Eigen Data Delen

Personal Data Stores – concept, techniek en gebruik

REDACTIE Wil Janssen

PROJECT REFERENTIE Digital We/PDS/1

TOEGANGSRECHTEN Publiek

VERSIE 1.3, 23 november 2015

Definitief

Inhoud

Managementsamenvatting

Bij een personal data store gaat het om een dienst die een individu in staat stelt om zijn persoonlijke informatie duurzaam te beheren en te onderhouden. Ook laat een personal data store het toe om deze informatie, wanneer de gebruiker dit in zijn belang acht, te delen met anderen. Elementen daarvan vinden we in de Mijn-omgevingen van verzekeraars en gemeenten, in MijnOverheid, maar ook in diensten als LinkedIn of Dropbox. Ook in het buitenland zijn er varianten van het concept, variërende van puur privaat, zoals DataCoup, waar je je gegevens kunt verhandelen, publiek-private samenwerkingen, zoals MyDex in het Verenigd Koninkrijk. Een personal data store is niet een kluisje of centrale opslag van gegevens. Het is een dienst; je zou dus ook kunnen spreken van een personal data service, of persoonlijk data management.

De economische waarde van persoonlijke waarde in enorm. Alleen al in Engeland wordt deze geschat op 11,5 miljard pond per jaar. Waarde wordt gerealiseerd door lagere fouten, persoonlijkere dienstverlening en hogere conversie. Toch blijkt het moeilijk om personal data stores van de grond te krijgen. Het concept is technologisch complex en het business model is niet eenvoudig te realiseren. Ook is de mate van standaardisatie nog beperkt. In Nederland is Qiy bezig met de ontwikkeling van een trust framework voor personal data stores. Internationaal zijn standaarden als OpenPDS en UMA interessant.

Nederlanders staan op zich positief tegenover het concept: een ruime meerderheid van 57% zou een dergelijke dienst waarderen. Overheidspartijen worden daarbij het meest vertrouwd om de gegevens te gebruiken. Van doorslaggevend belang is dat mensen overzicht van gegevens krijgen en controle over wie de gegevens gebruikt. Dergelijke functionaliteit zien we nog niet terug in bestaande initiatieven.

Wetgeving lijkt niet een probleem in de introductie van personal data stores, maar het wettelijk kader is wel belangrijk. De wet bescherming persoonsgegevens is een belangrijke basis; de Europese privacyrichtlijn zal daar in de loop van 2016/2017 een belangrijke aanvulling op zijn, die de rechtspositie van consumenten versterkt. Daarnaast zal de Payment Service Directive 2 voor banken er toe leiden dat ook bankgegevens in personal data stores kunnen worden geïntegreerd (verwachting: 2017).

De kansen en ontwikkelingen verschillen per sector. In de zorg is het EPD niet van de grond gekomen, maar speelt het landelijk schakelpunt wel een rol om informatie uit te wisselen. We zien wel een grote behoefte aan effectief delen van informatie vanuit de patiënt, als staat het gebruik van persoonlijke gezondheidsdossiers nog in de kinderschoenen. In de verzekeringsbranche zijn er verschillende private initiatieven. Branchebreed wordt nu gewerkt aan een poliskluis, vergelijkbaar met MijnPensioenOverzicht. Onder meer omdat voor verzekeringen echter geen DigiD gebruikt mag worden, in tegenstelling tot pensioen, is de poliskluis complexer om te realiseren en te voorzien van de juiste functionaliteit. In de overheid is MijnOverheid ooit opgezet als infrastructuur voor effectief delen van informatie. Het tempo waarmee MijnOverheid zich ontwikkelt, is echter beperkt: nog veel organisaties zijn niet aangesloten, en beheer van informatie is beperkt mogelijk. De focus ligt daar nu op digital berichtenverkeer.

Toch kan een personal data store een belangrijk concurrentievoordeel opleveren voor organisaties. Het kan de vertrouwensband met de consument versterken, betere dienstverlening opleveren en bijdragen aan de betaalbaarheid van de zorg door betere informatie. De introductie van een personal data store luistert echter nauw: mensen zijn nog niet bekend met het concept en veel van de huidige ontwikkelingen zoals in MijnOverheid en in de poliskluis leiden af van de echte toegevoegde waarde. Een initiërende of controlerende rol van de overheid ligt voor de hand, gegeven het vertrouwen dat de overheid op dit vlak geniet. Kies daarbij voor een doelgroep die open staat voor deze ontwikkeling, het nut ziet of de noodzaak heeft en lever functionaliteit die aansluit bij de wensen. Wacht daarbij niet tot standaarden zijn uitgekristalliseerd, dat kan nog lang duren, maar start met kleine initiatieven op specifieke doelgroepen om te leren hoe het werkt.

Auteurs zijn Arnout van Velzen, Adina Aldea, Marlies Rikken, Marc Lankhorst, Melissa Roelfsema, Ruud Kosman, Timothy Sealy en Wil Janssen. We willen graag Wouter Bronsgeest, Maarten Wegdam en Laura Claas bedanken voor uitgebreide commentaar op het stuk en hun suggesties voor verbeteringen.

Deze 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 en BiZZdesign. Het consortium bestaat uit de Manifestgroep, VGZ, Belastingdienst, Rijkswaterstaat, Gemeente Amsterdam, SIVI, BiZZdesign en InnoValor.

1 Inleiding

De hoeveelheid gegevens van en over ons is enorm. Het voelt alsof er overal en nergens data staat. We worden op honderden plaatsen geregistreerd, bij de overheid, winkels, bedrijven, verenigingen, noem maar op. Dat kunnen officiële registraties zijn, zoals de basisregistraties met een wettelijke basis. Maar ook informatie die over ons geregistreerd wordt vanuit ons gedrag (via een smartphone), via verkeer (camera's, verkeerslussen), activiteiten op het internet (surfgedrag), gezondheid (zorggegevens), etc. De wet bepaalt dat die gegevens van ons zijn, dat we inzage- en correctierecht hebben, enzovoorts. Het uitoefenen van dat recht is op dit moment echter zo simpel nog niet. De nieuwe Europese privacywetgeving gaat nog verder en geeft zelfs het recht je gegevens te verplaatsen van een dienstverlener naar een andere. Wel zo handig als je van de ene gezondheidsapp naar de andere wilt gaan. Eigenlijk zouden je gegevens onder je eigen beheer moeten staan. Het veld van persoonlijke gegevens en beheer daarvan is nadrukkelijk een veld waar doorbraken worden verwacht, met name in de vorm van Personal Data Stores.

Rond de eeuwwisseling is er een economie ontstaan rond digitale informatie over personen. Informatie wordt meer dan eens *de nieuwe olie* genoemd. Persoonsgegevens zijn geld waard. Engels onderzoek uit 2014 (CTRL Shift 2014) schat de waarde van data rond een persoon op drie tot vijf pond (€5,50) en daarmee de markt voor persoonlijke informatiemanagement systemen op 11,5 miljard pond in het Verenigd Koninkrijk alleen al (CTRL-Shift, 2014). Vermijdbare kosten als gevolg van foutief medicijngebruik, vaak te wijten aan gebrekkige informatie-uitwisseling, werden in 2006 geschat op ruim 40 miljoen euro per jaar, alleen al in Nederland (NPCF). Dit nog los van de kwaliteit van dienstverlening die op basis van betere informatie enorm kan groeien, waarmee de concurrentiepositie van bedrijven kan worden verstevigd. Kansen te over dus, zowel vanuit kostenperspectief, vanuit marktperspectief en vanuit gebruikersgemak.

Ontwikkelingen als de cloud en big data, alsmede data-giganten als Google, betekenen echter ook meer risico's rondom de privacy van gebruikers. Persoonlijke data staat steeds vaker gecentraliseerd op servers van online dienstaanbieders als Google in plaats van op de systemen van gebruikers. Deze trend geeft de controle en verantwoordelijkheid uit handen van de gebruiker, wat resulteert in een verlies van autonomie en mobiliteit van data. Regelgeving en technologie voor databescherming beschermt niet altijd de privacy of is niet ontworpen voor de genetwerkte wereld. De asymmetrie tussen datagiganten en de gebruiker leidt tot risico's in offline wereld. De gebruiker verliest hierdoor steeds meer vertrouwen en wil weer inzicht krijgen in de eigen data (InnoValor, 2015; Newcom 2015). Er vindt momenteel een verschuiving van aandacht plaats van het beheer van data naar het beheer van het *gebruik* van data. Hierin geeft het individu, de burger of consument, bewust toestemming voor het gebruik van persoonlijke data, afhankelijk van de context. Persoonlijke data verwijst naar alle data die door of over de gebruiker wordt aangemaakt en komt in vele vormen. Anders gezegd, het is informatie waar een individu een belang in, of controle over, heeft om vorm te geven aan zijn of haar omgeving en leven.

We definiëren een Personal Data Store (PDS) als volgt:

> *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.*

Met andere woorden, een PDS stelt de gebruiker in staat in te zien welke persoonlijke data waar staat en door wie wordt gebruikt, en toestemming te geven of weerhouden voor toegang tot deze data. Hierin nemen de identiteit en voorkeuren van de gebruiker een belangrijke rol in, en zijn gemak en overtuigen van de gebruiker doorslaggevend. PDS's verschillen van bijvoorbeeld personal cloud- of data vault-achtige oplossingen (die puur en alleen data opslaan en delen) door inzicht te geven in elders opgeslagen data en voorkeuren voor toegang tot die data in te stellen. 'Store' verwijst hier zowel naar opslag (als in 'storage') van data, als naar winkel (als in 'general store'). De voordelen voor de gebruiker zijn behalve privacy en autonomie, ook efficiëntie en mogelijk zelfs commercie (verdienen aan je eigen data). Denk aan waarde die je creëert met *targeted advertising*.

"People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time" (Mark Zuckerberg, oprichter Facebook, 2010)

Met het delen van persoonlijke data ontstaat niet alleen waarde, het brengt nadrukkelijk ook risico's met zich mee. Het concept staat op gespannen voet met privacy van de gebruiker. Gaat het delen op een zorgvuldige manier? Is de PDS provider voldoende betrouwbaar? Is de wijze van authenticatie van voldoende kwaliteit? En zijn we het eens met de doelen van de PDS? Want niet iedereen denkt hetzelfde over wanneer en met wie gegevens zouden moeten worden uitgewisseld. Een aardig voorbeeld daarvan is de controverse rond het Landelijk Schakelpunt in de zorg (LSP). Via het LSP kunnen zorgpartijen informatie uitwisselen over een burger, bijvoorbeeld als die zich meldt bij een spoedeisende hulp of weekenddienst en dus niet direct in contact staat met de huisarts. Burgers kunnen via het LSP zien wie informatie over hem of haar heeft uitgewisseld (niet de inhoud van de informatie). Een aantal huisartsen in de regio Amsterdam is in de zomer van 2015 begonnen om een regionaal alternatief voor het LSP te maken dat meer gericht is op de huisarts en van begin tot einde versleuteld is. Daarmee is voor de burger niet meer in te zien wie informatie heeft uitgewisseld, maar is wel een "end-to-end" beveiliging mogelijk. Maar is dat dan beter? En waarom staat de huisarts centraal en niet de burger? En is regionaal voldoende? Vragen te over, waarvan het antwoord niet bij voorbaat helder is.


Nieuws Cultuur & Leven deVolkskrant

Wetenschap

© ANP

Artsen experimenteren met 'veiliger' patiëntendossier

Twintig huisartsen in Amsterdam gaan experimenteren met een alternatief systeem voor het uitwisselen van medische gegevens. Deze methode is volgens

Figuur 1: Volkskrant, 10 september 2015

In dit document doen we een poging om het concept "Personal Data Store" in de vingers te krijgen: wat is het op dit moment, hoe zou het zich kunnen ontwikkelen, wat is de stand van de technologie en welke impact kan het hebben? Doelgroep van het stuk zijn mensen die zich bezighouden met het ontwikkelen of implementeren van een organisatiestrategie rond persoonlijke gegevens. Dit kan als beleidsadvies, als concept- of dienstenontwikkeling, of in het ontwikkelen van een meerjarig ontwikkelplan. Om te beginnen schetsen we in hoofdstuk 2 een drietal gebruiksscenario's voor PDS's: puur commercieel gebruik, maximale inzet in de publieke sector en een gemengd model. Die mogelijkheden zetten we af tegen de huidige voorbeelden van gebruik (hoofdstuk 4). Per domein kan de ontwikkeling van PDS's sterk verschillen. In hoofdstuk 5 gaan we in op persoonlijke gezondheidsdossiers, polismappen en –kluizen en de ontwikkeling van MijnOverheid en bekijken we de mogelijke impact in die sectoren.

