige jaren het programma Regie op Gegevens (RoG), van waaruit dit jaar onder meer een beleidsbrief richting de Tweede Kamer is gestuurd,[2] gewerkt wordt aan een kader van RoG en een kosten-batenanalyse is uitgevoerd. Ook worden proofs-of-concept gefaciliteerd. Samenwerkingsverbanden als de Dutch Blockchain Coalition en Techruption experimenteren aan de randen van het thema,[3] en EduMij zoekt in navolging van MedMij wat er in de educatieve sector zou kunnen gebeuren. De verzekeringsbranche kijkt nadrukkelijk ook

[1] https://cyber.harvard.edu/projectvrm/Main_Page
[2] Kamerbrief Visie Regie op Gegevens, 11 juli 2019. Beschikbaar via https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/11/kamerbrief-visie-regie-op-gegevens
[3] Zie https://www.brightlands.com/companies-institutes/smart-service-campus/techruption

naar deze ontwikkeling en in de financiële sector heeft de PSD2 richtlijn tot veel dynamiek gezorgd, meer nog buiten Nederland dan erbinnen.

Ook in Digital We is het thema al meerdere keren onderwerp van onderzoek geweest. In 2015 hebben we uitgebreid het concept en het potentieel van PDM onderzocht en hebben we een grootschalig onderzoek onder Nederlandse consumenten uitgevoerd naar de gebruikersbeleving van data delen. Dat leverde interessante inzichten op rond het adoptiepotentieel.[4]

Internationaal zien we met name de non-profit organisatie MyData Global als veelbelovende kracht in het veld. Na een aantal congressen over MyData en het opstellen van een manifest (de MyData Declaration) is in 2018, ondersteund vanuit Digital We, een wereldwijde organisatie opgezet om verantwoord benutten van persoonlijke gegevens te bevorderen. In termen van MyData: *make it happen and make it right.*

In deze kakafonie aan oplossingen, samenwerkingsverbanden, technologieën en standaarden kun je makkelijk verdwalen, zelfs als kenner, laat staan als geïnteresseerde leek. Deze deliverable moet helpen je weg weer te vinden in dit landschap, door zaken te ordenen en te duiden, zonder te oordelen.

1.1 DOEL EN DOELGROEP

Dit rapport richt zich primair op mensen die al actief zijn op het vlak van persoonlijk data management en een beter beeld willen krijgen van de status van de markt en het concept, zowel in Nederland als daarbuiten. In het rapport brengen we structuur in het landschap van oplossingen, concepten, technologieën en initiatieven. Om de vergelijking te objectiveren maken we gebruik van een referentiemodel van alle functionaliteiten die we tegenkomen in het ecosysteem, inclusief governance.

Voor een algemenere inleiding op het vraagstuk zie, bijvoorbeeld, *Eigen Data delen*,[5] het eerdere rapport van Digital We, of bezoek de website van Mydata (www.mydata.org) inclusief een video van Antti Poikola van MyData over het thema (https://mydata.org/mydata-101/).

1.2 ONDERZOEKSAANPAK

Dit onderzoek heeft gelopen van april 2019 tot december 2019. In april zijn we gestart met het opzetten van het referentiemodel aan de hand van literatuuronderzoek en een analyse van een aantal bestaande oplossingen. Dit model is vastgelegd in *A personal data commons* (april 2019)[6] Dit referentiemodel is internationaal gevalideerd in een expertgroep van MyData, hetgeen leidde tot een discussiepaper op de MyData 2019 conferentie.[7] Het programma Regie op Gegevens werkt aan een Kader van Regie Op Gegevens.[8] Eerste versie van het kader zijn in het opstellen van het referentiemodel meegenomen en uitkomsten van het Digital We onderzoek worden actief gedeeld met het programma.

Het referentiemodel is geoperationaliseerd in een vragenlijst voor PDM-oplossingen en afsprakenstelsels. Deze vragenlijst is uitgezet in Nederland en in beperkte mate daarbuiten bij ons bekende afsprakenstelsel en oplossingen. In totaal zijn er 29 vragenlijsten verzonden, waarvan er 15 ingevuld retour zijn gekomen. Slechts één initiatief heeft aangegeven niet mee te willen werken, vanwege beëindiging van het initiatief.

De analyse is tenslotte weer aan de indieners voorgelegd ter controle. In het maken van de longlist is onder meer samengewerkt met SURF en DUO (in het kader van EduMij) en met SIVI (www.sivi.org). Bij de selectie van de oplossingen hebben we niet gekeken naar het volledige spectrum aan persoonlijke gezondheidsomgevingen

[4] Nederlanders over persoonlijke data. InnoValor 2015. Beschikbaarbaar via https://drive.google.com/open?id=0BwOp97FBbJEjUDFFVWE5cE1ZN3c
[5] Janssen, W. (red.) Eigen Data Delen. Digital We deliverable PDS/1, versie 1.3, november 2015. Beschikbaar via https://drive.google.com/file/d/0BwOp97FBbJEjWmpDWnF3UE1naWc
[6] A personal data commons, Digital We 2019 D7. Beschikbaar via https://drive.google.com/file/d/1NdO_GxhErMkGpZsS2EN5f9JGo-hL6Uu3/view?usp=sharing
[7] Poikola, Langford, Huhtamäki, Sierla & Janssen. What is the MyData Operator. September 2019. Beschikbaar via https://mydata.org/wp-content/uploads/sites/5/2019/09/Discussion-paper-MyData-operator-final.pdf
[8] https://rog.pleio.nl/groups/view/34174102/kennisbank-regie-op-gegevens/files/57899630

(PGOs) omdat deze te domein-specifiek zijn voor dit overzicht. Ivido dient hiervan als voorbeeld. Het blijft een interessant domein, met name vanwege de dynamiek die hier nu is door de introductie van het afsprakenstelsel MedMij en de bijbehorende financieringsarrangementen vanuit het ministerie van VWS. MedMij is ook opgenomen in de rapportage. Vergelijkbare dynamiek geldt door PSD2 rond uitwisseling van gegevens over financiële transacties. In dit domein is nog niet heel duidelijk welke oplossingen hier in de nabije toekomst komen bovendrijven. Dit is een aandachtspunt voor 2020.

Het streven is de lijst met geanalyseerde oplossingen regelmatig te actualiseren en te publiceren op www.innovalor.nl. In maart 2020 zal er nog een internationale MyData workshop plaatsvinden in Amsterdam om het landschap van oplossingen ook internationaal verder uit te breiden en te analyseren.

2 Wat is PDM?

2.1 DEFINITIE VAN PDM

Persoonlijke data en digitale identiteiten zijn het digitale DNA van mensen. Het is waardevol en onlosmakelijk verbonden met het individu. Persoonlijke data kan een basis zijn voor nieuwe, gepersonaliseerde diensten en bedrijfsmodellen die ervoor zorgen dat je zelf je data kan inzetten voor betere, snellere dienstverlening, zoals het verkrijgen van een hypotheek of bij het voorkomen of oplossen van een schuldenpositie. De persoon zou dan ook zelf de controle moeten hebben of deze gegevens en niet publieke of private partijen. In deze rapportage gebruiken we de term persoonlijk data management, ofwel PDM, om te duiden dat mensen (persoonlijke) gegevens kunnen gebruiken om hun leven, werk of bedrijf te organiseren, terwijl belangrijke waarden als veiligheid en privacy geborgd zijn[9]. Persoonlijk data management gaat over toegang, corrigeren en delen van persoonlijke data, maar ook inzicht hebben in wie deze persoonlijke gegevens gebruikt, onder controle van het individu.

In de basis gaat persoonlijk data management over het individu, de inwoner, de zorggebruiker of de klant. Eerder onderzoek van InnoValor[10] toonde aan dat mensen controle willen over persoonlijke data en wie deze gegevens in kan zien en gebruiken. Mensen willen oplossingen waar ze vertrouwen in hebben en die passen bij de situatie: makkelijker samenwerken met de overheid voor een vergunning, om een hypotheek op maat af te sluiten, of voor een beter persoonlijk financieel overzicht.

Om controle over persoonlijke data mogelijk te maken, zijn nieuwe manieren nodig om gebruik te maken van de rechten die ons gegeven zijn, door zowel technologische oplossingen als nieuwe innovatieve diensten. Dit is waar persoonlijk data management en de ontwikkeling van persoonlijke data management oplossingen zich op richten. Zoals MyData[11] deze ontwikkeling stelt: *“Today, the balance of power is massively tilted towards organisations, who alone have the power to collect, trade and make decisions based on personal data, whereas individuals can only hope, if they work hard, to gain some control over what happens with their data. (..) [We] aim at restoring balance and moving towards a human-centric vision of personal data.”*

Er is nog nooit zoveel aandacht en momentum geweest voor persoonlijk data management. Recente schandalen zoals Cambridge Analytica dragen bij aan het publieke bewustzijn. Daarnaast is er striktere privacywetgeving ingericht in Europa (GDPR) die eisen stelt als data portabiliteit, rechten voor de gebruiker en transparantie. Daarnaast is er toegenomen concurrentie in de financiële sector dankzij het Payment Service Directive (PSD2). Dit doet vermoeden dat een doorbraak voor persoonlijk data management niet ver weg is.

Dit constructieve momentum laat zich zien in de hoeveelheid programma’s rond persoonlijk data management. De overheid zet grootschalige projecten op voor PDM[12], verzekeraars werken aan het halen van waarde uit data. Gemeenten onderzoeken hoe ze persoonlijke data kunnen inzetten om dienstverlening in het sociale domein te verbeteren. We zien oplossingen veelal ontstaan vanuit nichés binnen sectoren. Deze oplossingen richten zich op specifieke vragen van inwoners en consumenten. Andere oplossingen werken vanuit een algemeen gevoel van urgentie omtrent persoonlijke data, en proberen in een generieke, maar latente behoefte te voorzien om meer controle over persoonlijke gegevens hebben. De meeste oplossingen hebben nog een beperkt succes.

We zien veel initiatieven die controle over persoonlijke gegevens bieden. Echter, er is grote variatie in de volwassenheid en interoperabiliteit en een beperkte reikwijdte. Er is weinig samenhang en geen gedeelde visie voor persoonlijk data management oplossingen. Het risico bestaat daarmee dat deze initiatieven vastlopen, gebruikers verliezen en de adoptie van PDM beperkt blijft. Dit zorgt voor gemiste kansen voor nieuwe bedrijvigheid en betere diensten, en voor hogere kosten voor zowel personen als organisaties[13].

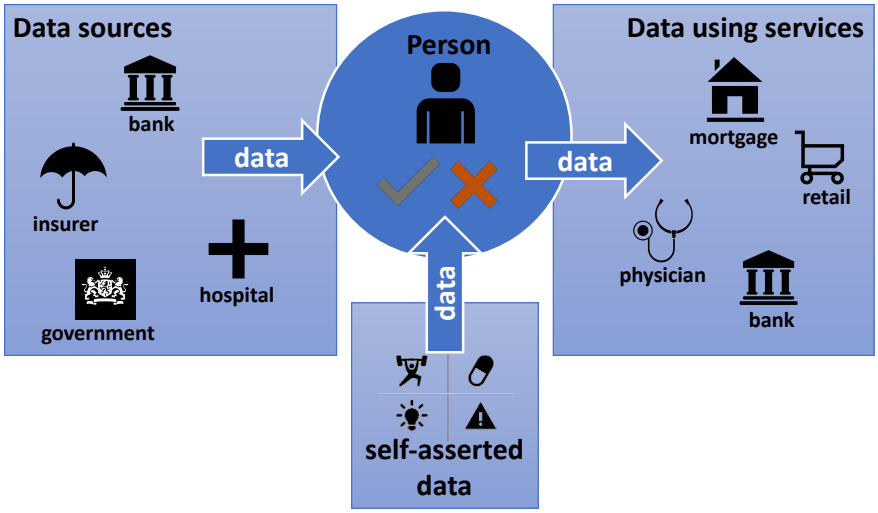
---

[9] Kader voor Regie op Gegevens
[10] Data om te delen. InnoValor, 2015 (in Dutch). Beschikbaar via www.innovalor.nl
[11] MyData Declaration. Available at www.mydata.org
[12] Programma Regie op Gegevens in Nederland, IHAN-programma van Sitra
[13] Unlocking the Value of Personal Data, World Economic Forum, February 2013.

Onze hypothese is dat, door structureel kennis en ervaring te delen, de ontwikkelsnelheid en kwaliteit van PDM-oplossingen zal verbeteren. We willen het begrip en de adoptie van persoonlijk data management vergroten, door een referentiemodel te ontwikkelen voor PDM: een open, gedeeld, begrip van persoonlijk data management en diensten de persoonlijke data gebruiken.

2.2 HET CONCEPT PERSOONLIJK DATA MANAGEMENT

Een persoonlijk data management oplossing kan faciliteren in het delen van data tussen data aanbieders en data afnemers. Een PDM-oplossing is een dienst die een individu in staat stelt om zijn persoonlijke informatie duurzaam te beheren en te onderhouden om deze, wanneer de gebruiker dit in zijn belang acht, te kunnen delen met anderen.[14] Dit betekent niet dat de gegevens in de PDM-oplossing opgeslagen zijn, het kan simpelweg een mechanisme bieden om persoonlijke data te managen, ook al staat de data bij de autoratieve bron. Dit is afhankelijk van de oplossing. Onderstaande figuur toont de basisprincipes van een PDM-oplossing.



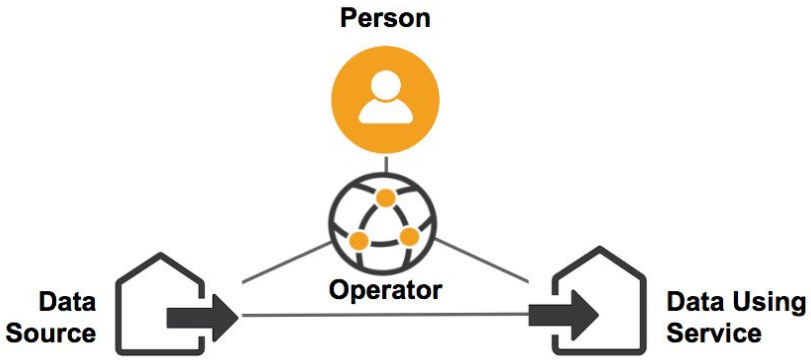
Figuur 2. Basisprincipes van persoonlijk data management.

Het concept persoonlijk data management is best een ingewikkeld concept, zowel voor het individu als de organisaties die data aanbieder of data afnemer zijn. Die complexiteit komt terug in de technologie en in het zoeken naar duurzame bedrijfsmodellen van persoonlijk data management oplossingen. Het is nog niet helder hoe een gezonde markt kan ontstaan voor oplossing waar concurrentie mogelijk is en de gebruiker een zekere keuzevrijheid heeft. Wie betaalt voor de datauitwisseling die plaatsvinden in het netwerk? Sommige oplossingen opereren volledig in het private domein, andere doen een poging om een brug te slaan tussen publieke en private datauitwisseling, weer andere richten zich volledig op het publieke domein. Allen stellen verschillende eisen aan de data die uitgewisseld wordt en aan het verdien- en tariefmodel.

2.3 ROLLEN IN EEN PERSONAL DATA ECO-SYSTEEM

De basis van PDM omvat de vier: de persoon, de operator die controle over persoonlijke data biedt aan de persoon (ook wel PDM service provider genoemd), data aanbieders (ook wel bronnen of leveranciers genoemd) en data afnemers (ook wel relying parties genoemd).

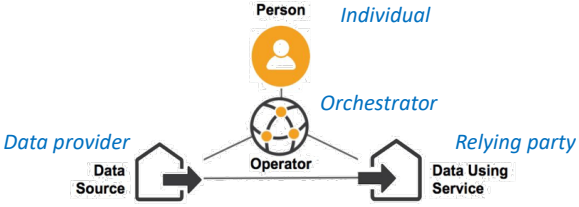
[14] Data om te Delen. InnoValor, 2015 (in Dutch). Beschikbaar via www.innovalor.nl



Figuur 3. Rollen in PDM (bron: MyData declaration, www.mydata.org).

De persoon is een individu die zeggenschap heeft over het delen van zijn over haar data, voor eigen doeleinden, en heeft een relatie met de andere drie rollen. Een data aanbieder verzamelt en verwerkt persoonlijke data die de andere rollen (inclusief de persoon) willen inzien of gebruiken. Een data afnemer kan geautoriseerd worden om persoonlijke data van een of meerdere aanbieders te gebruiken. Een operator maakt het mogelijk voor het individu om veilig persoonlijke data in te zien, gebruiken en te managen. Daarnaast maakt de operator het mogelijk om de uitwisseling van persoonlijke data met en tussen data aanbieders en afnemers te controleren. Individuen vervullen ook de rol van operator wanneer zij eigen data managen. In andere gevallen gebruiken operators de data niet zelf, maar voorzien in de connectiviteit en beveiliging die nodig zijn voor gegevensuitwisseling tussen de andere rollen in het ecosysteem; ze voorzien in persoonlijk data management services. De diversiteit aan operators en de functionaliteiten die zij vervullen, komt terug in hoofdstuk 4 en 5.

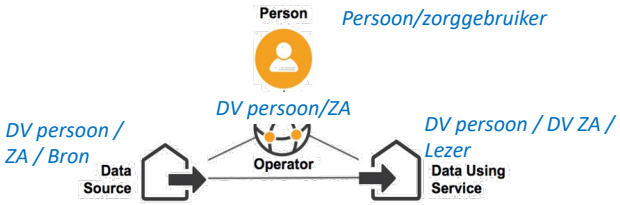
PDM Rollen - *Qiy*



Vergelijkbare rollen komen we in de meeste contexten tegen. Qiy spreekt in dit kader over de Data Provider, de Relying Party (als afnemer), de Individual en de Orchestrator. Regie op Gegevens spreekt over Bronhouder of Aanbieder, over Afnemer of Dienstverlener en over de Betrokkene.

In het afsprakenstelsel MedMij is een andere keuze gemaakt: daar zijn de rollen niet aan de “richting” van de data gekoppeld, maar aan de rol van in het zorg eco-systeem. MedMij spreekt over de Persoon en de Zorgaanbieder die elk een dienstverlener kennen, de Dienstverlener Persoon en de Dienstverlener Zorgaanbieder. Beide rollen kunnen zullen een data-aanbieder als -afnemer zijn en zelfs de rol van operator hebben: een Persoonlijke Gezondheidsomgeving (of PGO) vervult de rol van Operator en vervult bij MedMij onder de Dienstverlener Persoon rol.

PDM Rollen - *MedMij*



De internationale standaard van OASIS Classification of Everyday Living (COEL)[15] kent vergelijkbare rollen, waarbij ook de Operator dicht bij de persoon staat (Consumer), en de Service Provider de rol van data-afnemer vervult. COEL onderscheidt wel strikt de Data Engine (die data ontvangt, opslaat en verwerkt) van de Operator rol. Deze twee verantwoordelijkheden lopen in veel oplossingen door elkaar.