Tot slot kijken we naar de technische haalbaarheid van het concept (in termen van standaarden en patronen, hoofdstuk 6) en de wenselijkheid vanuit de gebruiker (hoofdstuk 7). Dit alles bij elkaar levert de ingrediënten van een roadmap voor Personal Data Stores in hoofdstuk 8.

2 Gebruik en potentieel PDS

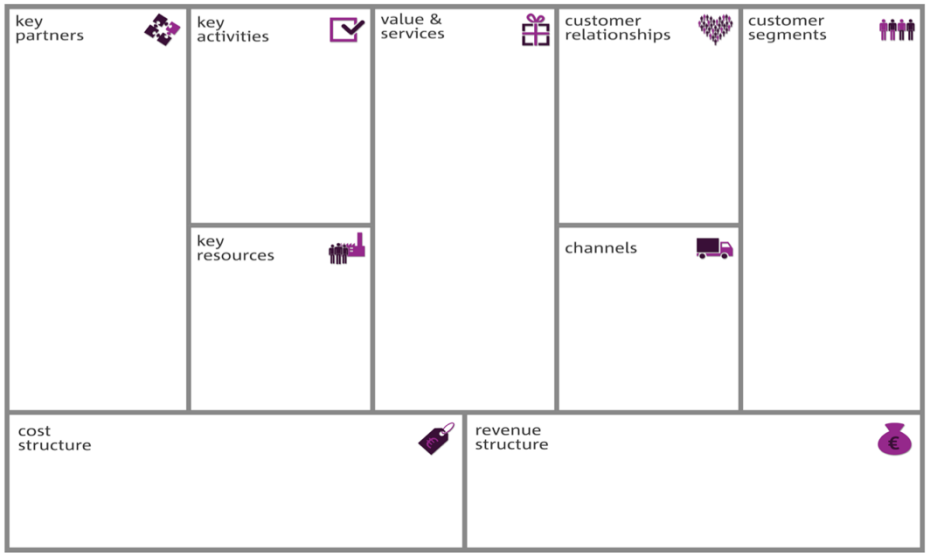
Om het concept te verhelderen en richting te geven aan de discussie, hebben we een drietal gebruiksscenario's ontwikkeld. Een daarvan richt zich op toepassingen in de private sfeer, met een commercieel doel, namelijk het scenario *Eigen Waarde*. Een puur publiek scenario richt zich sterk op het delen van de informatie en nooit meer dubbel vragen, *De Briljante Overheid*. Het laatste scenario combineert publieke en private elementen, gericht op optimale (in kwaliteit en prijs) dienstverlening, *Top Prestatie.* We beschrijven ze hieronder.

Elk scenario bestaat uit kort verhaal/scenario, een schets van het waardenetwerk, en het bedrijfsmodel rond de PDS provider. Een waardenetwerk laat zien hoe waarden of middelen stromen tussen partijen. Het geeft de interactie en wisselwerking weer tussen verschillende partijen rondom een bepaald product of een bepaalde service. Het is een manier om in kaart te brengen wat er nodig is om een bepaald product of dienst tot stand te brengen.

Dit waardenetwerk combineren we met de beschrijving van het bedrijfsmodel van de Personal Data Store in deze context, aan de hand van het business model canvas van Osterwalder.

Het Business Model Canvas (Osterwalder & Pigneur, 2009) is een instrument dat gebruikt wordt om business modellen te beschrijven, te visualiseren, te onderzoeken en te veranderen. De definitie van een business model is: *een business model is een blauwdruk voor de manier waarop een netwerk van bedrijven waarde wil creëren voor de klant en voor zichzelf*.

Deze generieke definitie is van toepassing op ieder type organisatie die diensten aan haar omgeving (klanten) levert. Dit kan in de vorm van een fysiek product (van een blikje cola tot aan een I-pad), of een dienst (het garanderen van veiligheid op straat, het leveren van consultancy of het faciliteren van het aangeven van belastingaangifte voor de burger). Iedere organisatie heeft dus een business model dat in kaart kan worden gebracht aan de hand van het Business Model Canvas. Een business model kan op verschillende niveaus worden beschreven. Het meest voor de hand liggende niveau waarop men business modellen beschreven ziet, is op het niveau van een gehele organisatie. Een organisatie levert een waarde door middel van een bepaald product of dienst aan haar externe klant.



Figuur 2: Het business model canvas

Het canvas bestaat uit 9 bouwstenen. Centraal staat de waarde propositie naar de klant. De rechterkant geeft aan hoe die waarde of diensten naar verschillende klantsegmenten wordt aangeboden: via welke kanalen, in welke relatie met de klant? De linkerkant geeft aan hoe die waarde wordt gerealiseerd: met welke kernactiviteiten,

welke resources (mensen en systemen) en met welke partners? Daarnaast kun je aangeven welke kosten en inkomsten aan de producerende en verkopende kant een rol spelen.

We beschrijven de 9 bouwblokken kort in de volgorde waarop het canvas het makkelijkst kan worden ingevuld:

- **Value & services - Waardepropositie en dienstverlening**: dit is het centrale element in het canvas. Welke toegevoegde waarde levert de dienst of het product? Het is goed hier niet alleen de toegevoegde waarde weer te geven, maar ook aan te geven welke producten of diensten daarbij horen. Neem een verzekeraar: de waardepropositie is dat een bepaald risico helder is afgedekt. Daar horen meerdere diensten bij: informeren, voorlichting, afsluiten, updates, etc.
- **Customer segments - Klantsegmenten**: producten en diensten lever je aan specifieke klantsegmenten. Welke zijn dat? Lever je alle producten en diensten aan alle segmenten of zit daar verschil tussen? Hoe groot zijn de verschillende klantgroepen? Wie als klant wordt beschouwd is volledig afhankelijk van het niveau waarophet business model is beschreven en kan dus een klant binnen of buiten de organisatie zijn.
- **Customer relationships, Channels - Klantrelatie en kanalen**: de koppeling tussen producten en diensten en segmenten loopt via kanalen die een bepaalde relatie realiseren. Verzekeraars werken via intermediairs; zorgverzekeraars ook via zorgkantoren en zorgverleners. De relatie die daarmee wordt onderhouden kan heel direct en persoonlijk zijn, maar ook meer op afstand (via internet) of door selfservice plaatsvinden.
- **Key activities, key resources - Kernactiviteiten en kernresources**: om de dienstverlening te realiseren voer je als organisaties bepaalde activiteiten uit die gebruik maken van resources binnen je organisatie. Wat zijn daarvan de belangrijkste? Het is niet de bedoeling hier in detail in te gaan op processen, maar meer op het niveau van bedrijfsfunctie. Een verzekeraar heeft klantrelaties, vermogensbeheer, marketing en polisbeheer. Een belangrijke resource daarbij is zijn klantadministratie, zijn risico-informatie en de medewerkers.
- **Key partners – Belangrijkste partners**: er zijn maar weinig organisaties die alles alleen kunnen. Bijna iedereen werkt samen met partners die mede bepalend zijn voor het succes. Welke partners zijn dit, en welke rol spelen ze? Vullen ze missende eigen resources aan, of zijn ze overlappend?
- **Cost structure, revenu structure - Kosten- en opbrengstenstructuur**: met de dienstverlening wordt waarde gerealiseerd, of het nu in de profit of non-profit is. Daarmee verbonden is een opbrengstenstructuur. Mensen zijn bereid te betalen voor de dienstverlening of op een andere wijze worden de kosten gedekt. Aan de andere kant worden er ook kosten gemaakt, voor eigen activiteiten, voor inschakelen partners enzovoorts. En, als het goed is, overtreffen de opbrengsten de kosten.

2.1 USE CASE 1: EIGEN-WAARDE

De eerste use case beschrijft een mogelijk commercieel gebruiksscenario.

Frank ter Morsch is een intensief gebruiker van het internet. Hij had als een van de eerste van zijn vrienden 4G en is altijd on-line. Facebook, LinkedIn, Google+, hij kan niet zonder. Met zijn smartphone en Apple watch houdt hij strak in de gaten wat hij doet, hoe veel hij beweegt en waar hij was. Zelfkennis die hij graag deelt. Sinds kort heeft hij zijn social media en health apps aangesloten op MeMyself&I (MeMy), een Personal Data Store die alle data aggregeert, beheert en eenvoudig inzichtelijk maakt voor Frank.

MeMy doet meer dan dat. MeMy nodigt namens Frank dienstverleners uit om met specifieke aanbiedingen te komen. Frank blijft liever zelf in controle over zijn informatie. Doordat hij €5,- per maand betaald aan MeMy kan hij bepalen van wie hij aanbiedingen ontvangt. Frank staat zeker open voor aanbiedingen van mobiele/internetproviders, zorgverzekeringen en gezondheidsadviezen. Frank bepaalt dus wie aanbiedingen doet en welke informatie de dienstverleners te zien krijgen. MeMy zorgt ervoor dat de dienstverleners niet de details van de gegevens van Frank specifiek kennen, maar alleen de relevante attributen.

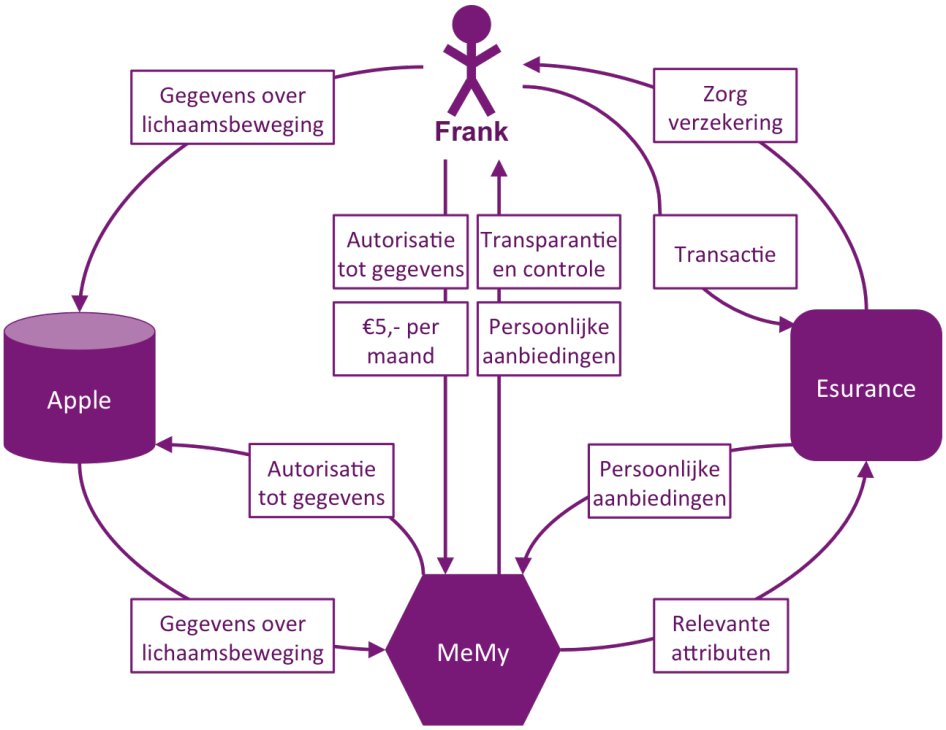
Een alternatief is dat MeMy €2,50 per maand aan de gebruiker betaalt, en zelfs €10,- per familie. In dat geval worden de gegevens direct verkocht aan service providers die daar interesse in hebben. De gebruiker heeft dan geen controle over wie de gegevens gebruikt en hoe ze worden gebruikt. Service providers kunnen de gegevens verder aggregeren en analyseren, bijvoorbeeld voor betere klantsegmentatie.

Frank is elke dag wel sportief bezig, fietsend gaat hij naar zijn werk en minstens twee keer in de week loopt hij hard. De Apple Watch registreert deze bezigheden en geeft Frank een compleet overzicht van zijn dagelijkse activiteiten. Frank is op dit moment niet blij met zijn huidige zorgverzekering. Omdat hij

actief met zijn gezondheid bezig is, wil hij wel een persoonlijke korting krijgen op een nieuwe zorgverzekering. Hij geeft MeMy onder andere toegang tot zijn Apple Watch gegevens. MeMy haalt deze gegevens op bij Apple Watch en verwerkt ze totdat relevante attributen overblijven. Deze relevante attributen worden door MeMy doorgestuurd naar de zorgverzekeraars. Op basis van deze attributen kunnen de zorgverzekeraars Frank een persoonlijke aanbieding sturen. Deze aanbiedingen worden via MeMy naar Frank gestuurd. Eén van de aanbiedingen springt er voor Frank bovenuit. Esurance heeft naast een goede aanbieding ook een zorgadvies bijgevoegd. Het viel Esurance op dat mensen die vaak hardlopen sneller last hebben van knie problemen. Deze bevindingen zijn gebaseerd op de geaggregeerde data van MeMy klanten. Esurance raad Frank aan om in de zorgverzekering fysiotherapie op te nemen en geeft hier tevens een goed aanbod voor. Frank waardeert dit advies en sluit zijn zorgverzekering bij Esurance af.

In dit scenario is de Personal Data Store een volledig private aangelegenheid, met verschillende producten en verdienmodellen. Zowel een betaald model waarin de informatie wordt verhandeld, als een betaald model waarin de eindgebruiker de controle houdt. Een service als MeMy kun je zien als een doorontwikkelde variant van DataCoup die nu al data van gebruikers verhandelt.

In het netwerk van deze private PDS zitten zowel de data providers als de service providers. De service providers zijn zowel klant als partner. In de bovenstaande use case is Apple de data provider en Esurance de service provider. In het figuur hierbeneden staat het waarde netwerk van deze use case.

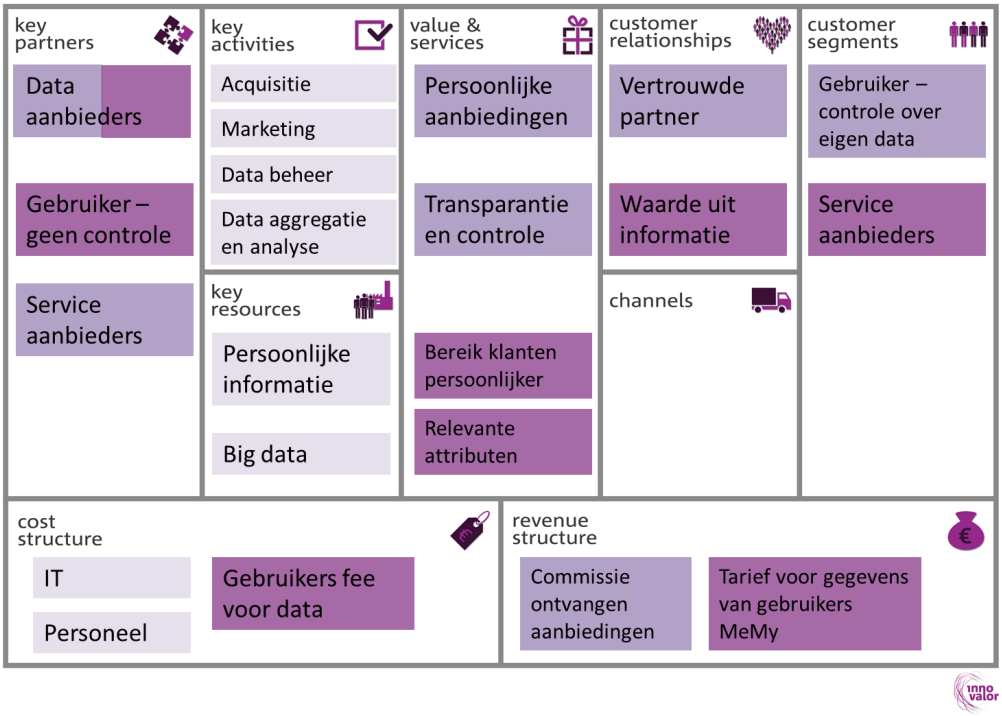


Figuur 3. Waardenetwerk voor privaat PDS

Aandachtspunten

Belangrijke aandachtspunten in alle scenario's rond de acceptatie zitten op het gemak voor de gebruiker, vertrouwen voor alle partijen en een solide business model. Een puur commercieel model zal nadrukkelijk het vertrouwen moeten hebben van de gebruiker en voldoende transparant moeten zijn in zijn handelen. Het is nog maar de vraag of geld als middel om de gebruiker te verleiden voldoende is. Ons eigen onderzoek en onderzoek aan de TU Delft doet anders vermoeden (InnoValor, 2015; Derikx, 2015). Tegelijk kan een business model waarbij de gebruiker betaalt voor de aggregatie en waarde realiseert in aanbiedingen van anderen wellicht goed functioneren.

Het business model van de PDS in deze situatie ziet er globaal als volgt uit.



Figuur 4: Bedrijfsmodel voor commerciële PDS

De PDS levert de gebruiker controle over eigen data en persoonlijke aanbiedingen. Voor dienstenleveranciers is het gericht op een beter bereik van klantsegmenten. Klanten zijn feitelijk hier ook partners: in het leveren van data en het samenstellen van aanbiedingen. Inkomsten kunnen zowel komen uit commissie bij dienstenleveranciers als vanuit een abonnementsmodel. Dit laatste zou je kunnen vergelijken met een betaalde klantenkaart die je stapje voor stapje terugverdient, zoals bij de ANWB.

2.2 USE CASE 2: BRILJANTE OVERHEID

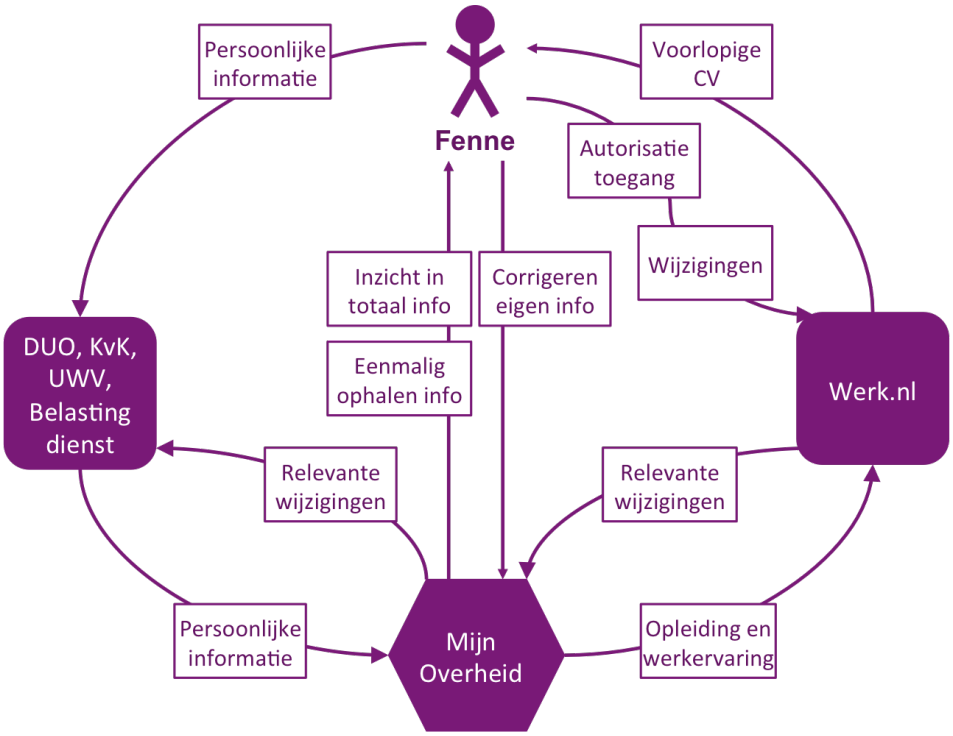
Het tweede gebruiksscenario kun je zien als de ultieme doorontwikkeling van MijnOverheid. Hierin staat Fenne centraal:

> *Fenne is freelance gitaarlerares. Ze heeft een klein contract bij de muziekschool en geeft daarnaast les aan huis. Dat levert wisselende inkomsten op. Doordat ze zelfstandig ondernemer is staat ze geregistreerd bij de Kamer van Koophandel. Ze vult elk jaar netjes haar belastingformulieren in en ze heeft haar pensioen geregeld bij de SVB. Daarnaast heeft ze samen met haar vriend een huis gekocht met een kleine studio erbij, dit staat geregistreerd bij het Kadaster. Kortom, er staat allerlei informatie over Fenne bij verschillende overheidsinstanties. Om het overzicht te bewaren heeft Fenne zich aangemeld bij MijnOverheid. Op MijnOverheid heeft ze inzicht in wie welke informatie over haar heeft. Naast het controleren van de informatie heeft Fenne ook de mogelijkheid om de informatie te corrigeren.*
>
> *Maar MijnOverheid doet meer dan dat. MijnOverheid zorgt ervoor dat alle overheidsinstanties verbonden zijn. Dit zorgt ervoor dat er een eenmalige uitvraag van informatie plaatsvind. Zodra Fenne informatie verstrekt aan een overheidsinstantie hebben andere overheidsinstanties, indien nodig, deze informatie ook. Over de uitwisseling van sommige informatie heeft Fenne geen controle indien dit wettelijk is vastgelegd. Fenne kan zien welke informatie er verplicht wordt gedeeld en ze kan zien over welke informatie ze controle heeft.*
>
> *Fenne vindt het moeilijk om de eindjes aan elkaar te knopen. Om iets meer basisinkomen te hebben besluit ze zich in te schrijven voor werk. Ze gaat naar Werk.nl en logt in op werkmap met haar telefoon*

en ID kaart, als opvolger van het eerder gebruikte DigiD. Zodra ze haar CV aan wil maken geeft Werk.nl een melding dat bepaalde gegevens over opleiding en werkervaring al bekend zullen zijn bij MijnOverheid. Werk.nl biedt haar een optie om deze gegevens bij MijnOverheid op te halen door werk.nl hiervoor te autoriseren. Fenne kan selecteren welke informatie werk.nl voor haar CV mag ophalen. Zo kan ze onder andere kiezen om via DUO haar diploma's en opleidingen toe te voegen, via KvK kan ze opgeven dat ze zelfstandig ondernemer is, via UWV kan ze ophalen of ze werkloos is geweest en voor hoe lang, en via de belastingdienst haar werkgeverservaringen. Ze heeft hier zelf de controle over welke informatie er gedeeld wordt met werk.nl. Met behulp van deze informatie kan werk.nl een voorlopig CV opstellen. Dat scheelt enorm veel werk. Met 10 minuten is er al een aardig compleet CV van Fenne opgesteld. Fenne kan hieraan meer gedetailleerde informatie toevoegen die overheidsinstanties niet over haar hebben. Bijvoorbeeld haar ervaringen met het geven van privé gitaarlessen.

Twee weken later leidt het tot een succes, drie ochtenden gaat Fenne werken in een muziekwinkel. Fenne geeft bij werk.nl dat ze niet langer werkzoekende is aangezien ze is aangenomen. De informatie dat Fenne een baan heeft gevonden wordt automatisch opgeslagen in MijnOverheid. Toeslagen van de Belastingdienst springt hierop in door Fenne een bericht te sturen via de berichtenbox van MijnOverheid. Hiermee notificeert Toeslagen Fenne dat zij haar nieuwe loon op moet geven aangezien dit veranderingen mee zal brengen voor haar zorgtoeslag. Iets later krijgt ze ook bericht van de Belastingdienst: het recht op teruggave van hypotheekrente is door haar extra inkomen gestegen en ze stellen voor de maandelijkse voorlopige teruggave te verhogen.