[15] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=coel#technical

3 Referentiemodel voor PDM

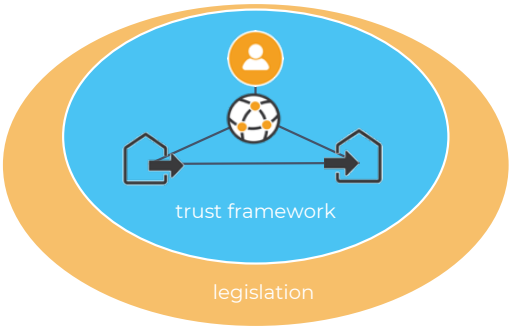
3.1 BOUWBLOKKEN EN AFSPRAKENSTELSELS

Operators zijn er in vele vormen en onder verschillende namen: persoonlijke data services, persoonlijk informatie management services (PIMS). Soms managen ze persoonlijke data, als een soort kluis, in andere gevallen faciliteren ze met name datauitwisseling.

Figuur 4. Voorbeelden van operators in de wereld.

Deze diversiteit is een logisch gevolg van de eerste stap in de evolutie van het persoonlijke data ecosysteem, maar het beperkt ook de adoptie en groei. De ontwikkeling van dit soort oplossingen begon al een decennia geleden; MyDex stamt uit 2007, net als het afsprakenstelsel Qiy. Er is sindsdien veel gebeurd, maar grootschalige adoptie heeft zich nog niet voorgedaan.

De operator moet zorgen voor vertrouwen en een gebruikersgedreven markt. Hij bestaat in een ecosysteem van data aanbieders en data afnemers, van publieke als private organisaties. Een ecosysteem als dit kan alleen floreren als er enige vorm van regulering, wetgeving of sociale normen bestaan.

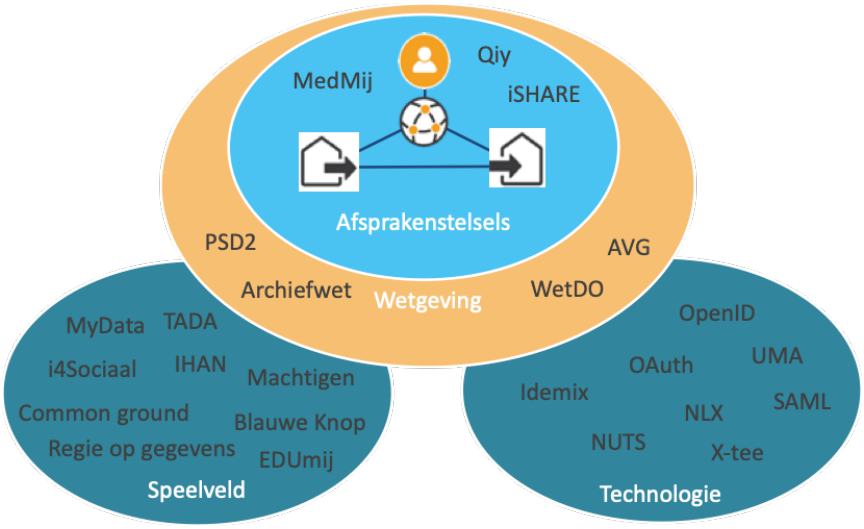


Figuur 5. Ecosysteem bouwt op afsprakenstelsels, die zich baseren op wetgeving.

In Europa is de GDPR wetgeving (AVG in het Nederlands) een stevige basis voor het mogelijk maken van datauitwisseling en het beschermen van privacy. In Japan zijn ‘data banken’ (commerciële bedrijven als operator) in nieuwe certificering verankerd. Dit soort wetgeving en regulering is nodig voor het creëren van vertrouwen, maar is vaak niet voldoende. Om een gelijk speelveld te verkrijgen in de marktzijn er spelregels

nodig tussen de verschillende rollen en actoren. Dit wordt vaak vastgesteld in de vorm van een afsprakenstelsel. Afsprakenstelsels zijn de onderliggende afspraken en regels die een volwassen ecosysteem mogelijk maken.[16] Ze beschrijven een contractueel bindende set van specificaties, afspraken en minimale technische specificaties die het ecosysteem beheren. Bekende voorbeelden buiten persoonlijk data management zijn creditcard systemen (zoals Visa), domein naam registratie systemen (beheerd door ICANN), of telecommunicatie raamwerken zoals GSM (beheerd door GSMA). In deze context zijn MedMij (Nederland), Findy (Finland) en HAT (UK) opkomende voorbeelden van gevalideerde afsprakenstelsels.

In Nederland worden er afsprakenstelsels ontwikkeld in verschillende sectoren die proberen deze set aan spelregel neer ze zetten. MedMij is een voorbeeld van een afsprakenstelsel dat ontwikkeld wordt in de medische sector. Het richt zich op afspraken over de uitwisseling van medische gegevens, een van de meest gevoelige soorten data. Het afsprakenstelsel bevat een overzicht van de basisprincipes die MedMij gebruikt, een referentie architectuur en details over de governance en informatiemodellen die gebruikt moeten worden bij het uitwisselen van data. Binnen dit afsprakenstelsel wordt gerefereerd naar andere standaarden zoals OAuth, OpenID connect en SAML. Op dit moment kunnen PDM-oplossingen een indiening doen bij MedMij om gecertificeerd dienstverlener te worden en financiering te ontvangen.



Figuur 6. Overzicht Speelveld, wetten en technologie voor PDM.

Niet alle PDM-oplossingen conformeren zich aan afsprakenstelsels. In tegendeel: veel van de huidige oplossingen zijn op zichzelf staand ontwikkeld en richten zich op een specifieke oplossing voor een specifieke doelgroep, en maken daarbij gebruik van zelf gekozen technologische standaarden. Daar is niks mis mee. Afsprakenstelsels kunnen helpen bij het maken van vertrouwde oplossingen, omdat ze dienen als manier om te certificeren. PDM-oplossingen zijn sterk afhankelijk van vertrouwen, iets waar certificering in kan voorzien. Vertrouwen is daarnaast makkelijker te creëren voor sectorspecifieke afsprakenstelsels, waar toepassingen makkelijker te begrijpen zijn voor gebruikers. Uiteindelijk is het verbeteren van interoperabiliteit ook een belangrijk kenmerk om te overwegen.

3.2 COMPONENTEN EN DEFINITIES

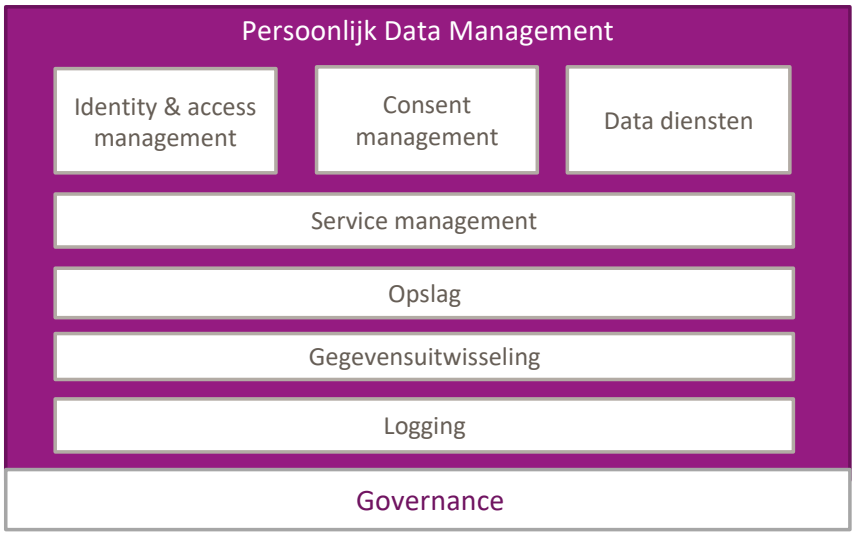
In dit complexe landschap is een basis nodig, een gedeeld begrip van de functionaliteiten die operators bieden. Dit moet helpen om van een gefragmenteerd landschap van oplossingen naar een duurzaam ecosysteem te bewegen. Om dit te kunnen doen is een referentiemodel een belangrijke stap. Het onderstaande figuur laat een samenvatting zien hoe de basiscomponenten aan elkaar relateren. De bouwblokken in het model zijn afgeleid van bestaande oplossingen en afsprakenstelsels, zoals MyData, MedMij, Qiy, digi.me en MyDex. De operator maakt het mogelijk voor een persoon om te bepalen welke data de data afnemers mogen ontvangen. Functionaliteit kan verdeeld zijn of zelfs overlappen tussen de verschillende rollen in het ecosysteem: niet alles

[16] Trust frameworks for identity systems. Esther Makaay, Tom Smedinghoff & Don Thibeau. OIX white paper, June 2017

ligt bij de operator en sommige functies liggen bij alle rollen (zoals logging). Voor afsprakenstelsels geldt in de regel: ze stellen eisen aan de invulling van de functionaliteiten (opslag van data zal een afsprakenstelsel niet aanbieden, maar ze zal er wel eisen aan stellen).

Belangrijke functionele componenten zijn (Figuur):

- Consent management – Het managen van (tijdelijke) toestemming voor het delen van data tussen data aanbieders en afnemers.
- Datadiensten – een PDM service kan zelf waarde toevoegen door ondertekening, analyseren, filteren en vertalen van de data. Kan ook gaan om het in rekening brengen van kosten voor het gebruik van data.
- Identity & access management - Functionaliteit ten behoeve van authenticatie en autorisatie van de persoon en de data afnemer.
- Service management - Maakt het koppelen van data afnemers en data aanbieders mogelijk. Data kan op meerdere plekken beschikbaar zijn en gebruikt worden door diverse afnemers. Biedt een overzicht van data aanbieders en afnemers die aangesloten zijn op de PDM-service.
- Gegevensuitwisseling – Interface die data uitwisseling mogelijk maakt op een veilige en gestandaardiseerde manier, tussen de persoon, afnemer, aanbieder en operator.[17] Dit kan middels gestructureerde data, ondersteunende automatische transactie of ongestructureerde data (zoals een pdf). Informatie kan zowel brondata zijn als afgeleide attributen. Het kan end-to-end encryptie bevatten tussen de data aanbieder en afnemer of verwerkt worden door de operator.
- Logging - Het bijhouden van gegevensuitwisseling die heeft plaatsgevonden, waardoor het zichtbaar is wie wanneer tot wat toegang had.
- Opslag – De dienst kan zelf zorgen voor opslag van data ten behoeve van (her-)gebruik. Denk aan de opslag van medische gegevens of het bewaren van gewaarmerkte data. Let op: veel diensten slaan ten behoeve van de gegevensuitwisseling data kortstondig op. Dat valt hier niet onder opslag, maar kan wel leiden tot een rol als verwerker onder de AVG.
- Governance – het besturen van het gebruik en de ontwikkeling van de onderliggende principes van het ecosysteem, inclusief management van het business model.



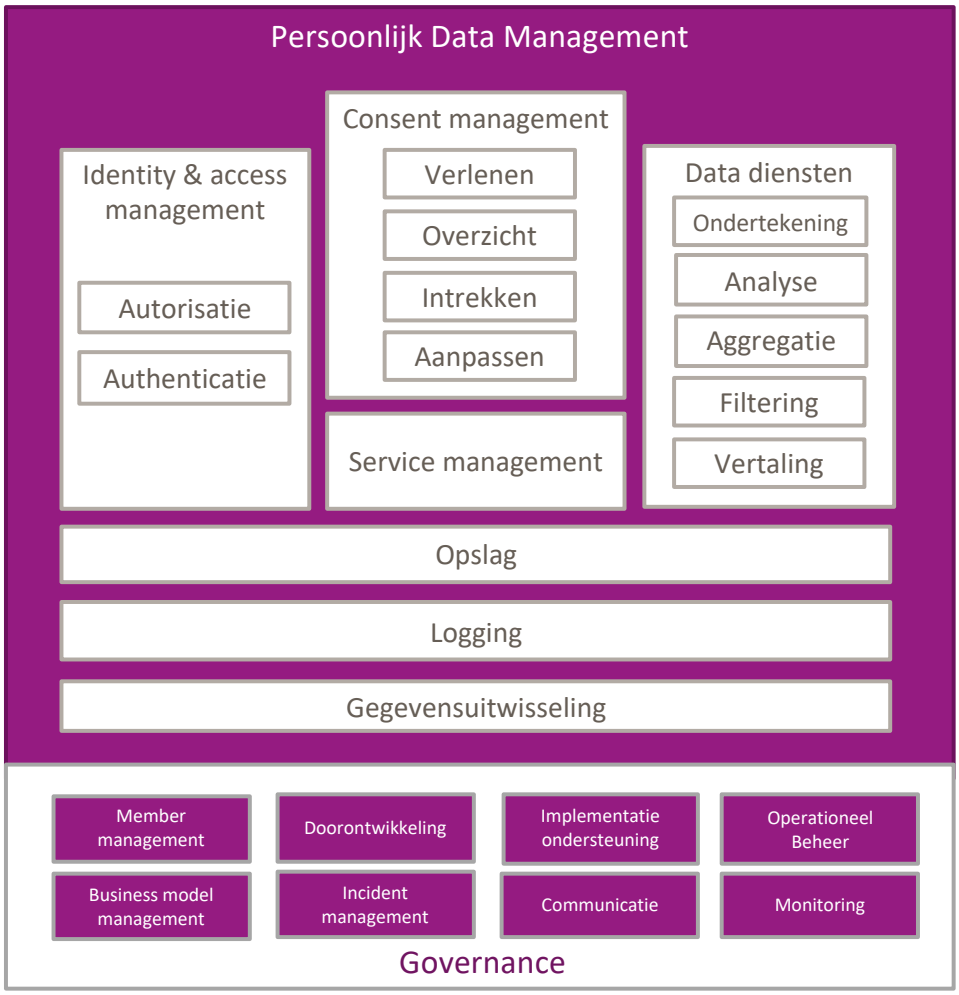
Figuur 7. Onderdelen referentiemodel voor PDM.

Meerdere data afnemers en meerdere data aanbieders zullen deelnemen in het ecosysteem. Het is onwaarschijnlijk en ongewenst dat er een enkele operator, of zelfs een enkel afsprakenstelsel zal overblijven. Gebruikers moeten kunnen kiezen welke persoonlijk data management oplossing bij hen past en welke

[17] Naast gegevensuitwisseling zou ook uitwisseling van waarde/geld meegenomen kunnen worden. In de geanalyseerde set van oplossingen is dit echter niet aan de orde. Amerikaanse oplossingen als Datacoup kennen dit echter wel.

uitdagingen zij willen aanpakken. Data kunnen bij verschillende, mogelijk overlappende, bronnen liggen, worden bemiddeld door verschillende oplossingen en gebruikt door verschillende diensten. Het is zonder twijfel een meerzijdige markt. Verschillende gegevens kunnen dan ook bij meerdere bronnen liggen. Service management speelt binnen de PDM diensten, maar ook in de governance: welke bron is de juiste bron voor welke data? Welk inkomensgegeven zetten we in, welk adres hebben we nodig? Deze situatie zorgt voor druk op interoperabiliteit en kan een barrière zijn voor adoptie. Standaardisatie is dus noodzakelijk op de technische interfaces van de bouwblokken, en mogelijk op concepten in de gebruikersinterface. Afsprakenstelsels als MedMij specificeren technische interfaces, maar geven geen richtlijnen voor gebruikers interactie.

We zien verschillen tussen de methoden die gebruikt worden voor gegevensuitwisseling. Aan de ene kan de operator zorgen voor gegevensuitwisseling, waarbij hij zelf mogelijk data (tijdelijk) opslaat. In andere oplossingen kan de data afnemer zelf data direct opvragen bij de data aanbieder. De operator-rol beperkt zich dan tot logging en consent management, zonder zelf daadwerkelijk de data te zien of op te slaan.



Figuur 8. Het volledige referentiemodel, inclusief governance.

Governance

De governance, het besturen en beheren van PDM-oplossingen met alle partijen in het ecosysteem, is net zo essentieel als de oplossingen zelf en worden typisch door het afsprakenstelsel zelf gedaan. Dit kan gaan om:

- Member management - Aan- en afsluiten van data afnemers, aanbieders en operators op de services of het afsprakenstelsel. Dit kan noodzakelijk zijn als er specifieke regels zijn waaraan voldaan moet worden (denk aan ISO27001). Partijen die niet voldoen moeten afgesloten worden.
- Doorontwikkeling – Ondersteunen van de doorontwikkeling van services en afsprakenstelsels om nieuwe functionaliteiten te realiseren.

- Incident management – Acteren op incidenten of data lekker om reputatie schade aan de services en het afsprakenstelsel te voorkomen en gevolgen te minimaliseren.
- Business model management – Faciliteren van waardestromen in het ecosysteem en het creëren van middelen om services en afsprakenstelsels te realiseren.
- Communication & klachten management – Interactie met gebruikers van services en afsprakenstelsels, buiten de context van services. Oplossen van klachten en issues.

Als voorbeeld, MedMij implementeert al deze componenten en creëert daarmee een vertrouwde context voor MedMij gebaseerde oplossingen.[18] Binnen MedMij specificeren het stelsel en de afspraken hoe de bovenstaande functionaliteiten geïmplementeerd onderhouden worden.[19] Het Qiy scheme gebruikt een gelaagd model, met een zogenaamde global scheme authority die verantwoordelijk is voor de ontwikkeling, en regionale autoriteiten die verantwoordelijk zijn voor member management.[20]

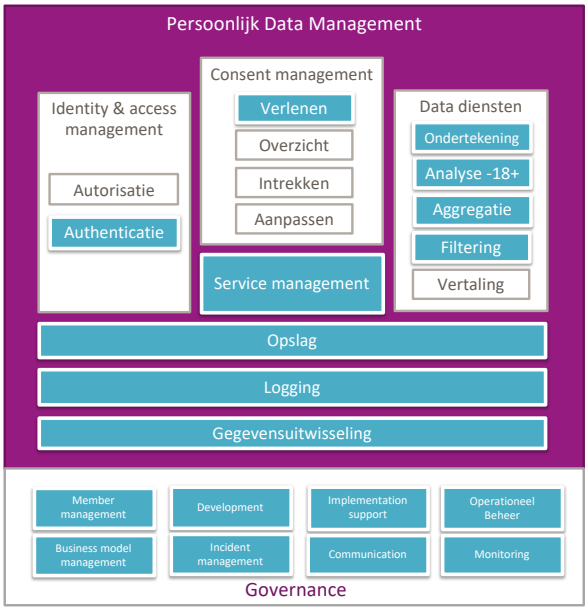
3.3 VOORBEELD: IRMA

Een concreet voorbeeld kan verhelderen hoe we het referentiemodel kunnen inzetten. IRMA[21] staat voor "I Reveal My Attributes" en is een mobiele applicatie die is gericht op het delen van attributen en het ondertekenen in een digitale wereld. IRMA wordt beheerd door de Stichting Privacy by Design. Alleen de attributen die een relying party nodig heeft worden gedeeld, zonder andere informatie te verstrekken. Zo kan een gebruiker bijvoorbeeld bewijzen dat hij ouders is dan 18, zonder zijn geboortedatum prijs te geven. Typische data aanbieders voor IRMA-attributen zijn: BRP (basisregistratie personen), SURF, BIG, AGB (Algemeen GegevensBeheer) en KvK.

Autorisatie en authenticatie doet IRMA met de middelen die passen bij het verkrijgen van het attribuut bij de leverancier: voor de BRP en DUO is dat dan DigiD, bijvoorbeeld. Voor bankgegevens de iDIN-login.

IRMA slaat de attributen veilig op in de applicatie en kan bij de uitwisseling van de attributen zelf ook afgeleide attributen ondertekenen. Zo kan IRMA de eigenschap 18+ afleiden uit de iDIN geboortedatum, en geeft dit als attribuut ondertekend door de Stichting Privacy by Design door aan data-afnemers.

IRMA kan gecombineerde informatie doorgeven (aggregatie) en delen ervan (filtering).



Figuur 9. Overzicht IRMA

[18] https://afsprakenstelsel.medmij.nl/display/PUBLIC/Beheerverantwoordelijkheden. In Dutch.
[19] https://pds.mydex.org/mydex-terms-members
[20] https://www.qiyfoundation.org/qiy-scheme/what-is-a-scheme/organisation/
[21] IRMA. https://irma.app

4 Een landschap vol oplossingen

4.1 TYPERING IN HET LANDSCHAP

Wat is Qiy? Wie is IRMA? Doet Ockto hetzelfde als Schluss? Wat zijn de verschillen tussen MedMij en Nuts? Is MyData een afsprakenstelsel of een PDM service? En hoe verhouden al de initiatieven in het PDM landschap zich tot elkaar?

Om tot meer overzicht en inzicht te komen van dit landschap maken we aan de hand van het referentiemodel een analyse van PDM-initiatieven. Deze analyse moet duiden welk onderscheid er is tussen de verschillende initiatieven. Het moet inzicht geven in de status van de bestaande initiatieven en welke functionaliteiten ze bieden. Dit onderzoek heeft als doel kennis op te bouwen van het PDM-landschap en de mogelijkheid bieden om (nieuwe) initiatieven te positioneren.

Om dit te kunnen doen maken we vooraf een onderscheid in de volgende type initiatieven:

1. Speelveld – groepen die zich bezighouden met de ontwikkelingen van het veld, onderzoeksprogramma's en beleidsinitiatieven. Dit kunnen zowel communities als programma's zijn.
2. Wetgeving – wetgeving die specifiek relevant is voor PDM
3. Afsprakenstelsels– afsprakenstelsels die specifiek relevant zijn voor PDM
4. Operators – Een dienst die een individu in staat stelt om zijn/haar persoonlijke informatie duurzaam te beheren en te onderhouden om deze, wanneer de gebruiker dit in zijn belang acht, te kunnen delen met anderen.
5. Authenticatievoorzieningen – voorzien primair in gegevensuitwisseling ten behoeve van het online identificeren van de gebruiker en diens autorisaties (machtigingen) voor toegang tot diensten.
6. Technologie – PDM-oplossingen kunnen op een veelheid van technologieën en standaarden zijn gebaseerd. Sommigen zijn uitermate relevant voor dit domein; deze nemen we mee.

Tabel 1. Overzicht besproken concepten en oplossingen.

Speelveld	Wetgeving	Afsprakenstelsels	PDM Services	Authenticatie	Technologie
Blauwe Knop	Archiefwet	iSHARE	Dappre	Cleverbase ID	Blockchain
Common ground	AVG (GDPR)	MedMij	Emrex	DigiD	GPF
E-Estonia	eIDAS	Qiy	fiKks	EduID	Idemix
EDUmij	PSD2		Financieel Paspoort	eHerkenning	NLX
IHAN	WetDO		Geens NPO	Idensys	NUTS
iSociaal			IRMA	iDIN	OAuth
Machtigen			Ivido	Itsme	openBadges
MyData Global			Meeco	MobileID	OpenID
Regie op Gegevens			MijnOverheid	SURFconext	PKIoverheid
TADA			Pensioen-overzicht		SAML
			Ockto		UMA
			Schluss		X-tee (X-road)
			Solid		Zero knowledge proof

4.2 SPEELVELD

De ontwikkeling van technologie, standaarden en juridische kaders worden veelal gedreven door programma's en communities in het speelveld van regie op persoonlijk gegevens. Deze groepen zijn een drijvende kracht zijn achter veel initiatieven, maar zijn zelf niet als bijvoorbeeld 'PDM Service' of technologie te beschrijven. Denk hierbij aan een community als MyData Global of het programma Regie op Gegevens. Dit soort netwerken en programma's zijn van groot belang om regie op persoonlijke gegevens te realiseren.

4.2.1 Communities

MyData Global: MyData Global[22] is een non-profit organisatie met leden over de hele wereld die de principes van de MyData declaration onderschrijven. MyData is voornamelijk een netwerk. Het doel van MyData is om personen de regie over gegevens terug te geven. Binnen de MyData community zijn er specialisten en

[22] MyData Global. www.mydata.org

onderzoekers van zowel publieke als private partijen te vinden die zich bezighouden met regie op persoonsgegevens.

TADA: TADA[23] is een beweging voor een verantwoorde digitale stad. Waarbij mensen zeggenschap en controle houden over data. TADA draagt in een manifest zes uitgangspunten uit voor het ontwerp van de verantwoorde digitale stad.

4.2.2 Programma's

Regie op Gegevens: Het programma werkt aan een 'kader voor regie op gegevens'[24] door middel van werkgroepen waarin de diverse publieke en private belanghebbenden zijn betrokken. Het 'kader voor RoG' is een normenkader waarin generieke, sector-overstijgende randvoorwaarden en uitgangspunten worden beschreven. Daarnaast stimuleert het programma initiatieven via simulaties, hackatons en pilots.

Common ground: Common Ground[25] is een programma voor hervorming van de gemeentelijke informatievoorziening. Het uitgangspunt is het meervoudig gebruiken van gegevens bij de bron. Op dit moment worden gegevens door gemeenten namelijk vaak gekopieerd, wat foutgevoelig is, sneller zorgt voor verouderde gegevens en het onoverzichtelijk maakt waar gegevens van een persoon staan. Common ground streeft naar: uniforme gegevens, ophalen van gegevens via API's, één gemeenschappelijke integratielaag (NLX) en data bij de bron.

IHAN: IHAN[26] is een programma vanuit het Finse Innovatie Fonds Sitra. De intentie van IHAN is om een governance framework, architectuur definities en requirements op te stellen voor de componenten van een 'data-driven' wereld. Een belangrijke stap hierin is de 'IHAN blueprint'[27] die omschrijft wat de componenten van het IHAN ecosysteem doen, waaronder een 'IHAN identifier' voor personen. De blueprint is momenteel in ontwikkeling.

Machtigen: Het overheidsprogramma 'Machtigen'[28] moet het recht om iemand te machtigen verbeteren. Het programma steeft ernaar om machtigen gebruiksvriendelijker te maken, wettelijke vertegenwoordigers rechtstreeks zaken te laten doen met de overheid en nieuwe vormen van machtigen, zoals nabestaandemachtiging, mogelijk te maken. Het programma bouwt voort op DigiD Machtigen[29].

I4Sociaal: i4Sociaal[30] is een samenwerkingsprogramma van een aantal gemeenten[31]. Binnen het i4Sociaal programma willen gemeenten Enschede, Deventer, Groningen, Zwolle, Leeuwarden en Zaanstad, samen met Dimpact, de 'systeem-en leefwereld' dichter bij elkaar brengen. Regie op eigen gegevens staat daarbij centraal. Binnen het programma is het platform MaximaalJezelf ontwikkeld. Inwoners kunnen op dit platform een profiel aanmaken, in dit profiel kan de inwoner gegevens toevoegen en ophalen middels DigiD. Op basis van de gegevens kan de gemeente passende oplossingen bieden en informatie tonen. De gegevens van de inwoner moeten helpen om te bepalen of hij/zij recht heeft op een voorziening en het makkelijker en sneller maken voor hulpverleners om de situatie van de inwoner te begrijpen.

Blauwe Knop Programma: De Blauwe Knop[32] is een initiatief dat is ontstaan vanuit het Kloosterhoeveberaad, met als doel mensen meer regie te geven op hun eigen gegevens. VNG Realisatie trekt dit initiatief samen met andere uitvoerders (zie ook Blauwe Knop onder 4.7 Operators). Het Nederlandse programma is geïnspireerd door het 'Blue Button Initiative' voor het downloaden van zorggegevens in de US [33].

---

[23] TADA. https://tada.city/
[24] Regie op Gegevens. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/gegevens/regie-op-gegevens/
[25] Conmon Ground. https://commonground.nl/ en https://vng.nl/artikelen/common-ground
[26] IHAN Proof of concept pilots. https://www.sitra.fi/en/projects/ihan-proof-concept-pilots/#what-is-it-about
[27] IHAN Blueprint. https://media.sitra.fi/2018/11/14144842/261018-ihan-blueprint-2.0.pdf
[28] Programma Machtigen. https://www.rijksictdashboard.nl/projecten/573449
[29] DigiD machtingen. https://www.digitaleoverheid.nl/dossiers/digid-machtigen/
[30] iSociaal. https://i-sociaaldomein.nl/
[31] Dimpact i4sociaal. https://www.dimpact.nl/i4sociaal
[32] Blauwe knop. https://www.vngrealisatie.nl/producten/blauweknop
[33] Blue Button Initiative. https://www.healthit.gov/topic/health-it-initiatives/blue-button

EDUmij: Het idee 'EDUmij' is ontstaan vanuit de Informatiekamer, waar onderwerpen in de informatieketen binnen het onderwijs besproken worden. De informatiekamer is een door OCW voorgezeten overleg van onderwijspartijen die acteren in de verschillende onderwijssectoren: OCW, DUO, de Onderwijsinspectie, PO-raad, VO-raad, MBO-raad, VH, VSNU, saMBO~ICT, Kennisnet en SURF. EDUmij positioneert zich op dit moment als volgt: een mechanisme of voorziening die het mogelijk maakt voor een lerende en zich ontwikkelende persoon om levenslang regie te voeren over eigen leer- en ontwikkelgegevens. Daarbij wordt EDUmij een implementatie van persoonlijk data management. Op dit moment onderzoekt EDUmij echter nog in welke richting het zich moet gaan ontwikkelen: afsprakenstelsel, operator of faciliterend programma.

e-estonia: Vanaf 1994 heeft de Estse overheid gewerkt aan een digitale overheidsinfrastructuur onder het concept e-estonia.[34] Begin deze eeuw leidde dit tot de introductie van de x-road infrastructuur voor gegevensuitwisseling en e-ID en digital signature services. Stap voor stap heeft Estland, vanuit een heldere visie en op basis van een uitgangsituatie waar er helemaal geen infrastructuur was, zich ontwikkeld tot de meest geavanceerde e-overheid infrastructuur (samen met Oostenrijk en Malta als leiders in Europa[35]). Estland wordt door velen gezien als een rolmodel voor e-diensten. Met maar 1,3 miljoen inwoners is de situatie niet vergelijkbaar met een land als Nederland, laat staan Duitsland. Toch is de manier waarop vanuit een visie de infrastructuur wordt ontwikkeld lovenswaardig, waarbij men ook bereid is pragmatische keuzes te maken. Het concept van regie op gegevens speelt in Estland vrijwel niet; de focus ligt op elektronische identiteiten en overheidsgegevensuitwisseling op basis van een wettelijke basis en transparantie.

4.3 WETGEVING

AVG (GDPR): De Algemene verordening gegevensbescherming (AVG)[36] gaat over het rechtmatig omgaan met persoonsgegevens. De AVG is de Nederlandse implementatie van de Europese verordening GDPR[37] (General Data Protection Regulation). De belangrijkste regels voor omgang met persoonsgegevens zijn hierin vastgelegd. Deze regels hebben gezorgd voor een uitbreiding en versterking van de privacy-rechten van personen. Er is meer verantwoordelijkheid belegd bij organisaties. Het geeft daarnaast toezichthouders, zoals de autoriteit persoonsgegevens in Nederlands, de bevoegdheid om boetes op te leggen aan overtreders van deze verordening. De AVG is een van de belangrijkste drijfveren van PDM in Europa en legt de wettelijke basis waarop PDM initiatieven voortbouwen.

eIDAS: De Europese eIDAS-verordening voor erkenning van nationale elektronische identificatie-oplossingen is op 29 september 2018 ingegaan[3839]. De verordening bepaald dat publieke organisaties en private organisaties met een publieke taak Europees erkende inlogmiddelen moeten accepteren binnen de digitale dienstverlening. Deze verplichting geldt onder meer voor organisaties die gebruik maken van DigiD. De Europese Unie wil hiermee regelen dat het makkelijker en veiliger wordt om binnen Europa online zaken te regelen. Bij een eIDAS login wordt een minimale set van persoonsgegevens wordt uitgewisseld met de betreffende dienstverlener. Deze set bestaat uit voor en achternaam en geboortedatum en persistent identifier. Optioneel kunnen ook adres, geslacht, geboorteplaats en familienaam (naam bij geboorte) worden opgevraagd.

[34] https://e-estonia.com/
[35] https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2019-trust-government-increasingly-important-people

[36] AVG. https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg
[37] GDPR. https://gdpr-info.eu/
[38] eIDAS vanuit Europa. https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32014R0910
[39] eIDAS vanuit de digitale overheid. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/eidas/

WetDO: De Wet Digitale Overheid is op dit moment nog een wetsvoorstel[40] [41]. In 2019 had het in werking moeten treden, op dit moment wordt echter nog gewerkt aan de details van de wetgeving. De WetDO betreft een infrastructuur voor het authentiseren van burgers; publieke dienstverleners zijn verplicht de authenticatiemiddelen die zijn toegelaten onder de WetDO te accepteren. In ieder geval zullen dit DigiD en eHerkenning zijn. De gegevens die onder WetDO kunnen worden uitgewisseld zijn ook de gegevens die de toegelaten authenticatiemiddelen kunnen verwerken. Voor DigiD is dat voorlopig BSN en voor eHerkenning is dat op dit moment een pseudoniem van de gebruiker, een KvK nummer van het bedrijf namens wie deze handelt en een machtiging hiervoor. (NB. De naam van de wet GDI, wet generieke digitale infrastructuur, is veranderd in naar de 'Wet Digitale Overheid).

PSD2: Het Payment Service Directive 2 (PSD2)[42] is de nieuwe Europese richtlijn voor betalingsverkeer van consumenten en bedrijven. Onderdeel van PSD2 is dat het voor derde partijen mogelijk wordt om transactiegegevens te verwerken, met toestemming van de rekeninghouder. Dit betekent dat het makkelijker wordt voor organisaties buiten de banken om financiële diensten aan te bieden, zoals een huishoudboekje of het realiseren van één financieel overzicht over meerdere bankrekeningen. Niet 'zomaar' alle derde partijen mogen hier gebruik van maken. Hier is een vergunning voor noodzakelijk die in Nederland bij de DNB moet worden aangevraagd.

PDS2 is net als de AVG een drijfveer voor de ontwikkeling van PDM initiatieven, echter primair op de financiële sector gericht. De veranderingen die hiermee in het financiële systeem ontstaan zorgen ervoor dat er meer kans ontstaat voor een PDM ecosysteem in de financiële sector.

Archiefwet: De archiefwet is een wetgeving uit 1995,[43] waarin beheer en toegang van overheidsarchieven geregeld wordt. Bewaartermijnen kunnen kort zijn, bijvoorbeeld een paar jaar, of lang, bijvoorbeeld tientallen jaren. Als de bewaartermijn voorbij is, moeten overheden de documenten vernietigen. In selectielijsten wordt vastgelegd welke informatie overheidsorganisaties willen bewaren en voor hoelang. De archiefwet is met name relevant voor overheidspartijen en PDM oplossingen in de publieke sector.

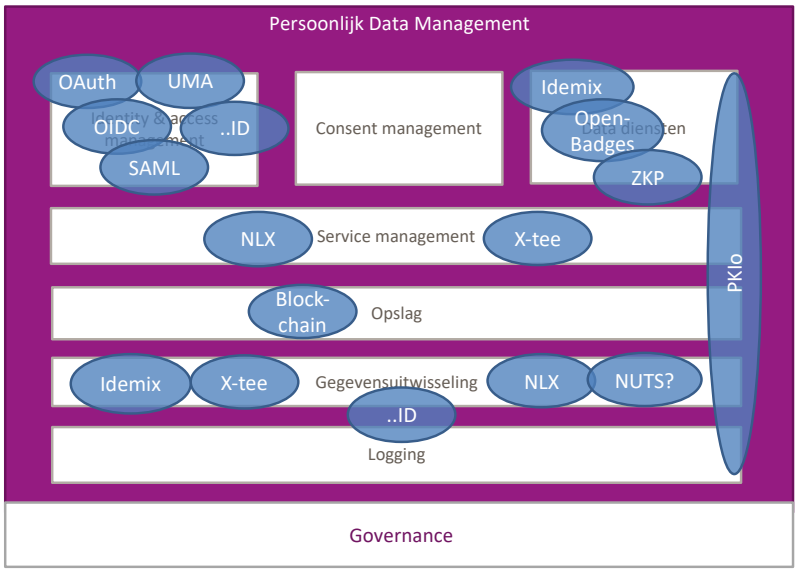
4.4 TECHNOLOGIEËN EN STANDAARDEN

De geanalyseerde technologieën zijn verdeeld in vier subcategorieën: concept, protocol en standaard voor gegevensuitwisseling. Elk wordt hieronder uitgelegd.

- Concept. Een concept is een abstract idee of plan van hoe bepaalde technologie kan werken om een proces te laten verlopen. Technologische concepten kunnen doorgroeien tot bijvoorbeeld protocollen, standaarden of PDM operators.
- Protocol. Protocollen beschrijven hoe bepaalde processen verlopen en zijn vaak implementaties van concepten. Protocollen zijn nog niet als standaard opgenomen.
- Standaard. Een technologische standaard beschrijft hoe bepaalde processen verlopen. Standaarden worden onderhouden vanuit standaardisatie organisaties.

De concepten, protocollen en standaarden voor gegevensuitwisseling die we hier beschrijven zijn technologieën. Een eindgebruiker kan deze niet "zomaar" gebruiken, maar ze maken deel uit van oplossingen die de eindgebruiker wel ziet. In onderstaande figuur is een globale positionering van de technologieën geschetst.