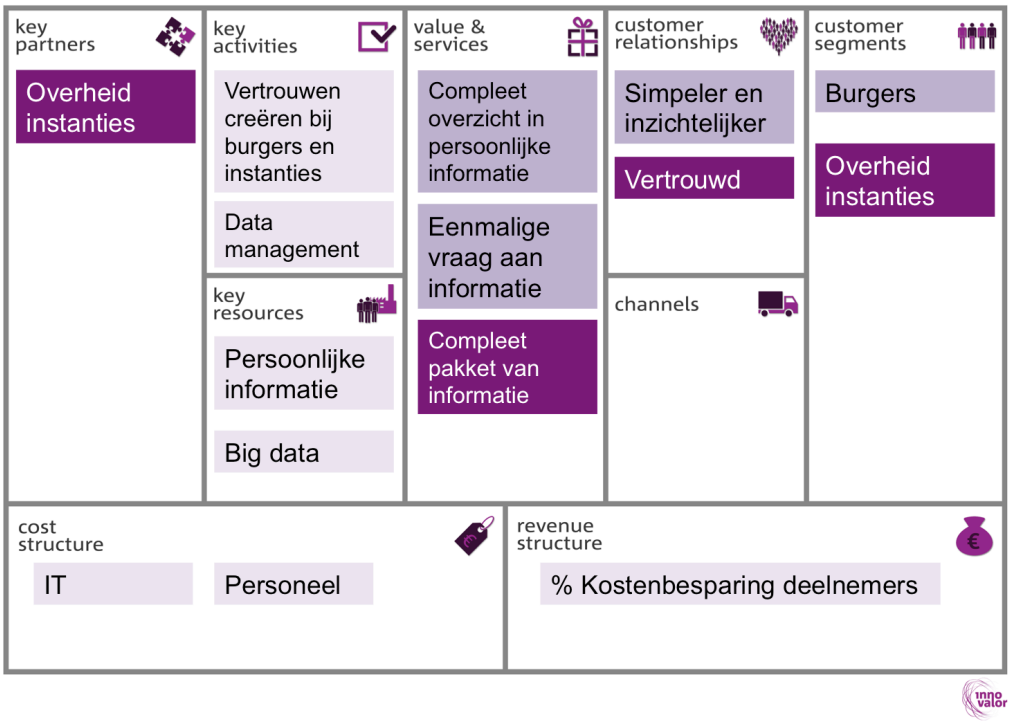
In dit scenario is de belofte van een overheid met eenmalige uitvraag verwezenlijkt. Alle informatie van de overheid is voor burgers en bedrijven transparant in te zien en te muteren. Ook is voor de burgers en bedrijven te zien waar welke informatie is ingezet. Daarbovenop gebruikt de overheid de informatie ook optimaal: op het moment dat er voldoende informatie is voor bepaalde diensten, of de status aanleiding geeft tot een dienst of transactie, neemt de overheid actie daartoe. Voorlopige aangifte, mogelijke vacatures, toeslagen etc. worden proactief afgehandeld en uitgekeerd. Dienstverlening wordt gepersonaliseerd aangeboden indien gewenst.



Figuur 5. Waardenetwerk publieke PDS

Een aandachtspunt hierin is de complexiteit van de informatiepositie. Er is veel informatie beschikbaar, van veel partijen en met verschillende mate van detail. Er is geen sprake van gebruik van informatie door private

partijen en de Personal Data Store ondersteunt niet het delen van informatie buiten de overheid. In het figuur hierbeneden staat het waarde netwerk van bovenstaande use case.



Figuur 6: Bedrijfsmodel publieke PDS

In de publieke PDS ligt de nadruk op kwaliteit. Kwaliteit die moet leiden tot kostenbesparing. Complex in dit model is de verrekening van die kostenbesparing: ook de PDS moet een gezond verdienmodel hebben. Voor de hand liggend is dat een overheidsdienst als deze direct wordt betaald uit de begroting van het ministerie van Binnenlandse Zaken/Logius, zonder complexe verrekening. De geschiedenis leert echter dat deze discussie minder eenvoudig ligt.

2.3 USE CASE 3: TOP PRESTATIE

Het ligt voor de hand om het private en het publieke scenario te combineren tot de “ultieme PDS”. Al is het voor de hand liggend, eenvoudig is het niet. De combinatie van publieke en private informatie, onder regie van de consument, is nog niet goed afgedekt door een wettelijk kader. Maar het scenario is zeker interessant.

> *Eva Jansen en Guus Cornelis staan op het punt om een huis te kopen. Jarenlang hebben ze gehuurd. Guus heeft een VOF samen met een vriend en Eva is zelfstandig adviseur, waardoor het een risico was om te investeren in een huis. Maar nu is hun droomhuis beschikbaar en willen ze het graag kopen. De jaarrekeningen van Eva en Guus staan bij elkaar in hun digitale dossier, PDS-Pro. In PDS-Pro beheren ze hun financiële zaken, samen met de accountant en de boekhouder. Sinds een paar jaar kunnen de gegevens van alle bankrekeningen hierin worden gecombineerd met de andere gegevens. PDS-Pro is door Eva en Guus geautoriseerd om alle overheidsinformatie rond de bedrijven en hen persoonlijk te ontsluiten. KvK gegevens, GBA en belastingaangiftes zijn dus bij elkaar beschikbaar.*
>
> *Na een kort gesprek met Eigen Huis besluiten ze om een viertal hypotheekverstrekkers een offerte te vragen. In PDS-Pro worden Interpolis, Florius, een Duitse en een Estse hypotheekverstrekker uitgenodigd te offreren. Daartoe mogen de hypotheekverstrekkers de relevante gegevens drie dagen inzien en moeten ze binnen vijf werkdagen offreren. Ze betalen een commissie aan PDS-Pro voor de mogelijkheid om een persoonlijke offerte te sturen naar potentiële klanten. ’s Avonds bekijken Eva en Guus de voortgang. Drie van de vijf hebben gegevens al bekeken; de Estse hypotheekverstrekker vraagt of ze een combinatie mogen aanbieden met een woonzekerpakket. Dat mag. De anderen worden geïnformeerd dat die optie er is. Uiteindelijk is het Duitse aanbod het meest aantrekkelijk. Op de*

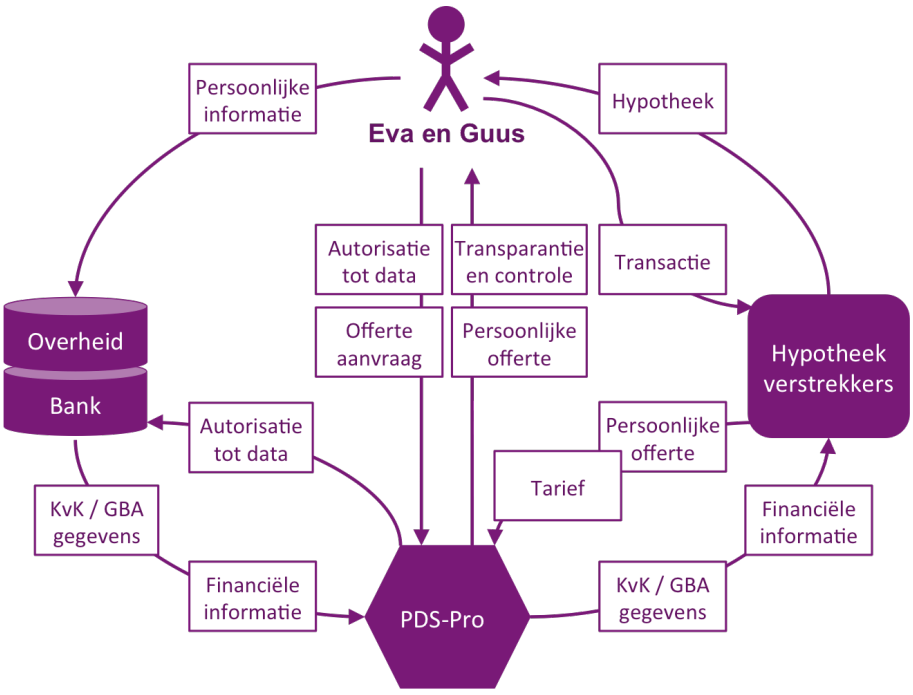
woonverzekering gaan Eva en Guus apart laten bieden, los van de hypotheek. Op 12 juli krijgen ze de sleutel van het huis en beginnen ze met een kleine verbouwing en veel schilderwerk. Gelukkig zijn er veel vrienden die de helpende hand reiken.

Op 17 juli krijgen ze bericht in PDS-Pro van de Belastingdienst die aangeeft dat ze de aankoop hebben gezien en de hypotheekgegevens hebben bekeken. Voorstel is om de hypotheekrenteaftrek maandelijks te verrekenen. Als het akkoord is wordt de eerste termijn 23 juli bijgeschreven. Meteen plannen Eva en Guus de housewarming party op 1 augustus.

In de ultieme situatie is de burger of het bedrijf zelf regisseur van de informatie, publiek en privaat. Regie betekent sturing op wie welke informatie ziet, voor welk doel en met welke prijs. Informatie die publieke organisaties hebben kan door de burger of het bedrijf gedeeld worden met private partijen onder voorwaarden, zoals een beperkte tijd, specifieke doelen of specifieke combinaties. De consument/burger kan dus informatie uit het publieke domein ontsluiten voor private doeleinden. Immers, het is zijn of haar informatie. Omgekeerd kan, als dat gewenst is, ook privéinformatie gedeeld worden met de overheid. Denk aan situaties als werkloosheid of schuldsanering, waarin privébezit en overheidsdiensten gecombineerd worden.

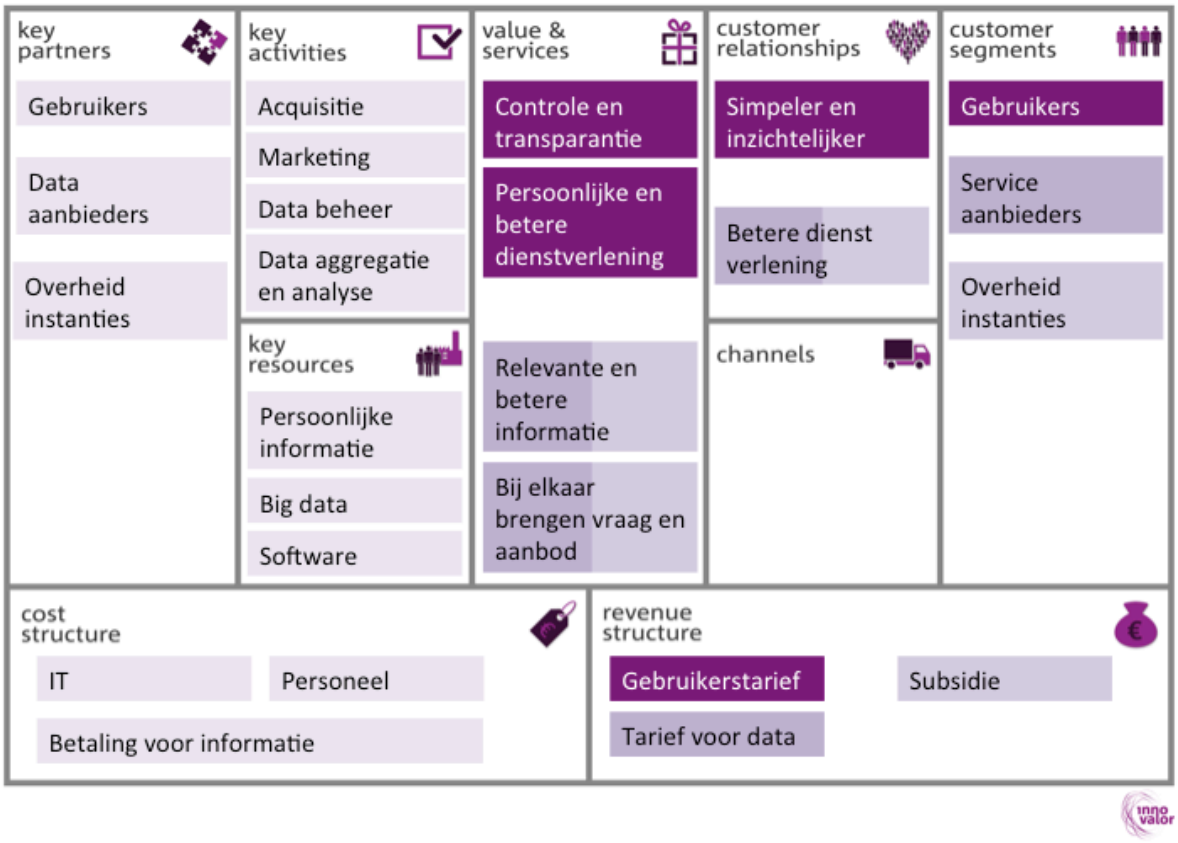
Ook de combinatie van zakelijke informatie met persoonlijke kan erg waardevol zijn. In Nederland zijn er bijzonder veel personen die ook ondernemer zijn, als zelfstandige of in het MKB. Dat zorgt er voor dat privé en zakelijk door elkaar gaan lopen, de grens is een stuk minder duidelijk. In het geval van diensten, zoals de hypotheek in het bovenstaande voorbeeld, brengt dat een enorme bewijslast of informatieverplichting met zich mee, daar waar voor werknemers vaak met een eenvoudige werkgeversverklaring kan worden volstaan.