[40] Wetsvoorstel WetDO. https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34972
[41] Wet Digitale Overheid. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/
[42] PSD2. https://www.dnb.nl/betalingsverkeer/psd2/index.jsp
[43] https://wetten.overheid.nl/BWBR0007376/2018-07-28, en https://www.rijksoverheid.nl/onderwerpen/archieven/archieven-van-de-overheid



Figuur 9. Indicatieve positionering van concepten en technologieën in het referentiemodel

4.4.1 Concepten

Blockchain. Een Blockchain, ook wel een distributed ledger genoemd, is een lijst van transacties (blokken), die aan elkaar gelinkt zijn. Blockchain transacties kunnen, nadat het grootse deel van de deelnemers in de blockchain de transactie heeft goedgekeurd, niet meer worden gewijzigd. Dit maakt het blockchain systeem erg uniek, samen met het decentrale karakter: er is niet één organisatie die alles te zeggen heeft. Een voorbeeld van een blockchain toepassing is de European Blockchain Services Infrastructure Pilot voor diploma registraties[44]. Blockchain implementaties zijn geen voor de hand liggende manier om persoonsgegevens uit te wisselen, omdat data voor iedereen toegankelijk is, kan iedereen alles zien. Daarbij biedt blockchain een oplossing als er geen vertrouwen is in de sector of een centrale partij, dat is in de EU landen minder een probleem.

Zero knowledge proof. Een zero knowlegde proof[45] is een wiskundige manier om te bewijzen dat je kennis hebt van een zeker gegeven, zonder dat gegeven daadwerkelijk te laten zien. Dit gegeven kan dus ook een persoonlijk gegeven zijn. Zero knowledge proofs worden gebruikt in Idemix, het protocol dat gebruikt wordt in IRMA.

4.4.2 Protocollen

De protocollen Idemix, X-tee, NLX, NUTS zijn manieren om gegevens uit te wisselen, maar zijn (nog) geen standaard.

Idemix. Idemix[46] is een protocol waarmee een partij gegevens kan opvragen van verschillende partijen en deze vervolgens weer anoniem en unlinkable kan delen met andere partijen. Idemix gebruikt zero-knowledge proofs en wordt gebruikt in IRMA.

X-tee. X-tee[47] is een protocol waarmee een partij bij verschillende bronnen data kan ophalen. X-tee is ontwikkeld in het e-Estonia project. Voorheen stond X-tee bekend als x-road.

[44] EBSI. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
[45] Zero Knowledge proof. https://en.wikipedia.org/wiki/Zero-knowledge_proof
[46] Idemix. https://cloud.ibm.com/docs/services/identitymixer?topic=identitymixer-getting-started-with-identity-mixer-experimental-
[47] X-tee. https://e-estonia.com/solutions/interoperability-services/x-road/

NLX. NLX[48] is een Nederlands overheidsinitiatief, gebaseerd op X-tee, waarbij een partij bij verschillende bronnen data kan ophalen. NLX is nog een concept waarin op dit moment en prototypes worden ontwikkeld. De NLX is een overheidsdatabus, gericht op het faciliteren van data-uitwisseling tussen overheden.

NUTS. NUTS[49] is een Nederlands initiatief, specifiek voor de zorg, waarmee zorgaanbieders bij verschillende zorgpartijen gegevens kunnen ophalen van de gebruiker. NUTS richt zich op de zorgsector.

4.4.3 Standaarden

De standaarden, OAuth 2.0, OpenID Connect, SAML, UMA, zijn allen standaarden voor gegevensuitwisseling bij het verkrijgen van toegang tot diensten.

OAuth. OAuth 2.0[50] is een standaard die ingezet kan worden om iemand tijdelijk toegang te geven tot een deel van je gegevens zonder hiervoor je wachtwoord te delen met de betreffende partij.

UMA. UMA[51] (User management access) is een standaard waarmee gebruikers toegang kunnen geven aan andere gebruikers tot bepaalde gegevens. UMA bouwt verder op de OAuth standaard.

OpenID, SAML. Zowel OpenID Connect[52] en SAML[53] zijn standaarden waarbij gebruikers federatief kunnen inloggen met een account van partij A bij partij B. OpenID Connect bouwt, net als UMA, verder op de OAuth standaard. SAML wordt onder andere gebruikt in bijvoorbeeld SURFconext, iDIN, DigiD, eHerkenning en Idensys.

openBadges. Openbadges[54] is een manier om diploma's, certificaten en andere bekwaamheden gevalideerd te kunnen delen (Discover Open Badges). Het is een open source technologische standaard (Open Badges v2.0 IMS Final Release). De technologie kan met verschillende operators gebruikt kan worden, waaronder badgr, Badgewell en My Open Badge. Er zijn een groot aantal instellingen aangesloten als data aanbieder, waar je openbadges kunt ophalen. Je kunt de badges vervolgens, met een open badges operator, delen op social media, op websites en via e-mail. EduBadges[55] is een voorbeeld van een implementatie van OpenBadges.

PKIoverheid. PKIoverheid is de Public Key Infrastructure (PKI) van de Nederlandse overheid. Net als elke andere PKI is het een afsprakenstelsel om digitale certificaten uit te geven en te beheren. PKIoverheid wordt beheerd door Logius, de policy authority. PKIo-certificaten bieden aanvullende zekerheden ten opzichte van algemene digitale certificaten. Een digitaal certificaat van PKIoverheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.[56]

Gegevensstandaard Persoonlijke Financiën (GPF): De standaard GPF zorgt voor herkenning van uitgewisselde gegevens en maakt de geautomatiseerde verwerking hiervan mogelijk. De standaard GPF verbindt en helpt structuur aan te brengen bij persoonlijke financiën. GPF maakt gebruik van open standaarden zoals: XML, XML Schema, XPath allen van de W3C. In de toekomst kunnen deze standaarden uitgebreid worden met bijvoorbeeld JSON en JSONpath. Voor de uitwisseling van berichten in technische zin, wordt gesteund op het Qiy framework.

4.5 AUTHENTICATIEVOORZIENINGEN

Een belangrijke rol in dit geheel spelen de authenticatievoorzieningen: daarmee kan een PDM gebruiker (Persoon) worden geauthentiseerd bij data-bronnen of data-afnemers. Een aantal identificatie methodes geven een gebruiker via een afsprakenstelsel toegang geven tot andere partijen. Deze methodes noemen we ook wel

[48] NLX. https://nlx.io/
[49] Nuts. https://nuts.nl
[50] OAuth. https://oauth.net/2/
[51] UMA. https://kantarainitiative.org/confluence/display/uma/UMA+FAQ
[52] OpenIDConnect. https://openid.net/connect/
[53] SAML. http://saml.xml.org/protocols
[54] OpenBadges. https://openbadges.org/get-started/displaying-badges/
[55] EduBadges. https://www.surf.nl/edubadges-nationale-aanpak-voor-inzet-van-badges
[56] PKIoverheid. InnoValor, Hulsebosch, De Vos, 2019

federatieve authenticatie oplossingen. Denk hierbij aan iDIN, eHerkenning,Idensys en het hierboven genoemde PKIoverheid. Met deze methodes wordt het mogelijk om een authenticatiemiddel te gebruiken om in te loggen bij diensten van meerdere relying parties. Dergelijke voorziening worden ook wel identiteitsfederaties of 'authenticatie afsprakenstelsels' genoemd.

iDIN. Bij iDIN loggen gebruikers in via hun eigen bank, de bank authentiseert de gebruiker en geeft een identiteitsverklaring af. iDIN geeft deze verklaring door aan de dienstverlener. iDIN is ontwikkeld door de banken voor consumenten. Bedrijven kunnen iDIN als inlog methode gebruiken om gebruikers te laten inloggen en deze uniek te identificeren. iDIN is daarmee een authenticatie afsprakenstelsel, waar banken zichzelf op kunnen aansluiten. Attributen die middels iDIN ontsloten worden zijn: naam, adres, leeftijdsindicatie, geboortedatum, geslacht, e-mail adres en telefoonnummer[57].

eHerkenning. In eHerkenning loggen gebruikers in via een middel dat is aangeschaft bij een van de deelnemers binnen eHerkenning. eHerkenning is voor bedrijven die zaken willen doen met de overheid en daarvoor moeten inloggen op bepaalde eIDAS betrouwbaarheid niveaus. eHerkenning is daarmee een authenticatie afsprakenstelsel, waar bedrijven zich op kunnen aansluiten. Attributen die eHerkenning ontsluit zijn onder andere: naam, leeftijdsindicatie, geboorteplaats, geslacht, e-mailadres, telefoonnummer, organisatie, KvK nummer en identifiers.[58]

Idensys. Met Idensys kunnen gebruikers op verschillende veiligheid niveaus inloggen bij publieke en private diensten. Op dit moment kan je bij Idensys inloggen via een speciaal account aangevraagd bij KPN, Reconi of digidentity. Het Idensys afsprakenstelsel deed samen met iDIN mee aan een overheidspilotvoor het gebruik van private inlogmiddelen bij publieke diensten, zoals de Belastingdienst. De Idensys pilot is op dit moment stopgezet; er kan niet meer mee worden ingelogd bij overheidsdiensten.

EduGAIN. EduGAIN[59] biedt studenten de mogelijkheid om met hun onderwijs account in te loggen bij andere instellingen en diensten. Het focust zich op het internationale onderwijs en omvat onder andere de Nederlandse SURFconext en Zwitserse SWITCH identiteitsfederaties. Het is dus een overkoepelend authenticatie afsprakenstelsel. Voor het uitwisselen van persoonsgegevens over studenten en medewerkers zijn afspraken gemaakt over welke standaarden te gebruiken voor de uitwisseling (SAML) en betreffende het gegevensmodel (eduPerson en SHAC).

SURFconext. SURFconext[60] focust zich op middelbaar en hoger onderwijs en onderzoek in Nederlands en laat gebruikers met hun universiteit of hbo-account inloggen bij andere instellingen en services. De dienstaanbieder kan zelf kiezen welke teams of personen hij toestaat tot zijn dienst. Attributen die worden ontsloten via SURFconext zijn onder andere: naam, e-mailadres, organisatie, type organisatie, werknemer/student nummer, taal en identifiers[61].

Er zijn een aantal initiatieven bekeken, namelijk DigiD, PKIoverheid, Itsme, Cleverbase ID en MobileID, die focussen op wie een gebruiker is en deze gebruiker op een unieke manier identificeerbaar maken. Deze unieke identiteit kan vervolgens aan andere partijen (digitaal) getoond worden.

DigiD. DigiD is de Nederlandse oplossing voor het authentiseren van burgers die in willen loggen bij dienstverleners in het BSN-domein. De onderliggende standaarden van DigiD zijn openID connect en SAML. DigiD is toegankelijk voor partijen die direct het BSN nummer van burgers moeten verwerken: zorg-, pensioen- en andere overheidsorganisaties. Een relying party die het BSN na een DigiD inlogsessie van een gebruiker heeft ontvangen kan op basis daarvan extra gegevens uit de Basis Registratie Personen (BRP) halen, zoals voor- en achternaam, geboortedatum, adres en geslacht.

---

[57] iDIN attributen. https://www.idin.nl/over-idin/veelgestelde-vragen/
[58] eHerkenning attributen. https://extranet.eherkenning.nl/1.11/attribuutcatalogus.xml
[59] eduGAIN. https://edugain.org/
[60] SURFconext. https://www.surf.nl/en/SURFconext-global-access-with-1-set-of-credentials
[61] SURFconext attributen.
https://wiki.surfnet.nl/display/surfconextdev/Attributes+in+SURFconext#AttributesinSURFconext-Attributeoverview

Itsme. Itsme is een Belgische variant van DigiD, die Belgische burgers een uniek nummer geeft, maar wel publiek en privaat gebruikt kan worden. Dit doet Itsme door gebruikers te identificeren met de Belgische identiteitskaart of via een bank, waarna gebruikers de app kunnen gebruiken om op verschillende plekken hun identiteit te laten zien. In december 2019 is Itsme ook in Nederland geïntroduceerd. Gegevens kunnen in de Itsme app zelf staan, of worden verrijkt door de Belgische overheid via het nationale register voor persoonsgegevens.

Cleverbase ID. Cleverbase ID is een authenticatie voorziening in de vorm van een mobiele app. De gebruiker maakt een CleverbaseID aan en kan vervolgens op andere plekken zijn unieke Cleverbase identiteit gebruiken om in te loggen en documenten te ondertekenen.

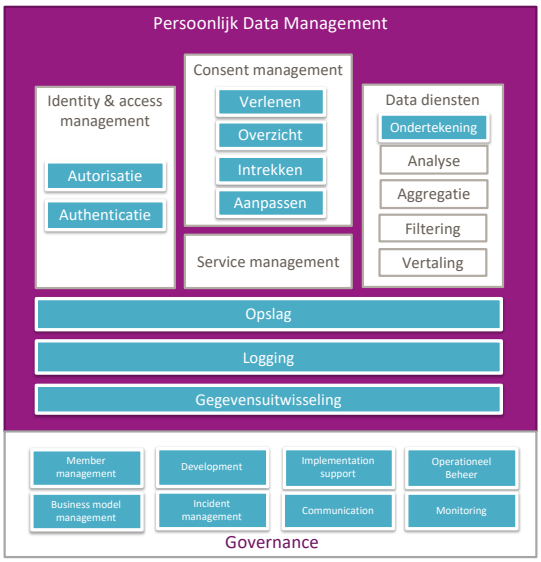
MobileID. MobileID geeft gebruikers de mogelijkheid om een online identiteit te creëren op basis van hun sim kaart. MobileID is een initiatief vanuit e-estonia's e-identity project.

EduID. EduID[62] is nog in concept fase, in tegenstelling tot de andere genoemde unieke ID's. EduID wil zich ontwikkelen tot een unieke identiteit voor studenten, leerlingen en mensen voor al hun educatieve gegevens.

4.6 PDM AFSPRAKENSTELSELS

MedMij: MedMij[63] is een Nederlandse standaard voor het veilig uitwisselen van gezondheidsgegevens tussen jou en zorgprofessionals. Deze uitwisseling vindt plaats via een PGO, een persoonlijke gezondheidsomgeving (oftewel, een operator). MedMij stelt eisen aan de PGO's en data aanbieders, deze zijn opgenomen in het MedMij afsprakenstelsel. Organisaties die hier aantoonbaar aan voldoen mogen het MedMij-label gebruiken. Op moment van schrijven zijn er dertien PGO's gecertificeerd met het MedMij-label.

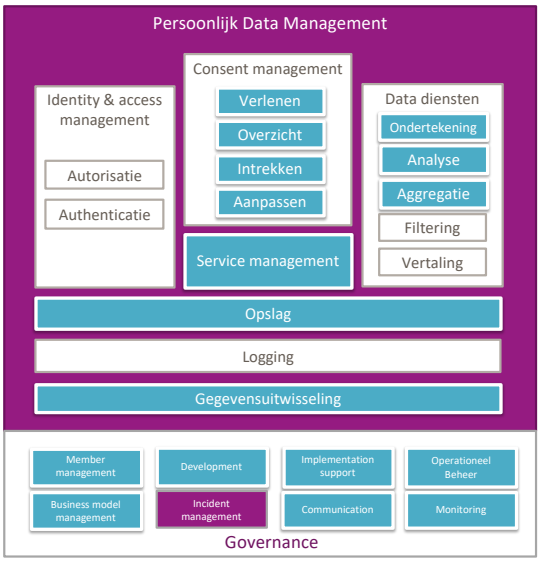
De ontwikkeling van MedMij is mogelijk gemaakt met ondersteuning vanuit het ministerie van Volksgezondheid en Zorgverzekeraars Nederland. Tijdens de projectfase was de Patiëntenfederatie, in samenwerking met Nictiz, de trekker van de ontwikkeling van MedMij. Het afsprakenstelsel is nu in beheer genomen door Stichting MedMij.



Figuur 10. MedMij overzicht.

Wanneer we MedMij in het kader van het referentiemodel bekijken, zijn vooral de functionaliteiten op de governance laag van toepassing, waaronder incident management en regels voor toe en uittreding tot het stelsel. *Blauwe arcering in de afbeelding betekend dat de functionaliteit wel benoemd of gebruikt wordt in het afsprakenstelsel/door de operator.* Naast de governance functies die MedMij heeft, onder andere incident management en operationeel beheer, stelt het eisen aan de functionaliteiten van PGO's in het afsprakenstelsel op het gebied van consent, opslag van gegevens, authenticatie, business model en gegevensuitwisseling.

[62] EduID. https://www.EduID.nl
[63] MedMij. https://www.medmij.nl/

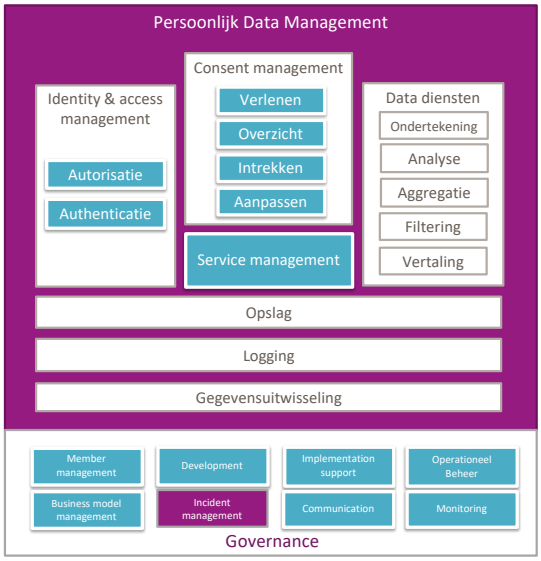


Figuur 11. Qiy overzicht

Qiy: De Stichting Qiy werkt sinds 2007 aan het Qiy Scheme. Dit afsprakenstelsel richt zich op alle individuen, organisaties en apparaten die persoonsgegevens verwerken. In tegenstelling tot MedMij beperkt Qiy zich niet tot een specifieke sector.

Qiy stelt geen specifieke eisen aan authenticatie van personen, het gaat uit van de eisen die de data aanbieder vraagt om de gebruiker te voorzien van gegevens. Het stelsel richt zich voornamelijk op eisen aan consent, opslag en gegevensuitwisseling. Voor de doorontwikkeling van het stelsel bestaan verschillende werkgroepen die opereren binnen de Qiy Foundation en de Review Board die input vanuit werkgroepen beoordeelt. Op dit moment werken drie operators volgens de principes van het Qiy stelsel: Dappre, fiKks en Financieel Paspoort.

iSHARE: Het afsprakenstelsel iSHARE is ontwikkeld in de topsector logistiek in 2017. Het stelsel richt zich op de logistieke sector en betrekt zich met name op gegevensuitwisseling tussen organisaties. Partijen hanteren dezelfde manier van identificatie, authenticatie en autorisatie om elkaar toegang te verstrekken tot data[64]. De afspraken hierover zijn erg gedetailleerd en zorgen ervoor dat zelfs partijen die elkaar niet kennen, gegevens kunnen uitwisselen op basis van 'gedelegeerde autorisaties'. Daarnaast stelt het stelsel eisen aan consent: de eigenaar van gegevens moet altijd de toegang tot data kunnen wijzigen. Over gegevensuitwisseling zelf doet iSHARE geen uitspraken.