Feitelijk is het een combinatie van de eerste twee use cases waarin dus privaat en publiek gebruik worden gecombineerd. Anders dan in het private scenario gaat het hier niet per se om geldelijk gewin, maar meer om kwaliteit van dienstverlening, prijs, en personalisatie. De complexiteit kan met deze combinatie een probleem worden. Het gaat om nog meer informatie, uit nog meer bronnen met nog meer gebruikers. Dit beheersbaar houden voor de gebruiker is een grote uitdaging.



Figuur 7: Waardenetwerk publiek-private PDS

Dit scenario is primair gericht op optimale dienstverlening, zowel in prijs als kwaliteit. Een belangrijk aandachtspunt in het business model is de samenwerking tussen het publieke deel en de PDS. Deze moet toegang hebben tot de publieke data, maar kan geen (semi-) publieke organisatie zijn. Het is een complexe en sterk vertrouwens gebaseerde rol.



Figuur 8: Publiek-private PDS

2.4 HET POTENTIEEL

Er zijn verschillende manieren waarop PDS's potentieel waarde creëren. Doordat het gebruik van een PDS het vertrouwen weet te versterken van de gebruiker zijn zij bereid meer informatie prijs te geven, bijvoorbeeld zgn. *volunteered personal information.* Daarnaast geven PDS's beter inzicht in de consument, door meer en betere persoonlijke data beschikbaar te maken, wat kan leiden tot verbeterde dienstverlening en innovatie.

Centralisering van persoonlijke data bij de gebruiker leidt tot meer recombinatie van data in de PDS en, mits vrijgegeven door de gebruiker, naar data afnemers, wat kan leiden tot nieuwe inzichten en meer of verbeterde persoonlijke informatie. PDS's verhogen ook de kwaliteit van persoonlijke data, bijvoorbeeld door meer accurate informatie door validatie tegen meerdere bronnen of correctie door de gebruiker, wat leidt tot een betere afstemming van vraag en aanbod, bijvoorbeeld in de vorm van gerichte marketing.

Verbeterd risicomanagement door inmenging van het data-subject (de gebruiker) leidt tot kostenbesparing ten gevolge van efficiëntie en minder incidenten. Beter inzicht uit nieuwe informatie draagt ook bij aan compliance met wet- en regelgeving. Verder ontstaat door het beheer van persoonlijke informatie deels uit te besteden aan de gebruiker ook meer efficiëntie en kostenbesparing.

Van de marktwaarde van PDS's zijn op dit moment alleen nog schattingen te maken. Zeker gezien er nog geen grote doorbraken op dit gebied zijn. Er lijkt veel potentie te liggen, maar of die gepakt kan worden is een tweede. Dat consumenten zich steeds bewuster bezighouden met vertrouwen en privacy risico's is in elk geval een feit. Onderzoeken van BCG en Ctrl-Shift schatten de waarde van PDS's in elk geval hoog in.

Personal Information Management Systems - An analysis of an emerging market (Ctrl-Shift, 2014)

- PDS's zijn een disruptieve technologie die de kosten van het maken en managen van informatie drastisch verlaagt.
- Er volgt economische waarde uit het bij elkaar brengen van vraag en aanbod, een verbeterd inzicht in consumenten, product innovatie, en verbeterd risicomanagement en compliance.
- Men voorspelt een volwassen markt voor PDS's van 16.5 miljard Pond in het Verenigd Koninkrijk, ofwel 1.2% van de nationale economie, groter dan de automotive (0.7%) en farmaceutische (0.97%) industrieën.
- Maar: instabielere markten door hogere 'churn-rate', disintermediatie, en commodificatie.
- De gevolgen verschillen per sector, er is bijvoorbeeld een verhoogd risico van disintermediatie voor de financiële sector, maar mogelijkheden voor betere dienstverlening van de overheid.

Voor organisaties in Europa zou er 660 miljard aan economisch voordeel uit personal data gehaald kunnen worden: "*at a 22% annual growth rate, applying personal data can deliver a €330 billion annual economic benefit for organisations in Europe by 2020*" (BCG, 2012). Dit getal is gebaseerd op de meest groeiende data intensieve industrie: online info en entertainment. De consumenten waarde zou zelfs op 670 miljard uitkomen, gebaseerd op lagere kosten doorberekend aan klanten, en tijdsbesparing door self-service zoals online dienstverlening.

Als we kijken naar ons eigen onderzoek en de getallen in Nederland lijkt de potentie ook groot te zijn. Uit het onderzoek blijkt dat mensen in het algemeen geen idee hebben van wie wanneer hun gegevens ziet of gebruikt. Er is dan ook een sterke behoefte aan meer inzicht in het gebruik van persoonlijke data. Dit zorgt ervoor dat 57% van de Nederlanders (boven de 18) een PDS dienst wel zouden willen gebruiken (InnoValor, 2015).

De relevantie van PDS's is wereldwijd, maar vroege adoptie wordt verwacht in landen met een hoge mate van digitale volwassenheid zoals Scandinavië, Nederland en de VS. Dit wordt weerspiegeld in de huidige initiatieven, er is nu een gefragmenteerd landschap zonder dominante spelers. Er is dus ook nog geen dominant model voor het verdienmodel en de technologie.

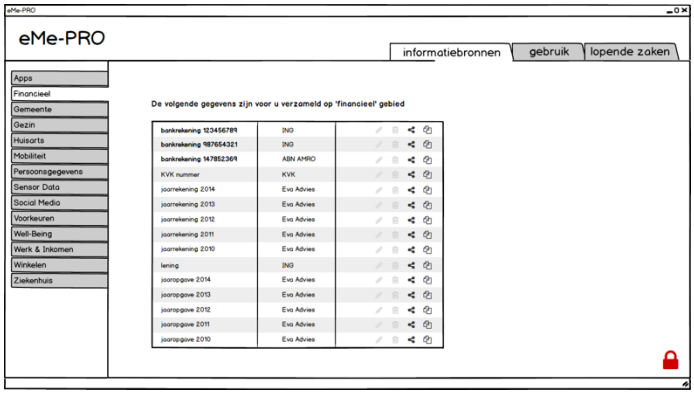
Deze technologie staat boven verschillen in demografieën, maar vereist wel enige mediawijsheid van de gebruiker. Er zijn al relatief veel vroege initiatieven, maar nog geen gevestigde merken. Naar verwachting zullen in eerste instantie PDS's voor sectorspecifieke data (bijvoorbeeld een zorgkluis) succesvoller zijn dan PDS's die sectoren met elkaar koppelen. Een volwassen markt wordt verwacht binnen 2 tot 5 jaar.

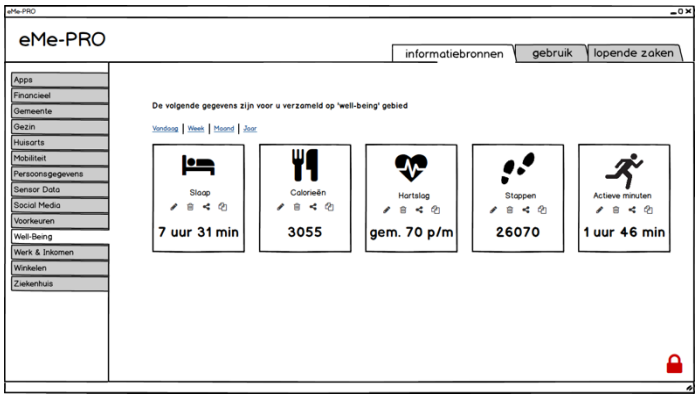
3 Het concept Personal Data Store

3.1 FUNCTIONALITEIT

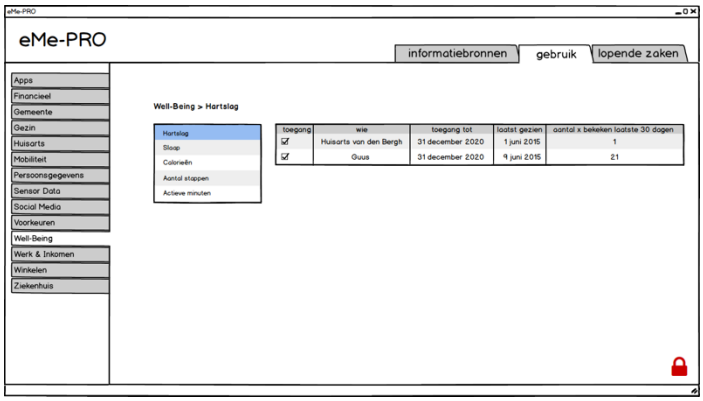
De omschrijving van PDS's laat nog veel zaken open. Hoe kan een PDS bijvoorbeeld gerealiseerd worden en wat is daar technisch voor nodig? En welke gegevens kunnen we beheren met een PDS? Daarnaast omvat de PDS een aantal basisfuncties, maar wat moet een PDS allemaal nog meer kunnen en wat vinden we de belangrijkste functies?

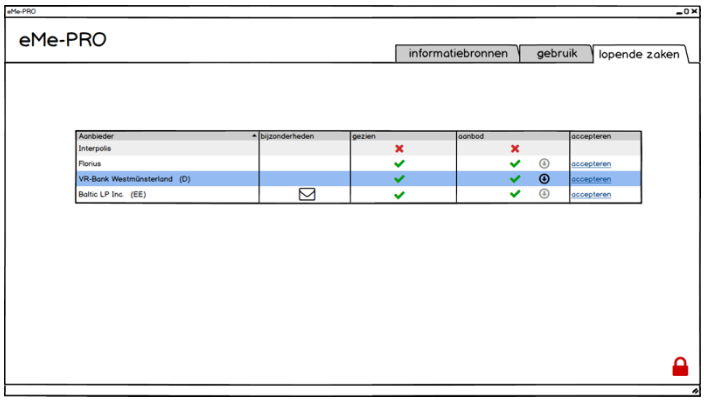
In een animatie hebben we geschetst hoe een publiek-private PDS zou kunnen werken, gebaseerd op het scenario van Eva en Guus. Dit combineert onderdelen van bestaande PDS initiatieven. Daarin worden verschillende informatiebronnen ontsloten (zie onderstaande schermen). Dit kunnen bronnen zijn bij de overheid, bij verzekeraars, banken, werkgever, noem maar op, maar ook informatie op persoonlijke devices, zoals slimme apps of fitheidsmeters.





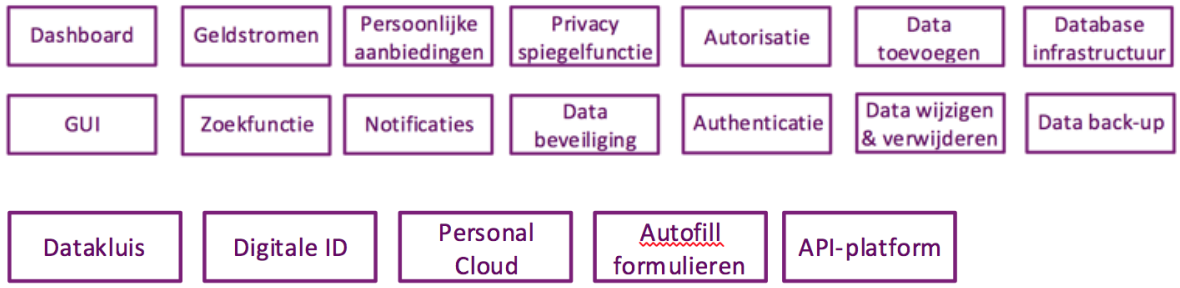
Die informatie kan gedeeld worden met anderen, zoals familie, artsen of dienstenaanbieders waarvan je een specifieke aanbieding wilt. Het delen kan gebonden zijn aan tijd (een bepaalde periode), aan een doel (een offerte, bijvoorbeeld), en een specifieke organisatie. Alles onder direct regie van de eigenaar van de data.





Wat zijn nu de onderliggende functionele bouwblokken?