Figuur 12. iSHARE overzicht

Het afsprakenstelsel wordt beheerd door de Stichting iSHARE. De stichting ziet toe op naleving van afspraken, beheert processen voor toetreding en faciliteert verbeteringen van het stelsel. De partijen die deelnemer zijn aan het stelsel worden vertegenwoordigd in een Council of Participants. De Change Advisory Board adviseert over doorontwikkeling van het stelsel. Het betreft hier niet direct uitwisseling van persoonsgegevens, echter is iSHARE wel interessant in deze context vanwege de 'gedelegeerde autorisaties' die elders ook toegepast kan worden.

[64] IShare. https://ishareworks.atlassian.net/wiki/spaces/IS/overview

4.7 OPERATORS

Het is op dit moment nog erg lastig om de verschillende operators die we vinden in de markt te vergelijken. Bieden ze puur de mogelijkheid om toestemmingen te managen? Zijn het kluizen waarin we onze gegevens opslaan of bieden ze slechts een beheerfunctie voor gegevensuitwisseling tussen data afnemer en data aanbieder (ook wel 'sluizen' genoemd)? Of iets daar tussenin?

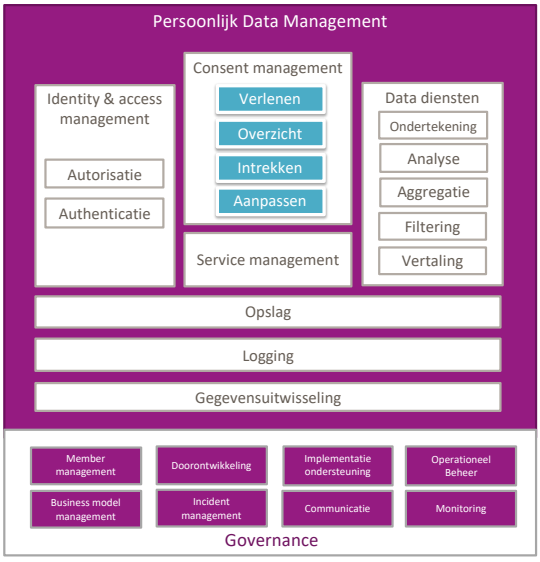
Om overzicht te krijgen in het speelveld en de verschillen tussen de oplossingen beter te begrijpen hebben we een analyse gedaan van operators in Nederland en in het buitenland. Deze analyse brengt de operators in kaart, waarbij gelet wordt op de functionaliteiten en kenmerken zoals we die in het referentiemodel beschreven hebben, plus een aantal kenmerken om de status en marktfocus van de initiatieven in kaart te brengen.

- Algemene kenmerken van de operator
- Governance en onderliggend afsprakenstelsel
- Functionaliteit door de operator geboden, zoals:
    - Wijze van consent management
    - Mogelijke opslag van de gegevens
    - Uitwisseling van de gegevens
    - Logging
    - Aanvullende datadiensten
    - Authenticatie van de gebruiker

Voor de analyse hebben we de volgende werkwijze gehanteerd: op basis van een korte desk research fase zijn alle relevante operators beknopt beschreven. Daarna is met de operator contact gezocht voor middels een vragenlijst (zie bijlage). De uitkomsten van die vragenlijst zijn daarna besproken met de operator en verder aangevuld om vergelijkbaarheid te verbeteren en ter goedkeuring voorgelegd. Op basis van de uitkomsten hebben we een classificatie van operators ontwikkeld die hier onder wordt beschreven. De volledige vragen- en antwoordlijsten zijn beschikbaar. Niet alle operators hebben aan de vragenlijst meegewerkt. Deze operators hebben we wel beknopt beschreven a.h.v. desk research. Daarbij gaat het om Ivido, Emrex, Solid en Digi.me.

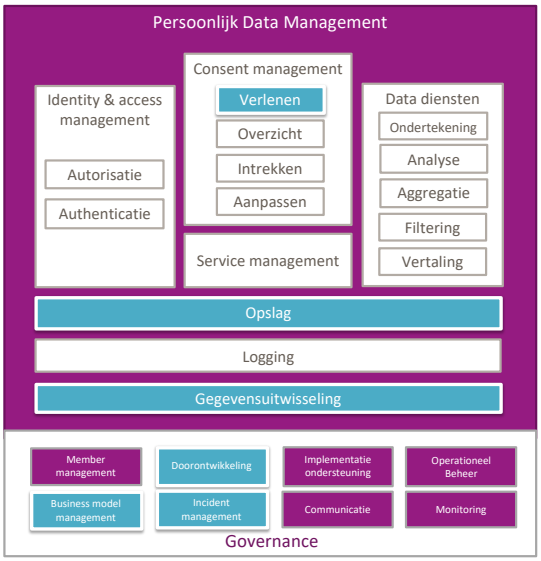
FiKks: FiKks[65] biedt gebruikers de mogelijkheid tot schuldinzage bij schuldeisers. Gebruikers kunnen FiKks machtigen om namens hen of haar inzage te krijgen op hun schulden. Deze worden geanonimiseerd opgehaald bij de authentieke bron. Een netwerk van vrijwilligers geeft vervolgens advies aan de anonieme gebruiker over oplossingen voor de schulden. Gebruikers zijn en blijven anoniem tot zij er zelf voor kiezen hun anonimiteit prijs te geven.

FiKks is een initiatief van de stichting Helden van De Wil en werkt samen met een aantal Nederlandse banken. FiKks volgt de regels van het Qiy afsprakenstelsel. FiKks is operationeel en focust zich op schuldhulpverlening in Nederland.



Figuur 13. Overzicht FiKks

[65] FiKks. https://wijgaanhetfiKksen.nl



Financieel Paspoort: Financieel Paspoort[66] is initiatief dat ijvert voor financiële zelfredzaamheid. Onderdeel daarvan is een mobiele app waarmee gebruikers gemakkelijk een overzicht van hun financiën krijgen, zonder dat andere mensen deze gegevens kunnen inzien of opslaan. Hiermee focussen ze zich op de financiële zelfredzaamheid van de Nederlandse burgers. De gebruiker kan zelf bij verschillende manieren van datadiensten, zoals de belastingdienst, de bank of het pensioenregister, gegevens ophalen en deze opslaan op een locatie en ter beschikking stellen aan een ontvangende organisatie naar keuze. Voor deze uitwisseling is ook de ontwikkeling van de Gegevensstandaard Persoonlijke Financien gestart. Hiermee instrumentaliseert Financieel paspoort de financiële zelfredzaamheid van de Nederlandse burgers. Financieel Paspoort richt zich op alle organisaties die zich bezighouden met de financiële gegevens van de persoon, zoals schuldhulpverlevers, banken, overheden en financiële dienstverleners.

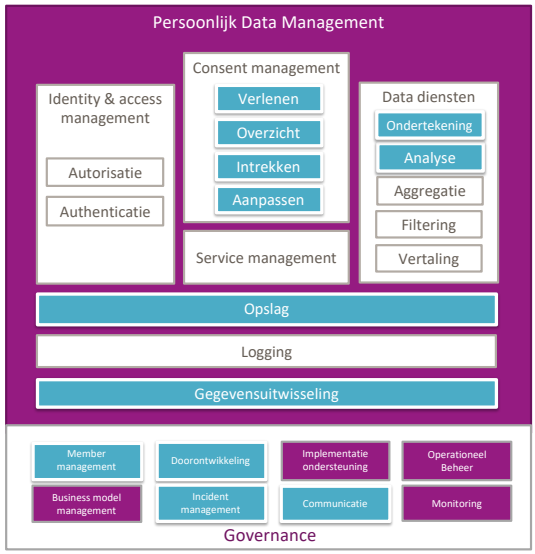
Figuur 14. Financieel paspoort.

Het Financieel Paspoort is ontstaan vanuit de denktank 2015 van het PensioenLab en zit op dit moment in de Pilot fase. De stichting is een burgerinitiatief en heeft geen winstoogmerk.

Buddy Payment: Buddy is een internetbankieren applicatie die is gemaakt om mensen te helpen met hun bankzaken. Buddy helpt kwetsbare Nederlanders met het maken van financiële keuzes. De Buddy app geeft een overzicht van de financiële situatie van de gebruiker, scheidt vaste kosten van leefgeld en geeft financiële tips. De gebruikers kunnen zelf hun gegevens vanuit de banken en schuldeisers in de applicatie laden.

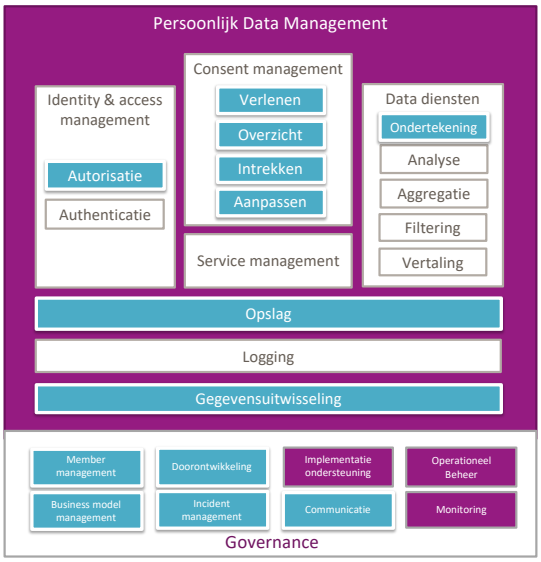
Buddy is ontstaan vanuit een samenwerking tussen gemeentes en de Rabobank. Buddy zit op dit moment nog in de pilotfase en focust zich op de Nederlandse financiële markt.

Buddy staat onder toezicht van AFM en DNB en maakt gebruik van verschillenden richtlijnen waaronder PSD2.



Figuur 15. Buddy payment

[66] Financieel Paspoort. https://financieelpaspoort.nl

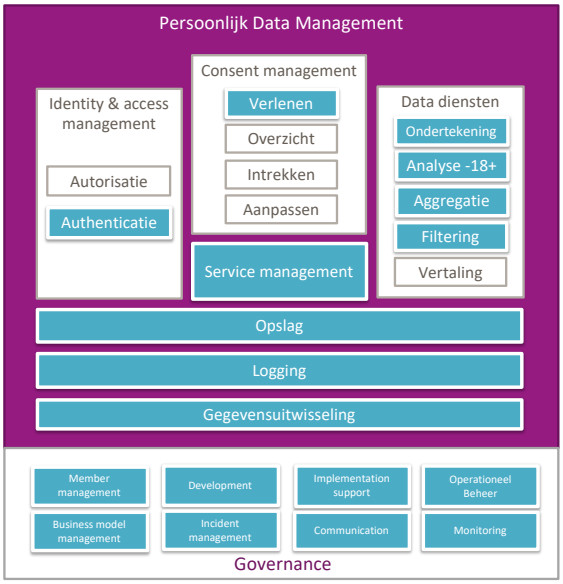


Figuur 16. Overzicht Geens.

Geens NPO: Geens NPO[67] is een onafhankelijk dataopslag platform voor individuen en bedrijven. De gebruiker heeft zelf volledig zeggenschap over hun data en de wijze waarop deze gedeeld wordt met derden. Geens NPO biedt een cloud platform waarom rechtstreeks of met behulp van een API data opgeslagen kan worden door gebruiker en gedeeld kan worden met derden. De data is end-to-end encrypted en kan ondertekend worden met een blockchain tijdsstempel.

Geens NPO is gestart in België en richt zich momenteel primair op de Europese markt. De service is op dit moment operationeel. Individuele gebruikers kunnen een gratis en betaald lidmaatschap afsluiten, bedrijven moeten altijd een betaald lidmaatschap afsluiten.

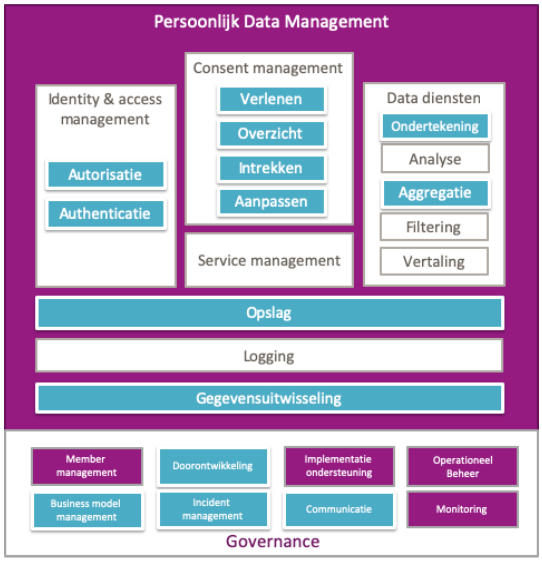
IRMA: IRMA[68] staat voor "I Reveal My Attributes" en is een mobiele applicatie die is gericht op het delen van attributen en het ondertekenen in een digitale wereld. Alleen de attributen die nodig zijn hoeven te worden gedeeld, zonder andere informatie te verstrekken. Zo kan een gebruiker er bijvoorbeeld voor kiezen alleen te bewijzen dat hij ouders is dan 18, zonder zijn geboortedatum prijs te geven. IRMA gebruikt het Idemix protocol om dit te doen. Attributen kunnen zowel in de online als de fysieke wereld worden opgehaald. Typische data aanbieders voor IRMA attributen zijn: BRP (basisregistratie personen), SURF, BIG, AGB (Algemeen GegevensBeheer) en KvK.



Figuur 17. Bouwblokken IRMA

IRMA is begonnen vanuit een initiatief vanuit de Universiteit van Nijmegen en is uitgegroeid tot de Stichting Privacy by Design. Daarbij werken ze sinds kort samen met SIDN. Wanneer data aanbieders data willen ontsluiten de IRMA app, sluiten zij een contract af de Stichting Privacy By Design en SIDN. IRMA is operationeel en focust zich nu op Nederland. IRMA kan, naast operator, ook gebruikt worden als een authenticatie dienst: de attributen die IRMA bevat worden door sommige partijen als login attributen gebruikt. Daarbij is IRMA ook data aanbieder van alle attributen die de app omsluit.

[67] Geens NPO. https://geens.com
[68] IRMA. https://irma.app

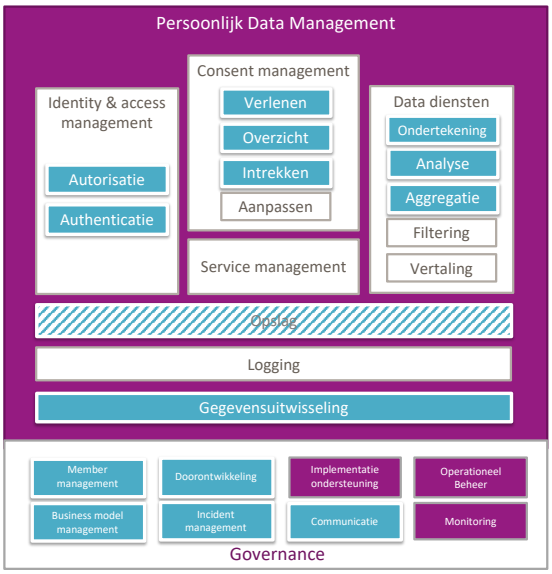


Figuur 18. Overzicht Dappre.

Dappre: Dappre[69] is een mobiele app waarin loyalty- en cadeaukaarten kunnen worden opgeslagen. Gebruikers houden zelf de controle over met welke partij ze persoonsgegevens delen, met welk doel en voor hoelang.

Dappre is ontstaan vanuit Digital Me en is ook gebaseerd op de Qiy Trust Principles. Dappre is operationeel en focust zich op de Europese markt van de consumenten sector. Dappre kan bij onder andere HEMA, Decatlhon, VVV, Albert Heijn en IKEA gebruikt worden.

Ockto: Ockto[70] is een platform waarmee consumenten data kunnen verzamelen vanuit verschillende databronnen en deze data kunnen doorgeven aan een datadienst. Ockto zorgt ervoor dat consumenten snel en simpel informatie kunnen verzamelen en deze met adviseurs, banken, hypotheekverstrekkers of andere dienstverleners kunnen delen. De gebruiker en data aanbieder kunnen Ockto gratis gebruiken, data afnemers betalen een transactie vergoeding als zij data vanuit Ockto willen gebruiken.



Figuur 19. Bouwblokken Ockto.

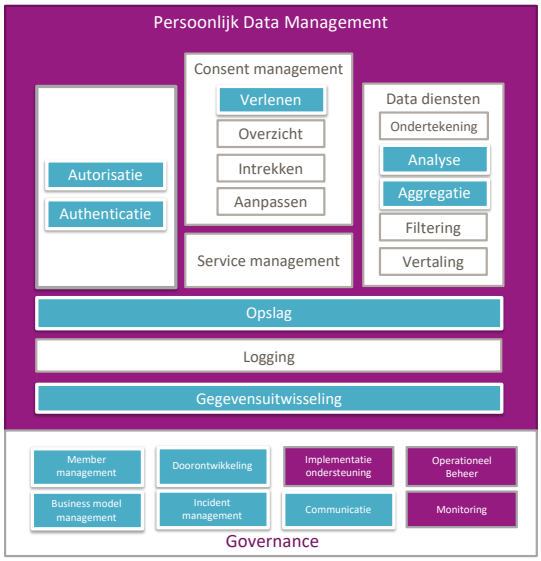
Ockto is een Nederlands initiatief en focust zich op de Nederlandse financiële markt. Ockto is operationeel: op dit moment kan een gebruiker met de Ockto app onder andere gegevens ophalen bij de Belastingdienst, UWV, mijnpensioenoverzicht en MijnOverheid middels een QR code.

De gegevensuitwisseling tussen Ockto en data aanbieders en afnemers verloopt de uitwisseling via API of screen scraping (bij screen scraping is er geen waarmerking vanuit de data aanbieder). De data wordt opgeslagen op het apparaat van de gebruiker en verwerkt op de server van Ockto. Een data-afnemer kan de gebruiker daarnaast vragen om de gegevens maximaal 2 maanden bij Ockto beschikbaar te houden. Daardoor kan een geldverstrekker de persoonsgegevens gebruiken voor het uitbrengen van een aanbod.

[69] Dappre. https://dappre.com
[70] Ockto. https://www.ockto.nl

MijnPensioenoverzicht: MijnPensioen overzicht[71] is een online platform waarop iedere Nederlandse burger een overzicht van zijn pensioenrechten kan opvragen. Daarbij biedt het de mogelijkheid, op verzoek van de burger, aan pensioenuitvoerders om te informeren bij welke andere pensioenuitvoerder een gewezen deelnemer pensioenaanspraken opbouwt ten behoeve van waardeoverdracht van pension. Gebruikers kunnen inloggen via DigiD of eIDAS.