Aan de ene kant heeft de PDS een dashboard en interface waarmee de PDS toegankelijk wordt voor de gebruiker. Hierop zien we bijvoorbeeld de laatste notificaties, persoonlijke aanbiedingen en een zoekfunctie. De gebruiker kan daarnaast organisaties autoriseren om zijn gegevens te gebruiken en zelf zijn gegevens bewerken, of een verzoek doen ter verwijdering van zijn gegevens.



Samengenomen vormen deze functies de kern van waar een PDS voor kan staan en hoe een PDS vormgegeven kan worden. De diverse voorbeelden van PDS's benadrukt de hoeveelheid aan verschillende onderdelen zoals ze hier genoemd staan. DataCoup houdt zich bijvoorbeeld meer met de geldstromen bezig, terwijl DataPlaza zich meer op het 'Digitale kluis' idee richt.

Wanneer we aan Nederlanders vragen wat ze de belangrijkste mogelijkheden vinden als het gaat om beheer van persoonlijke gegevens zijn dit (InnoValor 2015):

- Zelf toegang bepalen
- Inzicht in data gebruik
- Verwijderen
- Corrigeren

Deze vier zaken zouden daarmee in elke PDS ten minste terug moeten komen. De andere functionaliteiten die hier genoemd zijn zouden deze kern moeten faciliteren. Inzicht is namelijk te verkrijgen door een duidelijke dashboard met zoekfunctie. Het zorgen voor goede data beveiliging en authenticatie van organisaties faciliteert dat een gebruiker iets te kiezen heeft.

Binnen een PDS omgeving zijn er tal van soorten data die kunnen worden ontsloten. Kearns (2009) onderscheidt vijf types:

1. *My Data:* binnen het domein van het individu
2. *Your data:* binnen het domein van een organisatie
3. *Their data:* samengesteld door derden
4. *Everybody's data:* in het publieke domein
5. *Our data:* bovenstaande types data toegankelijk vanuit een transactie of relatie

Deze vijf types kunnen allerlei soorten (persoonlijke) gegevens bevatten. Denk bijvoorbeeld aan data uit sociale media, voorkeuren, financiële informatie, eigendoms- en licentierechten, zoekresultaten, medische gegevens, persoonsgegevens, sensordata of beeldmateriaal.

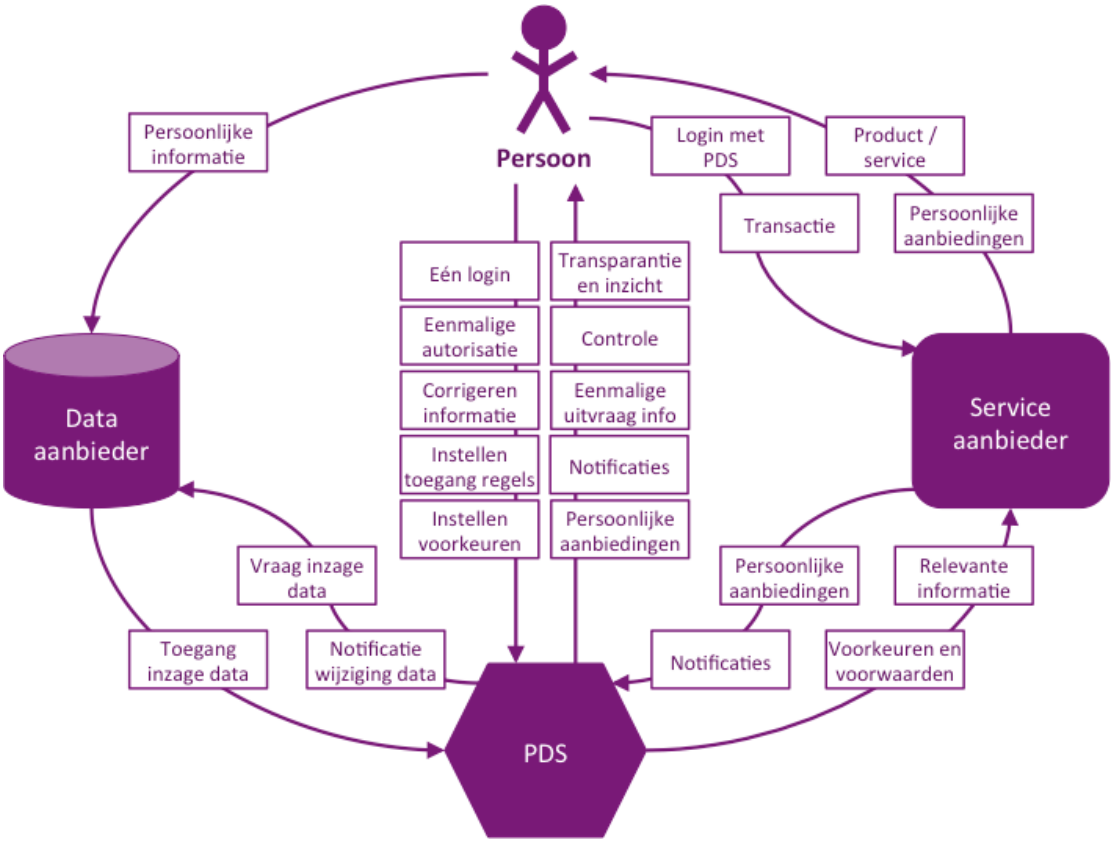
3.2 DE CONTEXT

De bovenstaande onderdelen van een PDS kunnen we tot een algemeen bedrijfsmodel en waardenetwerk vormen, gebaseerd op de scenario's uit het vorige hoofdstuk. In het waardenetwerk rondom Personal Data Stores zijn er vier rollen te vervullen:

1. De Personal Data Store
2. De aanbieder van de data
3. De aanbieder van de services
4. De persoon aangesloten bij de PDS: de gebruiker

De persoon als gebruiker van de PDS zal persoonlijke informatie opslaan bij een data aanbieder. Vaak gebeurt dit door een bepaald contact tussen de gebruiker en de data aanbieder. Doordat de gebruiker is aangesloten bij de PDS kan hij/zij met één login inzicht (en dus transparantie) krijgen in al zijn/haar informatie. Het is noodzakelijk om iedere bestaande data aanbieder van een eenmalige autorisatie te voorzien zodat de PDS daadwerkelijk bij de data van de gebruiker kan. Met deze autorisatie zal de PDS een vraag naar inzage in data

uitzetten bij de data aanbieder, deze zal vervolgens toegang tot inzage van de data geven. De gebruiker heeft vervolgens de mogelijkheid om informatie te corrigeren. Kortom, de gebruiker is in controle. De PDS biedt de gebruiker een eenmalige uitvraag van informatie. Dit betekent dat de gebruiker niet telkens weer al zijn informatie hoeft door te geven. Indien de gebruiker het toestaat of omdat het wettelijk is verplicht, wordt er een notificatie verstuurd aan de data aanbieders door de PDS dat er informatie is gewijzigd. Doordat de gebruiker zelf in controle is wordt er van hem verwacht dat hij toegangsregels en voorkeuren instelt. Op deze manier bepaalt de gebruiker wie welke informatie ziet en waar zijn persoonlijke informatie voor gebruikt mag worden.



Figuur 9: Waardenetwerk rondom de Personal Data Store

De gebruiker kan via de PDS op twee manieren in contact komen met service aanbieders. Eén van deze manieren is het ontvangen van persoonlijke aanbiedingen via de PDS. Dit houdt in dat op basis van de voorkeuren en voorwaarden bepaalde service aanbieders relevante informatie van de gebruiker te zien krijgen zodat er persoonlijke aanbiedingen of notificaties verstuurd kunnen worden. Deze worden door de PDS verstuurd aan de gebruiker. Indien de gebruiker ingaat op de aanbiedingen of notificaties kan er een transactie worden gemaakt met de service aanbieder, die het product of de service zal leveren aan de gebruiker.

Een andere manier van contact via de PDS is door middel van een PDS login op de omgeving van de service aanbieder. In plaats van een eigen login kan de persoon inloggen met zijn PDS login. Indien de voorkeuren en voorwaarden goed ingesteld zijn kan de service aanbieder gebruik maken van de gegevens die de PDS bezit. Mocht dit niet zo zijn dan zal er een notificatie verschijnen dat de gebruiker voor een persoonlijk aanbod zijn toegangsregels of voorkeuren moet aanpassen. Zodra de gebruiker hiermee akkoord gaat zal de service aanbieder op zijn eigen omgeving persoonlijke aanbiedingen kunnen creëren. Ook in deze situatie zal er direct met de service aanbieder een transactie plaatsvinden en zal de service aanbieder het product of de service aanbieden aan de gebruiker.

De rollen van dataaanbieder en service aanbieder kunnen door dezelfde actor worden ingevuld. In het geval van een transactie kan het zijn dat de gebruiker extra informatie doorgeeft aan de data aanbieder. Op dit moment wordt de data aanbieder tevens een service aanbieder. Dus er vindt een verandering in de rol plaats. Er wordt dan persoonlijke informatie gestuurd van de gebruiker naar de data aanbieder.

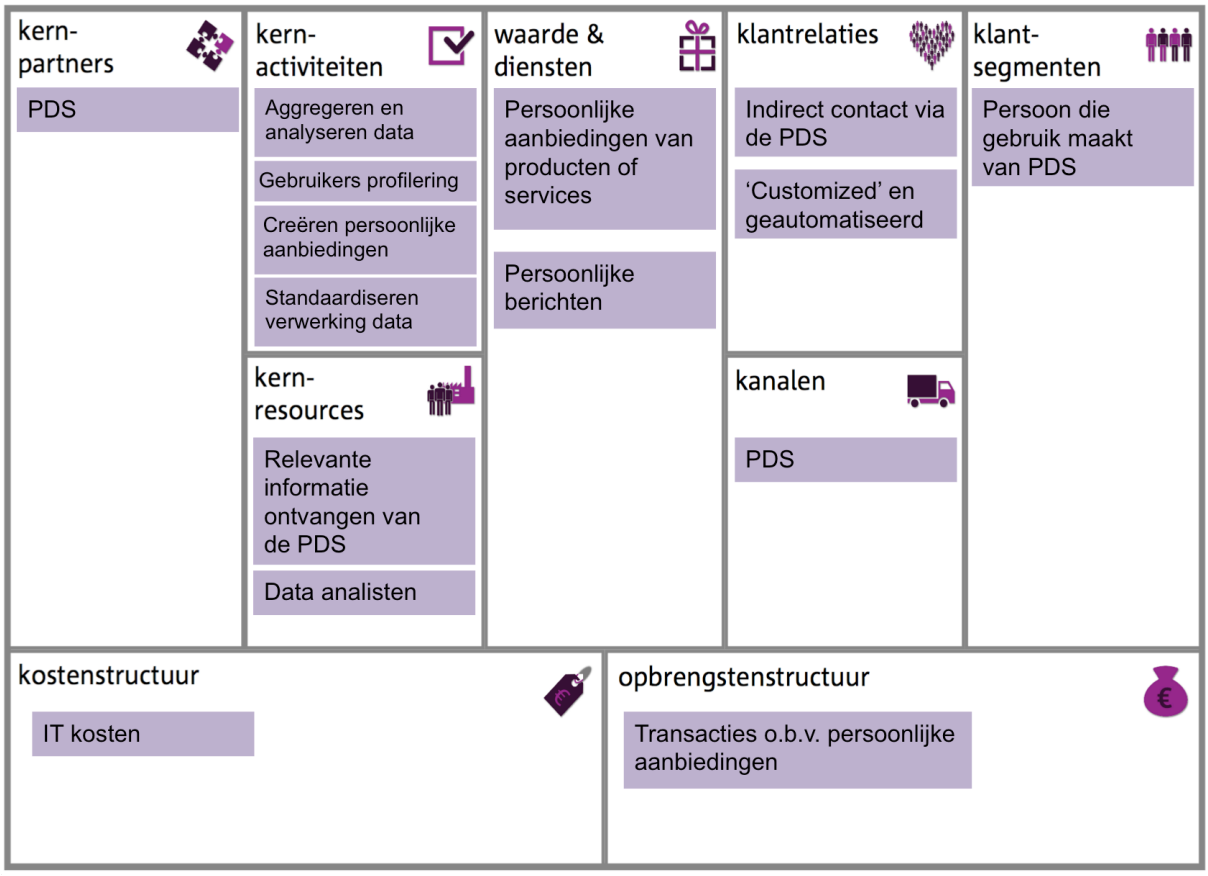
Drie van de vier rollen hierboven in het waardenetwerk genoemd betreffen organisaties. Deze organisaties hebben ieder een bedrijfsmodel. Indien de Personal Data Store een actieve rol krijgt en zijn services zal bieden aan de gebruikers dan zal dit een impact hebben op de bedrijfsmodellen van de data en service aanbieders. Er komt immers een andere speler in de markt omtrent persoonlijke informatie: de PDS.