Het pensioenregister is in 2011 opgericht in Nederland en focust zich op de Nederlandse pensioen markt. Het Pensioen register is operationeel en wordt onderhouden door de stichting pensioenregister. Het volgt een wettelijke taak uit (Artikel 51 pensioenweg) en via een regelement wordt bepaald welke gegevens de SVB en de pensioenuitvoerders moeten aanleveren. Stichting pensioenregister beheert geen individuele pensioengegevens van burgers. Deze worden alleen opgehaald bij de verzekeraars en ontsloten voor de individuele burger op het moment dat deze inlogt; alles wordt weer verwijderd wanneer de burger uitlogt.

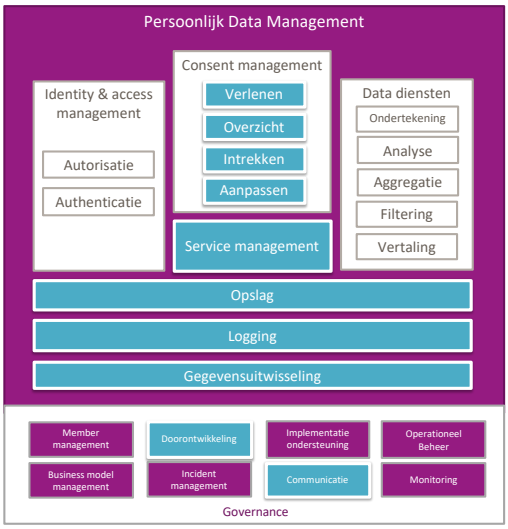


Figuur 20. Pensioenregister.

[71] Mijn pensioen overzicht. https://www.mijnpensioenoverzicht.nl/

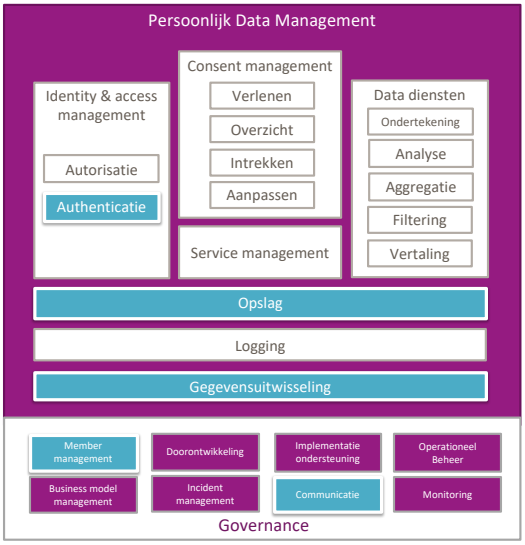
Schluss: Schluss[72] is een service voor het opslag, regie en overzicht over persoonlijke gegevens. Schluss levert een persoonlijke digitale kluis, waarin gegevens opgeslagen kunnen worden. Dit kan gaan om bijvoorbeeld adresgegevens, medische of financiële gegevens. Identificatie en autorisatie wordt gewaarborgd via derden. De persoon bepaald wie toegang krijgt, voor welk doel en voor welke periode. Er is een overzicht van welke inzagen verleend zijn zodat deze ook weer ingetrokken kunnen worden (afhankelijk van de juridische kaders).

Op dit moment zit Schluss in pilot fase. De toekomstvisie van Schluss gericht op het opstellen als kluis voor alle digitale informatie, maar tevens als 'sluis' variant waarbij alleen consent gegeven wordt via Schluss en uitwisseling tussen data aanbieder en afnemer verloopt.



Figuur 21. Overzich Schluss

MijnOverheid: MijnOverheid[73] is een combinatie van digitale post (Berichtenbox) en diensten voor de burger vanuit de overheid. Het geeft inzicht in persoonlijke gegevens die de overheid van de burger heeft. MijnOverheid ontsluit via een portaal de zaken die bij een veelheid van instanties lopen, van kinderbijslag bij de SVB, WOZ-waarde bij het kadaster tot gemeentelijke zaken; een operator voor burgers. Er is onder meer direct inzicht in de data die de basisregistratie personen (BRP) heeft, inkomensgegevens zoals bij de Belastingdienst bekend zijn, woninggegevens van Kadaster en kentekenregistratie van het RDW. Daarnaast wordt er ook naar een aantal andere 'mijn omgevingen' doorgelinkt, waaronder Donorregister, DUO en Pensioenregister.

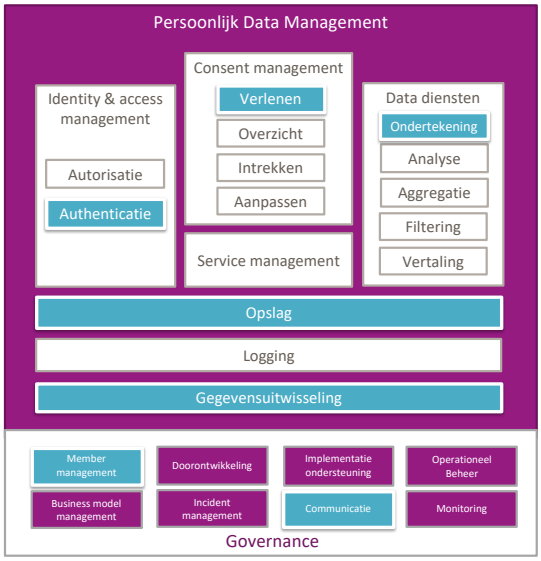


Figuur 22. Overzicht MijnOverheid

MijnOverheid ontsluit primair gegevens richting de burger, het speelt geen rol in het doorgeven van de gegevens aan derden. Gegevensuitwisseling met derden gebeurt door de achterliggende organisaties zelf op basis van wettelijke gronden, niet via de burger. Het is dus nog voornamelijk een data aanbieder, maar puur voor publieke organisaties. Inloggen bij Mijn Overheid gebeurt via DigiD. Sinds oktober 2015 is het gebruik van MijnOverheid voor burgers vanaf 14 jaar verplicht.

[72] Schluss. https://www.schluss.org/
[73] Mijn Overheid. https://mijn.overheid.nl/

MijnOverheid Pilot: Er wordt op dit moment door MijnOverheid verkend hoe de burger meer controle te geven over het delen van de gegevens. Ofwel, hoe aan MijnOverheid operator functionaliteit toe te voegen. Hiervoor wordt geëxperimenteerd in een pilot die zich richt op de use-case huren. In de pilot kunnen aspirant huurders hun inkomensgegevens (BRI) en adresgegevens (BRP) digitaal delen met woningcorporaties. Het doel daarvan is het verminderen van administratieve lasten voor burger en corporatie en het terugdringen van woningfraude, zoals scheefwonen. Middels een API worden gegevens uitgewisseld tussen MijnOverheid en woningcoroporaties. De keuzes van de gebruiker zijn hierin nog beperkt: er kan consent gegeven worden, maar er is geen overzicht of verdere keuze in de uit te wisselen gegevens.



Figuur 23. Overzicht MijnOverheid Pilot.

Ivido: Ivido[74] is een voorbeeld van een Persoonlijke Gezondheidsomgeving (oftewel, een operator gericht op een medische gegevens). Het is een van de initiatieven die een MedMij-label heeft verkregen. Binnen Ivido kunnen mensen medische gegevens bij elkaar brengen en communiceren met zorgverleners en desgewenst met familieleden. Het is ook mogelijk om gegevens vanuit wearables (zoals fitness horloges) toe te voegen. Interessant aan Ivido is dat het gekozen heeft om personen zich te laten identificeren en inloggen met het eerdergenoemde IRMA. Dit zorgt er daarnaast voor dat Ivido over de BRP-gegevens van de persoon beschikt.

Emrex: Emrex[75] is een platform waarom studenten hun gegevens kunnen delen. Wanneer onderwijsinstituten zichzelf hebben aangesloten op het systeem kunnen studenten bij hen inloggen en gegevens van andere instituten ook inladen en delen. Emrex focust zich op het samenbrengen van bestaande oplossingen en niet op het creëren van nieuwe standaarden en operators. Hierdoor raakt Emrex ook aan de functies van een afsprakenstelsels. Emrex is ook onderdeel van ESC (EU student card) afsprakenstelsel. Emrex is een operator, maar kan ook data aanbieder en data afnemer zijn. Emrex is een Europees initiatief, focust zich op de educatieve sector en zit nog in de pilot fase. Er zijn al verschillende instituten aangesloten, waaronder DUO vanuit Nederland, waardoor Nederlandse diploma's toegevoegd zijn.

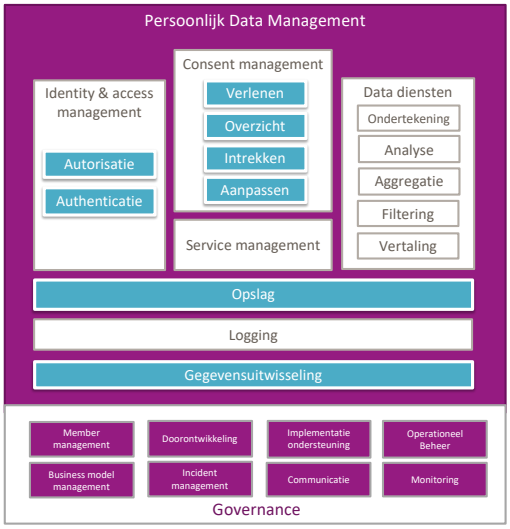
Blauwe Knop: De Blauwe Knop biedt mensen de mogelijkheid hun persoonlijke data te downloaden van overheidswebsites. Mensen kunnen deze data vervolgens zelf gebruiken voor verschillende doeleinden. Schuldhulpverlening is een van de belangrijke thema's waar op dit moment aan gewerkt wordt. De Blauwe Knop moet ervoor zorgen dat gemeenten en uitvoeringsorganisaties op een vergelijkbare manier mensen (deelsets van) persoonlijke data kunnen laten downloaden, in een gewaarmerkt document. In de praktijk krijgen organisaties die de Blauwe Knop willen toepassen een toolkit ter beschikking met het beeldmerk, generieke content, voorbeeldcode en architectuur en een stappenplan voor de implementatie. De Blauwe Knop zorgt daarmee voor standaardisatie van gegevens downloaden bij de overheid. Op termijn moet naast de downloadfunctionaliteit ook functionaliteit beschikbaar komen voor directe gegevensuitwisseling tussen organisaties (Zie ook Blauwe Knop Programma onder 4.2 Speelveld).

[74] Ivido. https://ivido.nl/
[75] Emrex. https://emrex.eu/

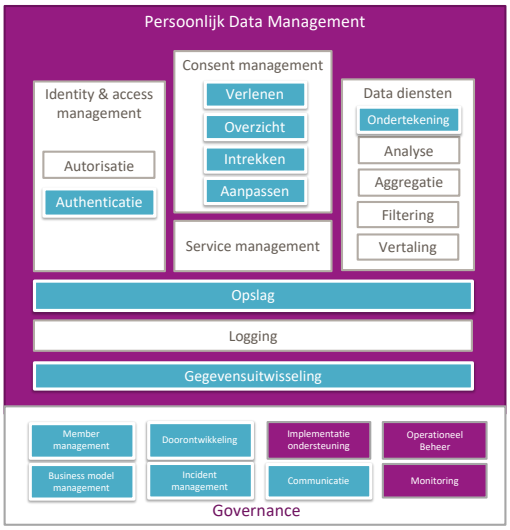
4.8 SELECTIE BUITENLANDSE OPERATORS

PDM is geen Nederlandse ontwikkeling, in tegendeel. Veel ontwikkelingen zijn gestart buiten onze grenzen, zoals OpenPDS, Mydex en Project VRM. Velen daarvan zijn ook alweer gestopt. We bespreken een klein aantal illustratieve voorbeelden.

Personium: Personium (JP) is een open source 'Personal Data Store Server' en is bedoeld als basis voor organisaties om een operator mee te bouwen[76]. OpenID connect (sectie 4.4.3) wordt hierbij toegepast. Onder andere financiële gegevens, energie verbruik en social data worden verwerkt in toepassingen van Personium. Typische gebruikers van Personium zijn banken, energiebedrijven en adverteerders. Personium levert zelf geen diensten direct aan de eindgebruiker. Personium is onder meer de basis van een paar van de Japanse "databanken", een nieuwe door de IT sector gestandaardiseerde rol voor bedrijven.[77]



Figuur 24. Personium



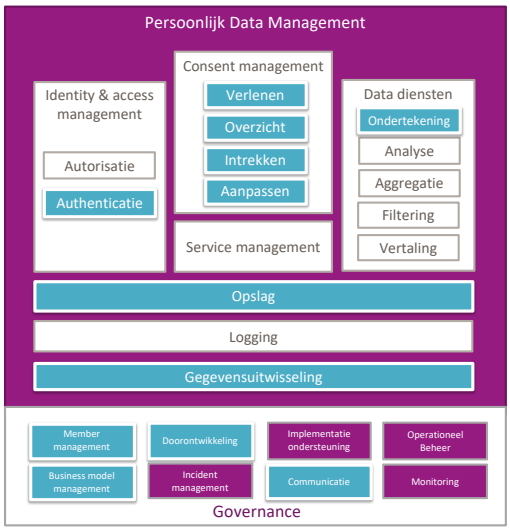
Figuur 25. MyFairData

MyFairData:
MyFairData (voorheen Fair&Smart) is een Frans initiatief dat sinds 2016 actief is[78]. MyFairData richt zich niet op een specifieke sector. Het is een dienst die opslag, veilige gegevensuitwisseling en consentmanagement biedt aan personen en organisaties. Op dit moment is MyFairData in operationele fase, het wordt met name gebruikt door publieke en zorg organisaties. Voor authenticatie maakt het gebruik van OpenID Connect. Gegevensuitwisseling verloopt voornamelijk middels REST API's, alleen onder consent van de persoon. MyFairData geeft garantie dat er niet met data die wordt uitgewisseld is 'geknoeid', maar er het is verder niet voorzien van specifieke waarmerking.

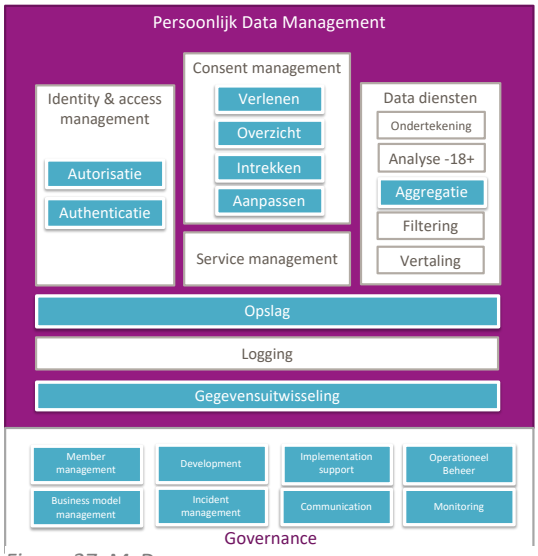
[76] Personium. https://personium.io/en/index.html
[77] Zie, bijvoorbeeld, https://mydata2019.org/programme-page/japanese-data-banks/ voor een korte introductie over de Japanse Data Banken.

[78] MyFairData. http://myfairdata.com/

Comuny: Comuny is een Duits initiatief dat personen een eigen digitale identiteit laat maken en persoonlijke gegevens kan delen met verschillende diensten. Het gaat daarbij met name om authenticatie gegevens. Comuny is op dit moment in de pilot fase. De gebruiker kan persoonlijke data verifiëren (zoals rijbewijs, id kaart en verzekeringskaart) en authenticatiemiddelen creëren (zoals stem of vingerafdruk). Comuny richt zich op dit moment op de verzekeringsketen, en dan met name op applicaties voor het aanmelden van klanten.



Figuur 26. Comuny

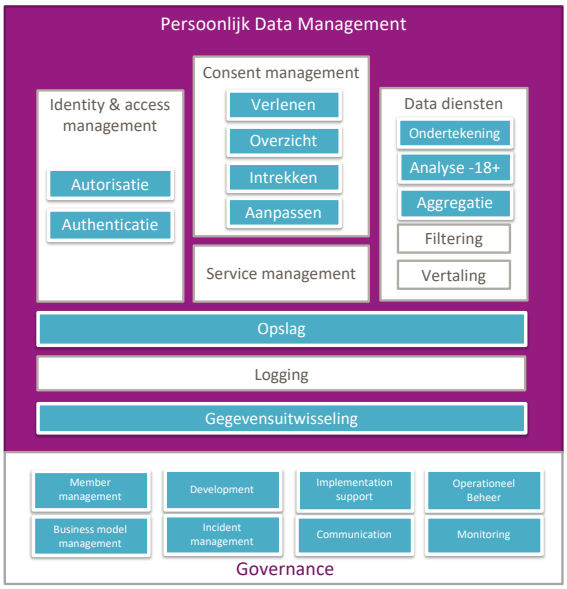


Figuur 27. MyDex

MyDex: MyDex (UK) bestaat al sinds 2007 en is daarmee een van de langst bestaande operators in het landschap, dat gezegd bevindt MyDex zich nog wel in pilotfase. Het levert diensten aan zowel het individu als organisaties. Het individu kan persoonlijke gegevens verzamelen in een overzicht en toegang krijgen tot diensten die gebruik maken van deze gegevens. Het positioneert zich daarmee als 'kluis'. Voor organisaties zorgt MyDex dat diensten geboden kunnen worden aan personen. Partijen die toegang willen moeten wel voldoen aan de regels die MyDex stelt (member management). MyDex focust op dit moment met name op de publieke sector en wordt ook aangeboden via de digital marketplace van de Britse overheid[79]. De cases waar MyDex zich op richt lijken op de 'life events' waar gemeenten in Nederland mee werken zoals schuldhulpverlening, verhuizen en overlijden. Verder maakt MyDex gebruik van meerdere protocollen voor authenticatie waaronder SAML en OpenID Connect.

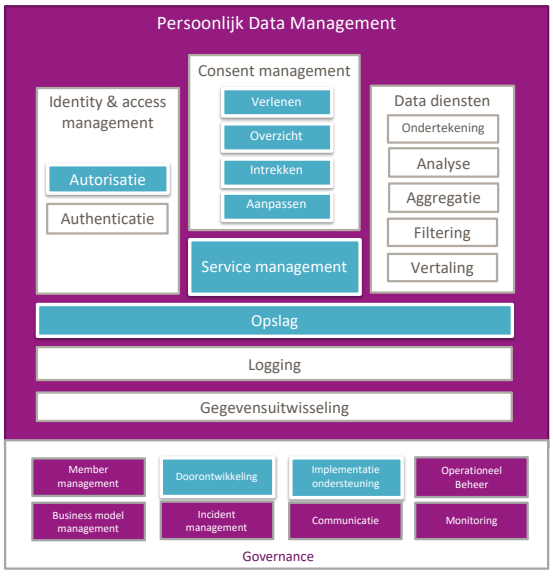
[79] MyDex. https://www.digitalmarketplace.service.gov.uk/g-cloud/services/457530744783729

Meeco: Meeco is een operator die in 2012 is opgericht in Australië. In augustus 2019 heeft Meeco ook een locatie in België geopend. De ambitie van Meeco is om te zorgen dat iedereen waarde krijgt uit de data die ze delen. Dit doet Meeco door te zorgen dat gebruikers gegevens veilig kunnen opslaan en uitwisselen onder consent. Op dit moment heeft Meeco met name financiële implementatie, zoals pensioen- en eigendomsgegevens, maar wil zich wel breed oriënteren. Meeco wisselt gegevens uit middels API's. Het maakt daarnaast o.a. gebruik van OAuth, OpenID connect voor de integratie met derde partijen.