Sommige bedrijfsmodellen hebben gelijksoortige karakteristieken; soortgelijke indelingen van de componenten van het bedrijfsmodel. Deze overeenkomsten in de indeling van het bedrijfsmodel worden ook wel patronen genoemd. Rondom de PDS zijn er drie bedrijfsmodel patronen te onderscheiden:

1. Het aansluiten op een PDS zal een soortgelijke impact hebben op de service aanbieders.
2. Data leveren aan de PDS zal een soortgelijke impact hebben op de data aanbieders.
3. En het opzetten van een PDS zal een impact hebben op de organisatie die de PDS opzet.

BM Patroon – Aansluiten bij een PDS (Service Aanbieder)

Voor een service aanbieder die zich aansluit bij een Personal Data Store zal er een nieuw klantsegment beschikbaar zijn, namelijk de personen die aangesloten zijn op de PDS. Dit klantsegment hoeft niet volledig nieuw te zijn aangezien huidige klanten ook gebruik kunnen maken van de PDS. Doordat de service aanbieder aangesloten is kan het persoonlijke aanbiedingen en berichten sturen naar dit klantsegment. Dit gebeurt dan via de PDS waardoor het contact met de klant enigszins indirect is. Daarnaast zijn de berichten weliswaar persoonlijk en dus 'customized' maar ook geautomatiseerd.



Figuur 10: Business model canvas van de service aanbieder die zich aansluit bij de PDS

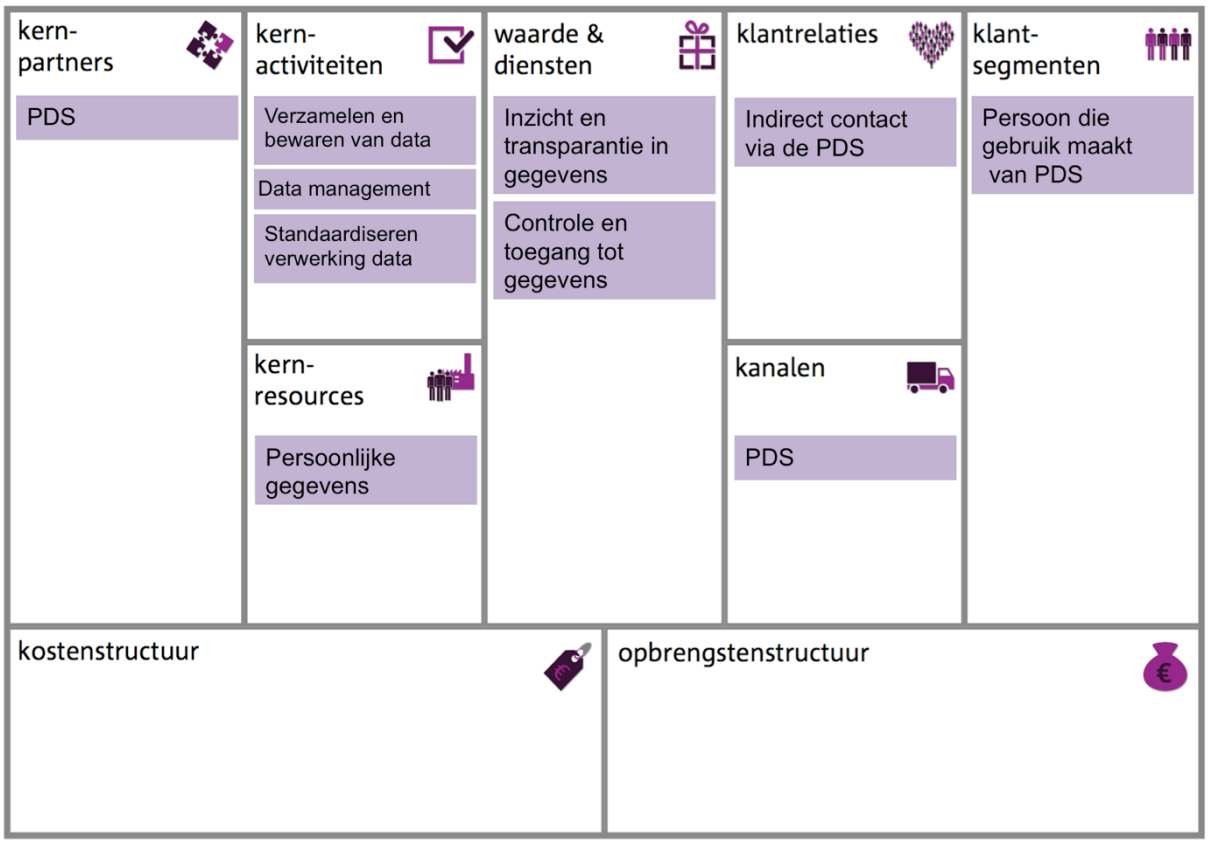
Al dit contact loopt via de PDS, dit is dus een extra kanaal voor de service aanbieder. Het aanbieden van deze extra waarde en diensten aan de klant zal zorgen voor transacties o.b.v. de persoonlijke aanbiedingen. De PDS fungeert niet alleen als een kanaal maar ook als een belangrijke partner van de service aanbieder. De PDS stuurt relevante informatie naar de service aanbieder, een belangrijk middel om tot de persoonlijke aanbiedingen te komen. Deze relevante informatie zal door de data analisten geaggregeerd en geanalyseerd

worden. Op basis hiervan zal er een gebruikersprofiel worden opgesteld en persoonlijke aanbiedingen worden gecreëerd. Om dit alles mogelijk te maken moet de manier van data verwerken gestandaardiseerd worden. Er zijn IT kosten verbonden aan het uitvoeren van de kernactiviteiten en het houden van de kernmiddelen.

Kortom: het aansluiten bij een PDS zal voor een service aanbieder extra opbrengsten en tevens extra kosten met zich mee brengen. De waarde en diensten die de service aanbieder biedt zal verbeteren door het persoonlijk maken van aanbiedingen en berichten. Daarnaast kunnen de huidige klanten van de service aanbieder ook gebruik maken van de PDS, en dus van de extra diensten profiteren.

BM Patroon – Aansluiten bij een PDS (Data Aanbieder)

Zodra de data aanbieder data verstrekt aan de PDS zal het een nieuwe klantgroep bedienen, namelijk de personen die gebruik maken van de PDS. Deze groep bestaat uit personen waarover de data aanbieder informatie heeft verzameld. Doordat de data aanbieder is aangesloten bij de PDS biedt het de mogelijkheid voor de personen om inzicht en transparantie te geven over de eigen gegevens. De data aanbieder geeft de personen controle en toegang tot hun gegevens. Dit gebeurt door middel van indirect contact via de PDS. De PDS is dus een belangrijk kanaal voor de data aanbieder. De PDS is zowel een belangrijk kanaal als een belangrijke partner van de data aanbieder. De PDS voorziet de omgeving waarin de persoonlijke informatie in kan worden gezien en worden beheerd. Voor de data aanbieder zijn de persoonlijke gegevens het belangrijkste middel, zonder gegevens hoeft het niet aangesloten te zijn bij de PDS. De data aanbieder zal deze gegevens moeten verzamelen en bewaren en doet dus aan data management. Daarnaast is het van belang dat de verwerking van data gestandaardiseerd wordt. Er zijn geen relevante kosten of opbrengsten verbonden aan het aansluiten bij een PDS voor de data aanbieder. Dit komt doordat de meeste activiteiten al worden uitgevoerd op dit moment en omdat er niet daadwerkelijk een nieuwe groep met klanten wordt aangesproken.



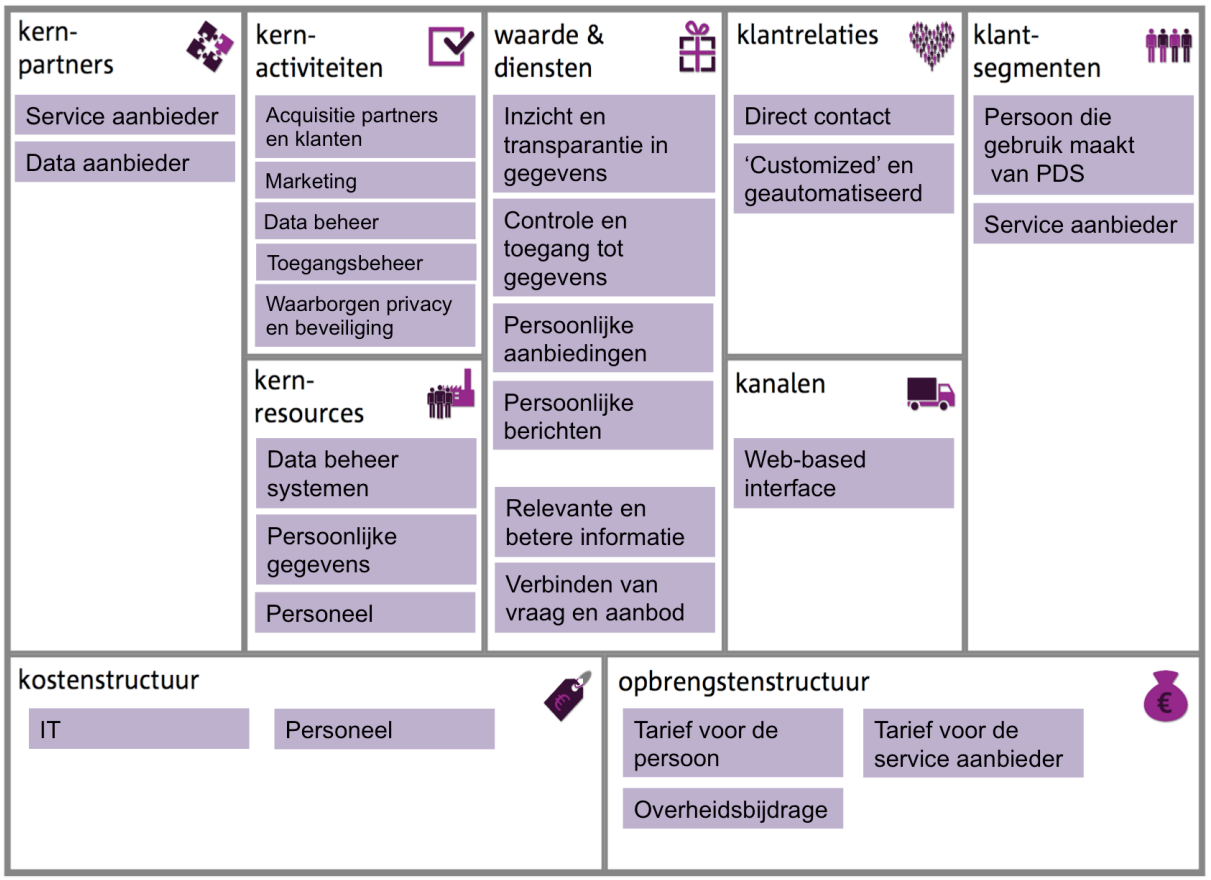
Figuur 11: Business model canvas van de data aanbieder die zich aansluit bij de PDS

Kortom: voor een data aanbieder is het aansluiten bij een PDS voornamelijk interessant doordat er meer waarde aan de klanten worden aangeboden. Dit zal kunnen leiden tot meer vertrouwen en een betere reputatie.