Figuur 28. Meeco

Solid: Solid is een ontwikkeling vanuit MIT, geleid door Tim Berners-Lee (de vader van het World Wide Web). Het richt zich op een totaal andere vorm van dataeigenaarschap op het web. Solid staat voor "Social Linked Data" en is dan ook een verzameling concepten en standaarden om gedecentraliseerde webapplicaties te ontwikkelen gebaseerd op linked data. De fundamentele achterliggende gedachte is dat data losgekoppeld moet worden van toepassingen. Nu bezitten Facebook, LinkedIn en Google jouw data over je netwerk of je documenten en kunnen daarmee nieuwe informatie afleiden ten behoeve van, bijvoorbeeld, adverteerders. In het Solid worden de data over je sociale netwerk, bijvoorbeeld, losgekoppeld van dienst zoals Linkedin of Facebook. Daarmee kun je dan ook eenvoudig van de ene dienst op de andere overstappen en wordt de markt toegankelijker voor nieuwe toetreders: zij kijken immers niet tegen een enorme data-achterstand aan maar kunnen direct bouwen op jouw persoonlijke data, onder jouw regie. Dit betekent dan ook dat er fundamenteel andere bedrijfsmodellen moeten gaan ontstaan. Immers, de data zijn niet meer van de diensteneigenaar en kunnen niet worden gebruikt als inkomstenbron.



Figuur 29. Overzicht Solid met governance vanuit Inrupt

Solid wordt op dit moment vooral ontwikkeld door het bedrijf Inrupt, dat de open source technologie ontwikkeld. Berners-Lee heeft dit samen met John Bruce, voormalig CEO van Resilient, opgezet. Ook vanuit Nederland is er betrokkenheid bij Inrupt. Het feit dat Berners-Lee zijn schouders er onder zet is een belangrijke factor voor het belang van de Solid ontwikkeling.

Data wordt opgeslagen in persoonlijke datadiensten, data pods, die aan de Solid specificatie voldoen. Deze kunnen door (commerciële) dienstverleners worden geleverd. Applicaties koppelen aan een of meerdere pods. Integratie tussen applicaties lopen ook via de pods; het is een volledig gedistribueerde architectuur, er is geen app-to-app communicatie.

Digi.me: Digi.me (UK) is een voorbeeld van een operator die zich zeer breed oriënteert en niet werkt vanuit een specifieke sector. Personen kiezen zelf op welke dienst ze willen gebruiken om de gegevens die via de app verkregen worden op te slaan (Google Drive, Dropbox, OneDrive). De gegevens die met digi.me verzameld kunnen worden zijn divers: financieel, medisch, social, entertainment. De gegevens die opgehaald kunnen worden zijn, buiten de socials en entertainment gegevens, met name gericht op het VK en de VS. De ambitie van digi.me is het creëren van een markt aan apps die vervolgens op basis van de opgehaalde gegevens

diensten kunnen verlenen. Onder consent van de gebruiker: de gebruiker kiest zelf welke apps hij of zij wil gebruiken en tot welke gegevens deze apps toegang krijgen.

5 Conclusies

5.1 ORDE IN DE CHAOS?

Vanuit het overzicht van initiatieven en operators ontstaat niet direct een kristalhelder beeld. We zien een grote diversiteit aan operators, in verschillende stadia van volwassenheid. De rol van afsprakenstelsels is nog beperkt, maar lijkt groeiend: MedMij zorgt voor stimulans onder de PGO's, EDUmij wordt (potentieel) een afsprakenstelsel voor PDM in het onderwijs en drie operators werken inmiddels onder Qiy. Business modellen zijn niet altijd duidelijk en nog beperkt duurzaam. In de schuldhulp zien we initiatieven zonder winstoogmerk (Financieel Paspoort, fiKks) en er wordt voor de ontwikkeling van initiatieven nog geleund op stimuleringsmaatregelen (PGO's). Typische kenmerken van een markt die zich nog moet ontwikkelen, van een ecosysteem dat zichzelf nog aan het uitvinden is.

Ook de programma's in het speelveld die we hebben besproken zijn divers en maar beperkt samenhangend. Voor betrokkenen is het moeilijk overzicht te krijgen en samenwerking te realiseren. De koers binnen de overheid op dit vlak is nog niet eenduidig, verschillende ministeries zetten verschillende koersen uit. In het BZK programma Regie op Gegevens worden pilots die experimenteren met PDM gestimuleerd[80]. Echter worden er ook kritische Kamervragen gesteld aan OCW over de koppeling van hypotheekverstrekkers met studieschuld gegevens van DUO[81]. Voor de stakeholders is gegevensuitwisseling op deze manier relatief nieuw en moeten nog nadenken over wat ze in de context van PDM wel of niet mogen, en wel of niet willen.

Volwassenheid van het landschap

Een aantal operators is de pilotfase al ontstegen, al is de schaal waarop ze worden gebruikt nog beperkt, even los van gevestigde initiatieven als het pensioenoverzicht. Ockto heeft onder meer samenwerkingsverbanden met ABN AMRO en Rabobank. Ook fiKks en Financieel Paspoort worden in beperkte mate al gebruikt. De adoptie van IRMA groeit ook sterk, met veel pilots bij gemeenten en een aantal koppelingen in de zorg.

Alle operators in het landschap staan nu nog los van elkaar; interoperabiliteit is nog geen aandachtspunt bij de operators. Financieel Paspoort, Dappre en fiKks bouwen voort op Qiy als afsprakenstelsel; dit leidt echter (nog) niet tot interoperabele oplossingen. Er worden alsnog bilaterale afspraken en SLA's gemaakt. Daarnaast zien we ook operators die zich los van afsprakenstelsels ontwikkelen zoals Schluss en Ockto.

In de rest van Europa is de situatie niet veel anders: we zien een aantal opkomende operators met meerdere pilots. Uitzonderingen zijn digi.me en Meeco die al meerdere jaren bestaan en ook internationaal sterk groeien. Beide zijn ook relevant voor de Nederlandse situatie; Digi.me is sinds kort ook in het Nederlands beschikbaar. Meeco is ontstaan is Australië, maar heeft inmiddels zijn thuisbasis in Brussel.

Functionele verschillen – dataopslag

Een belangrijk onderscheid tussen oplossingen zit in de benadering van data: daarbij kan de operator alleen data doorgeven, data opslaan/aggregeren, afgeleide informatie afgeven of zelfs ondertekenen. Ockto en digi.me zijn primair gericht op data doorgeven, net als FiKks; Financieel paspoort is er juist op gericht de data te aggregeren voor dat doel. IRMA slaat gewaarmerkte informatie op in de app, en kan zelf ook afgeleide attributen waarmerken. Daarmee worden data-leverancier en data-afnemer van elkaar ontkoppelt: de bron weet niet wie de data gebruikt en hoeft ook niet met de afnemer te koppelen. Het gebruik van afgeleide attributen is daarbij ook waardevol: in plaats van je id-kaart te laten zien, of je geboortedatum, kan alleen het feit dat je 18+ en 65- bent worden gedeeld.

Een voordeel van alleen doorgeven (en dus niet opslaan) is dat de operator geen verwerker is van de data. De rol van de operator is daarmee beperkt. Dit is een vorm van privacy-by-design en data minimalisatie. Aan de

[80] Hackathon Regie op Gegevens. https://rog.pleio.nl/news/view/57899734/uitnodiging-regie-op-gegevens-hackathon

[81] Kamervragen studieschuld DUO. https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2019Z18615&did=2019D47108

andere kant, als data wordt opgeslagen en via de operator wordt gedeeld, beperkt de ontkoppeling van leverancier en afnemer ook de hoeveelheid informatie die nieuw in de transactie ontstaat, namelijk de relatie tussen bron en afnemer. Ook dat is privacy by design. Voor beide is dus iets te zeggen.

Functionele verschillen – identiteit

Net zoals persoonlijke data kan worden opgeslagen in de operator, kopiëren (cachen) sommige operators ook de identiteit. Deze kunnen daarmee als inlogmiddel gaan functioneren. Met name IRMA doet dit, waardoor IRMA nu al inlogmiddel ingezet kan worden door Ivido en VGZ (pilot). Ook gemeenten onderzoeken deze rol van IRMA. Ook van Self Sovereign Identities (als concept) is het idee dat deze identiteit van gebruikers kunnen hergebruiken.

Tussen operators en authenticatiestelsels zit een grijs gebied: bij het identificeren van een persoon worden ook gegevens uitgewisseld. Neem bijvoorbeeld iDIN: er worden geverifieerde gegevens als naam en leeftijdsindicatie gedeeld met de dienstverlener wanneer een persoon met iDIN bij een dienst inlogt. De bank is de data aanbieder en de dienstverlener de data afnemer. Daartussen zit typisch een DISP (digital identity serviceprovider) die integratie verzorgt en consent vraagt.

Van authenticatie naar PDM

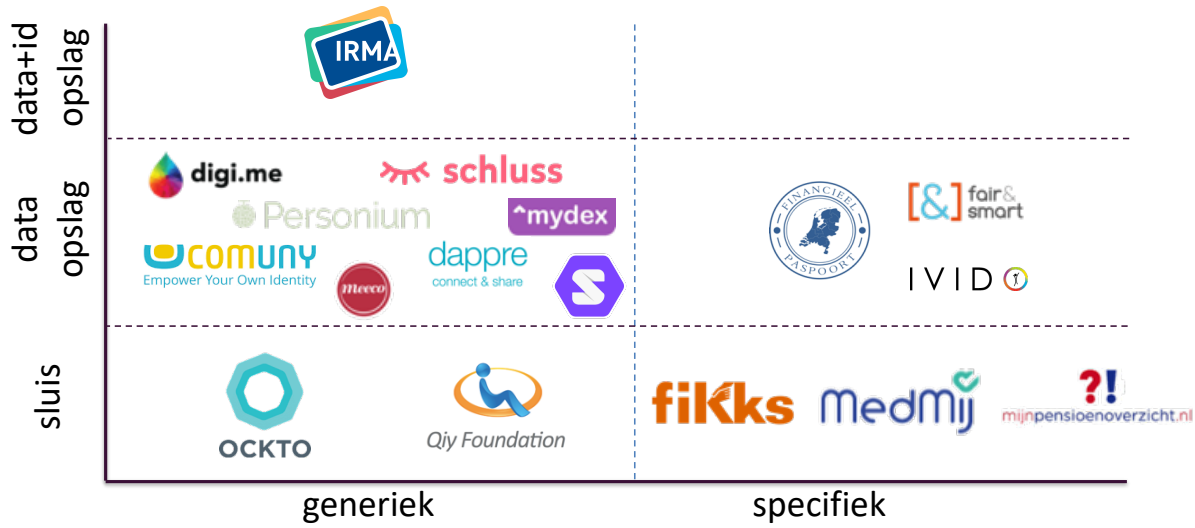
In dit rapport hebben we aantal stelsels besproken waar de focus ligt op authenticatie, zoals iDIN, SURFconext of Open ID Connect. De scheidslijn tussen authenticatiestelsel en een PDM-oplossing met operatorrol is een dunne: een authenticatiestelsel kun je zien een specifieke implementatie van een PDM-stelsel met de focus op geverifieerde identiteitsgegevens en niet zozeer informatie die aan mijn identiteit gekoppeld is (zoals een diploma of een medisch dossier). Voorbeeld: in iDIN worden geverifieerde gegevens over mij (naam, 18+, enzovoorts) gedeeld met de dienstverlener als je inlogt. De bank is de data-aanbieder en de dienstverlener de data-afnemer. Daartussen zit typisch een DISP (digital identity service provider) die integratie verzorgt, consent vraagt en heel goed kan worden ingezet voor aggregatiedoeleinden over meerdere bronnen. Typisch de rol van de operator. Op een vergelijkbare manier werkt SURFconext: SURFconext vult identiteitsverklaringen van de universiteit (de identity provider) aan met extra gegevens over de persoon voor bijvoorbeeld autorisatiedoeleinden (lidmaatschap van een onderzoeksgroep bijvoorbeeld) uit een andere op de hub aangesloten bron (SURFconext Teams). Vanuit de kennis is die in dit diensten is ontwikkeld is prima lering te trekken voor de opkomende PDM-oplossingen als IRMA en Ockto en die de gebruiker meer controle geven over het delen van gegevens.

Stelsels als iDIN, SURFconext en eHerkenning werken op basis van doorgeven van data, de data blijft bij de bron en staat niet bij de operator. Dit in tegenstelling tot bijvoorbeeld IRMA of Itsme en de mogelijk toekomstige DigiD app die straks ook BRP-gegevens in zich heeft.

Toepassingsgebied – generiek of specifiek

Een laatste onderscheidend element is het toepassingsgebied. We zien zowel smalle operators als generieke operators ontstaan. Veel van de early movers waren generiek, zoals Dappre van Qiy en MyDex. De laatste jaren komen daar specifiekere operators bij, gericht op het overheidsdomein, de zorg of financiële sector. Tegelijk komen er ook nog steeds generieke initiatieven bij, zoals Schluss, Solid en Sovrin. De diversiteit groeit. Het lijkt erop dat in het huidige tijdsgewricht de domeinspecifieke oplossingen relatief het snelst opgepakt worden. Deze spreken immers een directe behoefte aan en niet een latente behoefte van “regie voeren over je data”. Tegelijk zorgen de AVG en diverse dataschandalen ervoor dat de latente regiebehoefte mogelijk ook actueel wordt, maar we zien dit nog niet sterk naar voren komen in het gebruik. In het algemeen zijn gebruikscijfers nog maar heel beperkt beschikbaar en is gebruik dus moeilijk te duiden. We kunnen wel zeggen dat er nog geen heldere ‘winnaar’ is en ontwikkeling van PDM nog steeds evolutionair verloopt. Ondanks de schandalen en AVG nog steeds geen revolutie, wel groei en meer bewustzijn, tot kamervragen aan toe.

De dimensies generiek/specifiek en opslag lijken samen een aardige omspanning te geven van het veld, met een verdeling over alle vlakken.



Figuur 30. Operators en afsprakenstelsels geordend.

De meeste operators slaan persoonlijke data zelf op, zowel bij generieke als specifieke oplossingen. IRMA maakt zelfs hergebruik van de identiteit mogelijk en functioneert ook als inlogmiddel daarmee. Dit zou ook in specifieke contexten toegepast kunnen worden, bijvoorbeeld door IRMA te verbijzonderen naar het domein ("IRMA" voor zorg, "IRMA" voor gemeenten) om zo ook sneller vertrouwen te realiseren in dat gebied. Mogelijk zijn er bij de PGOs al oplossingen die iets vergelijkbaars doen, ons overzicht is daar niet compleet.

5.2 SUCCESFACTOREN OPNIEUW BEKEKEN

In een analyse t.b.v. ICTU over PDM initiatieven[82] kwamen we tot de volgende 6 succesfactoren voor PDM oplossingen:

1. Er is geen "first-mover advantage";
2. Zorg voor een sluitend bedrijfsmodel;
3. Vertrouwen vereist transparantie;
4. Begin smal en begin vanuit noodzaak;
5. Overheid moet vertrouwen realiseren;
6. Digitale identiteit essentiële component.

In de zorg zien we dat het relatieve succes van MedMij op een aantal vlakken hier mee te verklaren is: het voorafgaande EPD mislukte, de overheid zit nadrukkelijk aan tafel en faciliteert het business model, in de zorg kan in elk geval DigiD worden gebruikt, al zijn er op substantieel niveau nog tekortkomingen, en de noodzaak is duidelijk. Ook zien we dat veel van eerste initiatieven, zoals Qiy/Dappre en MyDex zichzelf opnieuw hebben uitgevonden of moeten gaan uitvinden. Qiy speelt nu een rol onder het Financieel Paspoort en fiKks.

[82] ICTU, Initiatieven en Stelsels Personal Data Management. Versie 1.4, 10/11/17. Beschikbaar via https://rog.pleio.nl/file/download/57899047/Initiatieven%20en%20stelsels%20PDM_Juli2017.pdf

Figuur 31. Succesfactoren voor operators (ICTU, 2017)

Ook de rol van de overheid komt vaak terug. Adoptie van IRMA vindt tot nu toe veelal plaats in een overheidscontext (gemeenten), waardoor vertrouwen ontstaat. IRMA is ook sterk in transparantie en bouwt op de digitale identiteit die gebruikt wordt bij de bron. En ook IRMA heeft zichzelf opnieuw uitgevonden als app na de eerste versie met een kaart gebonden oplossing. Onduidelijk is nog of het bedrijfsmodel van IRMA zich duurzaam zal ontwikkelen. Ook zien we vaak een stichting als basis voor de governance: de Stichting Privacy by Design voor IRMA, stichting Financieel paspoort, de Qiy foundation of de Community Interest Company achter Mydex. Een dergelijke vorm benadrukt dat er geen winstoogmerk achter de dienst zit als zodanig.

Een belangrijke meerwaarde van IRMA is het ontsluiten van de BRP-gegevens. Deze gegevens zijn voor heel veel afnemers interessant/relevant om te ontvangen. Dit toont aan dat een andere factor voor een succesvolle PDM oplossing de capaciteit voor het ontsluiten van (relevante) aanbieders van gegevens betreft.

Het pensioenregister en MijnOverheid leunen ook sterk op overheidsvertrouwen: pensioenregister komt voor uit wettelijke taak en kan DigiD gebruiken. Het vult een specifiek doel in: overzicht in de toekomstige situatie. MijnOverheid ontsluit een flink aantal overheidsbronnen. Andere oplossingen, zoals het Financieel Paspoort, bouwen weer op deze basis.

Een aantal operators werkt vanuit een heldere noodzaak: schuldhulpverlening. fiKks en Financieel paspoort. Ze bouwen op Qiy als afsprakenstelsel en worden gesteund door overheden. Het bijbehorende business model is echter nog net uitgekristalliseerd: wie gaat uiteindelijk betalen voor de kosten die worden gemaakt?

Ockto scoort ook op een aantal punten goed: het vult een noodzaak in (snelle en correcte overdracht van gegevens bij processen als een hypotheekaanvraag) en heeft een duidelijk business model dat gedreven wordt door de data-afnemer. Echter, de overheid werkt niet actief mee (ze staan scraping toe voor dataverzameling, maar faciliteren het niet via nette interfaces), waardoor het vertrouwen vanuit de consument soms wordt geschaad. Ockto probeert te profiteren van het vertrouwen dat banken genieten door hier dicht op te zitten.

Buitenlandse oplossingen als MyFairData bouwen voort op de basis die de AVG legt rond data-portabiliteit en kiezen daarbij een business model dat niet de consument maar de data-afnemer laat betalen. Dit lijkt ook kansrijk.

6 Vervolgstappen

Het is belangrijk het overzicht dat nu begint te ontstaan actueel te houden. Zo blijven we in staat de markt te duiden en goede beslissingen over de inzet van PDM voor data-afnemers en data-leveranciers te nemen. Dit overzicht zal worden gepubliceerd op www.digitalwe.nl en daar ook worden bijgehouden.

Vanuit het overzicht en inzicht dat nu ontstaan is willen we een aantal vervolgstappen zetten:

4. Uitwerken van een checklist / infographic t.b.v. praktische keuzes: waar moet een organisatie op letten indien ze aan de slag gaat met PDM? Dit operationaliseert een aantal van de aspecten uit de analyse voor data-afnemers en -leveranciers.
5. Internationale consensusvorming op principes voor PDM: op basis van dit onderzoek wordt in MyData verder gewerkt aan een beschrijving van de MyData operator. Daarbij gaat het niet alleen om een functioneel kader, maar ook om een normatief kader: wanneer voldoet een operator aan de MyData principes?
6. Nationale harmonisatie: we zoeken aansluiting bij initiatieven als het programma Regie op Gegevens om tot een geharmoniseerde terminologie te komen en zo begripsverwarring in het veld zo veel mogelijk te voorkomen.
7. Aanvulling met initiatieven die gerelateerd zijn aan de invulling van PSD2. Dit is nu nog bewust achterwege gelaten. Er komen echter de nodige initiatieven rond open banking die ook in Nederland hun impact hebben. Een voorbeeld is Yolt van ING dat al in de UK is uitgerold, maar ook in Nederland zijn er al enkele tientallen PSD2 vergunningen uitgegeven.[83]

Ook op technologisch vlak is er een aantal zaken om rekening mee te houden. Onder meer de ontwikkeling van Self Sovereign Identities is eentje die veel aandacht krijgt, met name in de blockchainhoek. Feitelijk kan dit worden gezien als een nieuwe generatie identiteitstechnologieën die een aantal manco's van user centric identiteiten en gefedereerde identiteiten wegneemt. Ook IRMA zou je kunnen zien als een Self Sovereign Identity.[84]

Tenslotte is het belangrijk juist naar het speelveld te kijken: dynamiek daar wordt deels bepaald door de markt, deels door technologie en deels door de politiek. Een ontwikkeling als MedMij van de Patiënten Federatie heeft een enorme impuls gekregen van het Ministerie van VWS. Dan nog is niet gezegd dat de markt het omarmt.[85] Ook de implementatie van de Brief aan de Tweede Kamer over Regie op Gegevens kan nieuwe impulsen geven, of juist tegenwerken. Zo blokkeerde de Tweede Kamer de medewerking van DUO aan het recht op inzage van oud-studenten in hun eigen studieschuld via een downloadknop, waarmee in feite zelfs de AVG onder druk komt te staan. Juist het politieke aspect is een moeilijk te voorspellen dimensie. Volgen, voorlichten en informeren is daar minimaal noodzakelijk.

[83] https://fd.nl/beurs/1324410/bespaarapp-dyme-krijgt-toestemming-om-bankdata-consumenten-in-te-zien

[84] zie het overzicht van SSI ontwikkeling zoals gepubliceerd binnen Digital We, december 2019.

[85] Zie, bijvoorbeeld, het blog "19 PGO's waar je niets mee kunt van Jan Jacobs. https://www.smarthealth.nl/2019/11/28/blog-negentien-pgos-waar-je-niets-mee-kunt/

7 Bijlage. Onderzoeksmodel Operators

7.1 ONDERZOEKSMODEL OPERATORS

Bij het onderzoek zijn leveranciers benaderd met de volgende vragenlijst. Na beantwoording van de vragen heeft nog een interview plaatsgevonden (telefonisch of persoonlijk). De volgende inleiding is bij de vragenlijst meegestuurd.

> Geachte …,
>
> Graag willen we uw medewerking vragen bij een onderzoek naar persoonlijke datadiensten in Nederland. Middels dit onderzoek willen we een overzicht realiseren van alle oplossingen in Nederland, de fase van ontwikkeling waarin ze zijn en hoe ze van elkaar verschillen. Ook uw oplossing, {XYZ}, willen we graag in dit onderzoek betrekken.
>
> Het onderzoek vindt plaats in het kader van Digital We, een onderzoeksprogramma waarin een aantal gemeenten, overheden en private partijen samenwerken (zie www.digitalwe.nl voor meer informatie). De resultaten zullen vrij ter beschikking komen. Uiteraard zal dit alleen plaatsvinden na uw goedkeuring van de manier waarop we {XYZ} hebben beschreven. De bedoeling is nadrukkelijk niet te komen tot een 'consumentenbond' oordeel van diensten. Het onderzoek is inventariserend van aard.
>
> We willen u verzoeken de vragenlijst in te vullen en aan ons terug te sturen. Dit duurt ongeveer 30 minuten. Op basis van de antwoorden willen we graag contact met u opnemen om interpretatiefouten te voorkomen en de weergave van de uitkomsten af te stemmen. Eind oktober ronden we de inventarisatie af.
>
> Voor meer informatie over de achtergronden kunt u contact opnemen met Marlies Rikken van InnoValor (tel. 06-10418028). We hopen van harte op uw medewerking. Het concept van regie op gegevens, in al haar verschijningsvormen, is gebaat bij een helder overzicht, om zo een doorbraak dichterbij te brengen voor personen, burgers, inwoners, zorggebruikers, studenten en noem maar op.
>
> Met vriendelijke groet,
> Wil Janssen
> *Managing Partner InnoValor*
> *Projectleider PDM in Digital We*

Algemene kenmerken

- **Doelstelling**. Wat is de algemene positionering / doelstelling van de service?
- **Origine**. Standplaats van het initiatief (land) en wanneer is het ontstaan
- **Volwassenheid**. In welke fase van ontwikkeling is dienst?
    - Conceptfase
    - Pilotfase (in ontwikkeling / wordt nog getest in gebruikerstest)
    - Operationeel (bruikbaar voor personen in tenminste één live proces)
- **Dienst.** Welke dienst wordt geleverd aan een gebruiker?
- **Marktfocus**. Op welke sector en geografische regio richt de dienst zich voornamelijk?
- **Bronnen**: wat zijn typische data-aanbieders waarvan de oplossing gebruik maakt?
- **Afnemers**: wat zijn typische data-afnemers voor de dienst?

Governance (besturing en beheer)

- **Afsprakenstelsel**. Maakt de dienst expliciet gebruik van een afsprakenstelsel (zo ja, welk)?

Zo niet:

- **Toetreding**: welke regels zijn er voor toetreding van partijen (data-afnemers, gebruikers, data-bronnen) en het verwijderen ervan?
- **Incidenten**: op welke wijze kunnen gebruikers incidenten melden en worden ze geïnformeerd over incidenten?
- **Ontwikkeling**: wie is verantwoordelijk voor doorontwikkeling en beheer van de diensten?
- **Communicatie**. Op welke wijze worden gebruikers geïnformeerd over de afspraken in de dienstverlening en de ontwikkeling daarvan?

Consent

- **Ophalen.** Kan een persoon consent geven voor het ophalen van gegevens bij een data aanbieder?
- **Uitwisselen.** Kan een persoon consent geven voor het uitwisselen van gegevens met een data afnemer?
- **Tijdsduur bepalen.** Kan een persoon bepalen voor welke tijdsduur de consent geldig is?
- **Specifieke gegevens**. Heeft de persoon keuze om een gedeelte van de set gegevens te delen met de afnemer?
- **Consent overzicht.** Kan de PDM service een overzicht gegeven van de toestemmingen die zijn gegeven?
- **Consent aanpassen**. Kan uitgegeven consent gewijzigd worden?
- **Consent intrekken**. Kan gegeven consent ingetrokken worden?

Opslag van gegevens

- **Opslag.** Worden persoonlijke gegevens opgeslagen?
- **Plaats van verwerking/opslag.** Waar worden gegevens verwerkt/opgeslagen?
    - Device van de gebruiker
    - Op server van de PDM service
    - Op zelf te kiezen cloudoplossing
    - Overig – graag specificeren
- **Duur van opslag.** Hoe lang worden gegevens bewaard?
    - Is dit alleen voor de uitwisseling of ook als “kluis”

Gegevensuitwisseling

- **Ophalen.** Hoe worden gegevens opgehaald bij databronnen (API, screen scraping, uploaden, blauwe knop, anders?)
- **Manier van uitwisseling.** Hoe worden gegevens uitgewisseld met data afnemers? (API, anders?)
- **Gegevens aanvullen.** Kan een persoon zelf data toevoegen, of wordt alleen gewerkt met data uit bronsystemen?

Data diensten

- **Waarmerking**. Zijn de gegevens gewaarmerkt door de bron, PDM Service of niet?
- **Analyse.** Worden er door de PDM Service analyses gedaan over de gegevens? (vb. geboortedatum omzetten naar leeftijd)
- **Aggregatie.** Worden gegevens geaggregeerd (bijv. van gezondheidsdata een BMI, of gecombineerd uit meerdere data aanbieders.
- **Revocatie.** Kunnen gegevens door de data-aanbieder ongeldig verklaard worden? (bijv. als een BIG registratie wordt ingetrokken, maar nog wel in de PDM Service staat?)

Authenticatie.

- **Inloggen bij de PDM service.** Hoe bepaalt de PDM service de identiteit van de gebruiker?
- **Gegevens ophalen.** Wordt er bij het ophalen van gegevens gebruik gemaakt van bestaande identificatiediensten zoals DigiD, EHerkenning, iDIN?
- **Autorisatie.** Hoe worden autorisaties beheerd?
- **Privacy.** Welke maatregelen, naast consent, zijn getroffen om de privacy van de gebruiker te borgen? (privacy-by-design aspecten)

Business model

- **Inkomsten**. Welke partijen/partners betalen in het eco-systeem (data-aanbieders, data-afnemers, persoon, beheerorganisatie, …)?
- **Vorm**. is dit een abonnement, pay-per-use, vaste bijdrage

- **Andere inkomstenbronnen**. Zoals verkoop van anonieme data, advertenties, upselling/cross-selling

Overig

- Zijn er nog zaken niet aan de orde gekomen die van belang zijn voor een goed begrip van de dienst?

8 Bijlage. Onderzoeksmodel Afsprakenstelsel

8.1 ONDERZOEKSMODEL AFSPRAKENSTELSEL

Brief een aanpak vergelijkbaar met diensten, mutatis mutandi. Zie vorig hoofdstuk.

Algemene kenmerken

- **Doelstelling**. Wat is de algemene positionering / doelstelling van het stelsel?
- **Origine**. Standplaats van het stelsel (land) en wanneer is het ontstaan
- **Beheerder**. Welke organisatie of consortium beheert het afsprakenstelsel?
- **Volwassenheid**. In welke fase van ontwikkeling is het stelsel?
    - Conceptfase
    - Pilotfase (in ontwikkeling / wordt nog getest in gebruikerstest)
    - Operationeel (in gebruik door verschillende dienstenaanbieders)
- **Dienstaanbieders.** Welke dienstaanbieders werken nu met het stelsel?
- **Marktfocus**. Op welke sector en geografische regio richt het stelsel zich voornamelijk?
- **Bronnen**: wat zijn typische data-aanbieders waarvan de oplossing gebruik maakt?
- **Afnemers**: wat zijn typische data-afnemers voor de dienst?

Governance (besturing en beheer)

- **Toetreding**: welke regels zijn er voor toetreding van partijen (data-afnemers, gebruikers, data-bronnen) en het verwijderen ervan?
- **Incidenten**: op welke wijze kunnen gebruikers incidenten melden en worden ze geïnformeerd over incidenten?
- **Ontwikkeling**: wie is verantwoordelijk voor doorontwikkeling en beheer van de diensten?
- **Communicatie**. Op welke wijze worden gebruikers geïnformeerd over de afspraken in de dienstverlening en de ontwikkeling daarvan?

Functionaliteit

Welke functionele aspecten van de dienstverlening worden voorgeschreven door het stelsel?

Consent: Ophalen, Uitwisselen, Consent overzicht, Consent aanpassen

Opslag van gegevens: duur, locatie

Gegevensuitwisseling: welk model? Direct of via operator?

Data diensten: Waarmerken, analyse etc.

Authenticatie en autorisatie: wat is hierbij voorgeschreven?

Gebruikersinteractie: hoe navigatie en vormgeving van oplossingen moet zijn?

Business model

Schrijft het afsprakenstelsel een specifiek verdienmodel voor of legt het restricties op aan de verdienmodellen van deelnemers?

Overig

- Zijn er nog zaken niet aan de orde gekomen die van belang zijn voor een goed begrip van het afsprakenstelsel?

9 Bijlage: Engelse variant onderzoek

Dear …,

We want to ask for your participation in our research into personal data services. Through this study we hope to offer insight into the international landscape of personal data services, the phase of development they are in and how they differentiate from eachother. We would like to include your solution {XYZ} in this study.

The study is part of our reseach programme Digital We, in which several municipalities, governmental organizations and private parties collaborate (see https://innovalor.nl/en/digital-trust/digital-we for more information). The results will become freely available and will only be published after your consent to the way your service is described. The intention is not to present the findings as 'consumer guide': the study is explorative nature.

We kindly request you to complete the survey and send dit back to us. This takes about 30 minutes. Based on your answers we would like to contact you in order to prevent any mistakes and to confirm our findings. At the end of October the survey will be wrapped up.

For more information about the survey and its background, you can contact Marlies Rikken (06-10418028). We hope for your participation in this research. Data empowerment, in all its forms, will benefit from better understanding of the field in order to bring a breakthrough closer. For people, citizens, patients, students and all others.

Kind regards,
Wil Janssen
Managing Partner InnoValor
Projectleider PDM in Digital We

9.1 PDM SERVICES

General aspects

- **Goal**. What is the general positioning / goal of the service?
- **Origin**. Where is the service headquartered (country) and when was it founded.
- **Maturity**. What phase of development is the PDM service in?
    - Concept phase
    - Pilot phase (in development / being tested in usertests.)
    - Operational (useable for people in at least one live process.)
- **Service.** What service does the PDM service deliver to a user?
- **Market focus**. Which sector and geographic region are the service's main focus?
- **Data sources**: what are typical data sources the PDM service uses?
- **Data using services/data consumers**: What are typical data using services/data consumers to the PDM service?

Governance

- **Trust framework**. Does the service explicitly make use of a trust framework? (If yes, which?)

If not:

- **Admittance**: what rules exist for admittance of new parties? (data consumers, users, data sources) and for removing them?
- **Incidents**: In what way can users report incidents and how are they notified if any incidents happen?

- **Development**: Who is responsible for continued development and administration of the service?
- **Communication**. In what way are users informed of (developments in) the service agreement?

Consent

- **Retrieving.** Can a person give consent fort he retrieval of data at a data source?
- **Exchange.** Can a person give consent for data exchange with a data using service?
- **Determining timespan.** Can a person determine for which timespan the consent is valid?
- **Specific data**. Does the person have a choice to select specific parts of the dataset to share with data using services?
- **Consent overview.** Can the PDM service show an overview of all the instances that consent has been given out?
- **Consent adjustment**. Can given consent be adjusted?
- **Consent revocation**. Can given consent be revoked?

Data storage

- **Storage.** Is personal data being stored?
- **Place of processing/storage of data.** Where are the data processed/stored?
    - Device of the user
    - On a server of the PDM service
    - On a self-chosen cloud solution
    - Other – please specify
- **Duration of storage.** How long is the data stored?
    - Is data stored only for exchange or as 'vault'?

Data exchange

- **Collection.** How are data collected at data sources? (API, screen scraping, uploading, other?)
- **Method of exchange.** How is data exchanged with data using services? (API, other?)
- **Self-asserted data.** Can a person add data themselves? Or does the service only use verified sources?

Data services

- **Certification**. Are data certified by the source, PDM service or not at all?
- **Analysis.** Are there any analysis made on the data by the PDM service? (such as converting a birth date into age).
- **Aggregation.** Are data aggregated (such as health data to a BMI, or combined from multiple data sources.)
- **Revocation.** Can data be revoked by the data source? (Such as a doctors permit that is retracted, but is still noted in the PDM service).

Authentication.

- **Logging into the PDM service.** How does the PDM service determine the identity of the user?
- **Data collection.** Are existing methods for identification used when collecting data from a data source? Which?
- **Autorisation.** How are autorisations administrated?
- **Privacy.** Which measures, outside of consent, are taken to guarantee the users privacy? (privacy-by-design aspects)

Business model

- **Income**. Which parties/partners pay in the eco-system? (data sources, data using services, person, adminstrative organisation, other?)
- **Model**. What is the main revenue model? (Subscription, pay-per-use, fixed price, other?)
- **Other income.** Is there any income from selling anonymous data, adverts or upselling/cross-selling?

Other

- Are there any points that haven't been mentioned, that are important for a good understanding of the PDM service? Please elaborate.

9.2 AFSPRAKENSTELSELS

Algemene kenmerken

- **Goal**. What is the general positioning / goal of the trust framework?
- **Origin**. Where is the trust framework headquartered (country) and when was it founded.
- **Administrator**. Who/which party is the administrator of the trust framework?
- **Maturity**. What phase of development is the PDM service in?
    - Concept phase
    - Pilot phase (in development / being tested in usertests.)
    - Operational (useable for people in at least one live process.)
- **Services.** What services currently work with the trust framework?
- **Market focus**. Which sector and geographic region are the service's main focus?
- **Data sources**: what are typical data sources that are used within the trust framework?
- **Data using services/data consumers**: What are typical data using services/data consumers in the trust framework?

Governance

- **Admittance**: what rules exist for admittance of new parties? (data consumers, users, data sources) and for removing them?
- **Incidents**: In what way can users report incidents and how are they notified if any incidents happen?
- **Development**: Who is responsible for continued development and administration of the service?
- **Communication**. In what way are users informed of (developments in) the service agreement?

Functionaliy

What fuctional aspects of the PDM services are prescribed/regulated by the trust framework?

Consent: collecting, exchanging, consent overview, consent adjustment

Data storage: timespan, location

Data exchange: Is data exchanged directly from the data source to the data using service or is it exchanged via an operator?

Data services: certification, analysis, aggregation, revocation

Authentication en autorisation: what is prescribed in terms of authentication and autorisation?

User interaction: are there requirements on the way the user navigates the service and how the service is designed?

Business model

Does the trust framework prescribe a specific revenue model or does it put any limitations on the revenue model of participants?

Other

- Are there any points that haven't been mentioned, that are important for a good understanding of the trust framework? Please elaborate.