BM Patroon – Ontwikkelen van een PDS

Een organisatie die een PDS gaat ontwikkelen als 'core business' of 'side business' zal een aantal klantsegmenten aanspreken. Als eerste zijn er de personen (consumenten, burgers) die gebruik gaan maken van de diensten van de PDS. Daarnaast kunnen de service aanbieders die aangesloten zijn worden beschouwd als een klant. De PDS biedt de personen een manier om inzicht en transparantie te krijgen in hun eigen gegevens. Daarnaast krijgen ze controle en toegang tot hun gegevens. De PDS maakt het tevens mogelijk om persoonlijke aanbiedingen en berichten te ontvangen, gebaseerd op relevante informatie van de persoon. De PDS biedt de service aanbieders relevante en betere informatie waardoor het voor de service aanbieders mogelijk wordt om persoonlijke aanbiedingen te creëren. Als laatste verbind de PDS vraag en aanbod met elkaar wat voor beide kanten gunstig is. De PDS heeft direct contact met de personen en service aanbieders. Het contact met de persoon is dan wel persoonlijk en 'customized', het is tevens geautomatiseerd. Er is geen face-to-face contact. Het contact verloopt via een 'web-based interface' voor de personen en de service aanbieders. Er zijn voor de PDS drie manieren om opbrengsten te genereren: een tarief voor de persoon, een tarief voor de service provider, en/of in het geval van een overheidsinstantie als service aanbieder kan er een overheidsbijdrage beschikbaar komen.

De service aanbieder en de data aanbieder zijn beide belangrijke partners voor de PDS. De data aanbieder zorgt voor de persoonlijke gegevens van de gebruikers terwijl de service aanbieder zorgt voor de persoonlijke aanbiedingen en berichten. De persoonlijke gegevens is een belangrijk middel van de PDS maar niet het enige middel. Zonder een data beheer systeem en personeel kan de PDS niet bestaan. De PDS houdt zich met name bezig met de acquisitie van klanten en partners. Dit gebeurt o.a. door middel van marketing. De data moet worden beheerd en de toegang tot data moet worden beheerd. Van belang is dat de PDS zich altijd richt op het waarborgen van privacy en beveiliging van gegevens. Aan deze middelen en activiteiten hangt een prijskaartje in de vorm van IT kosten en personeelskosten.



Figuur 12: business model canvas van het ontwikkelen van een PDS

Kortom: een PDS heeft drie manieren waarop het opbrengsten kan genereren, maar er zijn tevens een aantal kosten aan verbonden. In het volgende hoofdstuk zullen de drie verdienmodellen aan het licht komen en de impact hiervan. Een PDS bestaat in een complex netwerk van klanten en partners, maar kan hier tevens veel waarde toevoegen. Deze waarde komt niet uit zichzelf maar zal door een aantal activiteiten en middelen tot stand komen, en niet te vergeten een goed afsprakenstelsel.

Verdienmodellen PDS

Zoals hierboven is genoemd zijn er drie manieren waarop een PDS geld kan verdienen. Een PDS kan een tarief aan de gebruiker vragen, een tarief aan de service aanbieder vragen, of een overheidsbijdrage ontvangen. We zullen de drie manieren beschrijven door te kijken welke typische verdienmodellen er bij passen.

Tarief voor gebruiker

Het tarief voor de gebruikers kan op meerdere manieren worden bepaald. Kortom, er zijn meerdere verdienmodellen die hier toepasbaar zijn. Er zijn drie verdienmodellen die het meest geschikt zijn voor het berekenen van dit tarief: 'pay per use', 'add-on', en 'freemium'.

Pay per use is een model waarin de gebruiker toegang heeft tot alle middelen beschikbaar gesteld door het bedrijf, maar de gebruiker betaalt slechts voor daadwerkelijk gebruik. Gebruikers betalen naar rato van gebruik uitgedrukt in een hoeveelheid. Voor de PDS kan dit model ingezet worden om het tarief te berekenen op basis van het werkelijke gebruik van de functionaliteiten die door de PDS worden aangeboden. **Voorbeeld**: Car2Go biedt een dienst aan die het mogelijk maakt om auto's te delen zonder de moeilijkheden omtrent eigenaarschap van de auto's en de conventionele autohuur. Je betaalt eenmalig voor een lidmaatschap en Car2Go vraagt een tarief voor elke minuut.

Add-on is een model waarbij gebruikers een klein bedrag betalen voor de kern van een product of service. Vanuit die basis heeft de gebruiker de mogelijkheid om tegen extra betaling het product of service naar wens uit te breiden. Voor de PDS kan dit model ingezet worden om de kern van de PDS aan te bieden voor een lage prijs, voor alle uitbreidingen zal de gebruiker extra moeten betalen. **Voorbeeld**: Vliegtuigmaatschappij Ryanair biedt de gebruiker goedkope vluchten aan maar met minimum comfort en service. Op deze manier maken ze vliegen mogelijk voor iedereen. Tegen bijbetaling kan er bijvoorbeeld meer beenruimte, een maaltijd of vliegverzekering verkregen worden.

De term Freemium is een samenvoeging tussen de woorden 'Free' en 'Premium'. Het is een verdienmodel waarin in eerste instantie een product of dienst gratis wordt aangeboden. Voor de geavanceerde gebruiksmogelijkheden of uitgebreide functionaliteiten wordt dan wel geld gevraagd. Voor de PDS kan dit model ingezet worden om een klein gedeelte van de functionaliteiten gratis aan te bieden, zodat potentiële gebruikers worden aangetrokken. Als een persoon gebruik wil maken van alle opties dan zal hier extra voor betaald moeten worden. **Voorbeeld**: LinkedIn is een klassiek voorbeeld van een succesvol Freemium model. De gratis versie maakt het mogelijk om professionele profielen te vinden en te delen. Daarnaast biedt LinkedIn een aantal premium opties aan zoals talent solutions voor recruitment professionals.

Tarief voor service aanbieder

Het tarief voor de service aanbieders kan tevens op meerdere manieren worden bepaald. De verdienmodellen die hier het beste bij passen zijn: 'revenue share', 'licenties', en 'affiliation'.

Het delen van opbrengsten (revenu share) is een model waarbij een organisatie een gedeelte van de operationele winst en verlies deelt met partner(s) die aan dat deel hebben bijgedragen. Voor de PDS kan dit model ingezet worden zodat de service aanbieders gratis gebruik kunnen maken van de functionaliteiten. Zodra de service aanbieder opbrengsten creëert dankzij deze functionaliteiten zal een gedeelte hiervan toekomen aan de PDS. **Voorbeeld**: Groupon is een online aanbieder van exclusieve kortingen ter promotie van lokale bedrijven. Groupon onderhandelt met de bedrijven over de hoogte van de korting en het minimum aantal gebruikers van die korting. Zodra het minimum aantal gebruikers is bereikt krijgt Groupon 50% van de winst waaraan zij aan hebben bijgedragen tijdens de promotie.

Licenties is een verdienmodel waarbij een organisatie de rechten voor het gebruikmaken van een product aan de gebruiker verkoopt voor een vastgestelde periode. Voorbeelden van gebruikelijke licentiemodellen zijn: End User License Agreement, Pay-Per-Use, Sharing Licenses en Site License. Voor de PDS kan dit model ingezet worden om het recht van gebruik te verkopen aan service aanbieders onder een aantal voorwaarden, zoals maximale duur of maximaal aantal gebruikers. **Voorbeeld**: Adobe is een softwarebedrijf dat haar producten verkoopt met een licentie. Enkel met deze licentie kan hiervan gebruikt worden gemaakt. De gebruiker wordt nooit eigenaar van het product maar kan door contractverlenging het product gebruiken.

Er is sprake van affiliation als iemand, de affiliate, zich inspant voor de marketing van andermans producten of diensten. Online advertenties en links worden op de affiliate's website geplaatst om transacties voor een ander te generen. Voor de PDS kan dit model ingezet worden door te verwijzen naar service providers op zijn platform, in ruil hiervoor zal de PDS een gedeelte van de opbrengsten (die voortkomen uit de verwijzing) krijgen. **Voorbeeld**: Booking.com heeft een affiliation programma. Een affiliate heeft bij Booking.com de keuze uit banners, zoekmachines en links om te plaatsen op zijn/haar eigen website.

Overheidsbijdrage

Zodra de PDS waarde creëert voor overheidsinstellingen, bijvoorbeeld door betere uitvraag van informatie, zal er wellicht een bijdrage van de overheid aan de ontwikkelingen en ondersteuning van de PDS komen. Dit kan tevens worden gezien als een verdienmodel.

4 Het actuele landschap

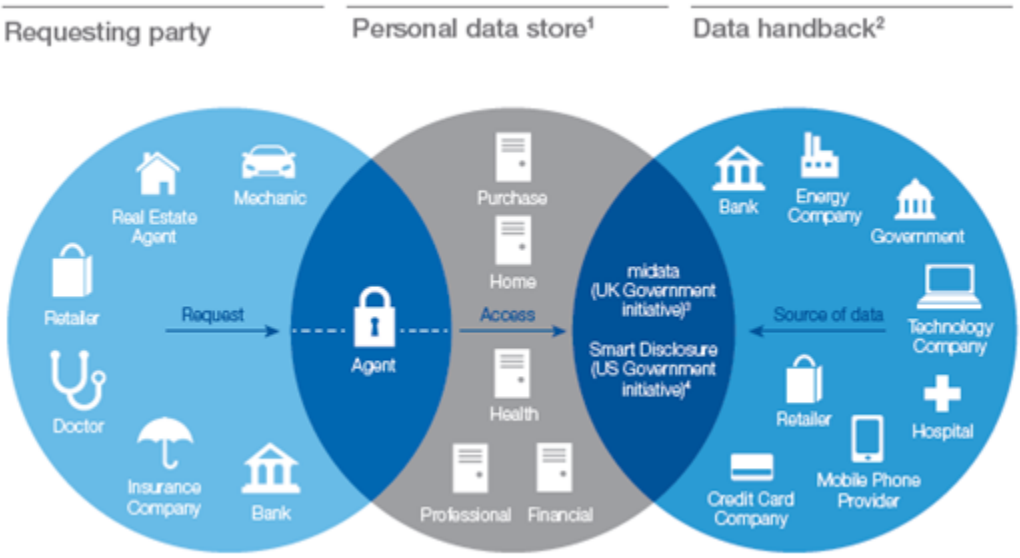
We hebben nu gezien wat Personal Data Stores zijn, wat voor functionaliteit deze technologie biedt, en dat het bijzondere economische potentie betreft. In dit hoofdstuk kijken we verder hoe het landschap voor PDS's er uitziet. Allereerst worden een aantal noemenswaardige initiatieven uitgelicht. Daarna zal de context van PDS's worden bezien: waar de markt bestaat, in welk ecosysteem PDS's zich bevinden, en hoe dit zich verhoudt tot andere trends. Ten slotte wordt ingegaan op wet- en regelgeving en standaardisatie met betrekking op PDS's.

4.1 HET SPEELVELD

De relevantie van PDS's is wereldwijd, maar niet verrassend wordt vroege adoptie verwacht in landen met een hoge mate van digitale volwassenheid zoals Scandinavië, Nederland en de Verenigde Staten. Deze technologie staat boven verschillen in demografie, maar vereist wel enige mediawijsheid van de gebruiker. De universaliteit van PDS's wordt weerspiegeld in de huidige initiatieven; er is nu een gefragmenteerd landschap zonder dominante spelers. Er zijn al relatief veel vroege initiatieven, maar nog geen gevestigde merken, en daarmee ook nog geen dominant verdienmodel of technologisch raamwerk.

Naar verwachting zullen in eerste instantie PDS's voor sectorspecifieke data (bijvoorbeeld een zorgkluis) succesvoller zijn dan algemene of cross-sectorale PDS's. Een volwassen markt wordt verwacht binnen 2 tot 5 jaar. Er is op dit moment nog een relatief lage barrière om in te stappen in de PDS-markt. Zoals gesteld ligt er dan ook grote economische potentie in het openbreken van de markt voor persoonlijke data.

Als verbindende factor hangt een PDS in een ecosysteem van partijen en elementen. Aan de ene kant zijn er data-aanbieders; dit kunnen tal van overheids-, commerciële of andere partijen zijn die persoonlijke data over gebruikers verzamelen, verwerken of beheren. Aan de andere kant zijn er data-afnemers; afhankelijke partijen die toegang willen tot de data van data-aanbieders om diensten te kunnen leveren aan gebruikers of voor eigen doeleinden. Hiertussen bevindt zich de PDS als makelaar van toegangsrechten, waarmee de gebruiker data-afnemers toestemming kan verlenen tot "zijn" data bij data-aanbieders. In de PDS kan zich ook persoonlijke data bevinden, dan is de PDS zelf een data-aanbieder. Tussen de PDS en data-aanbieder, respectievelijk data-afnemer, dient dus een interface te zijn geïmplementeerd die transacties faciliteert. Tussen de gebruiker en de PDS is dit in veel gevallen een grafische interface. Het ecosysteem is hieronder weergegeven.



Figuur 13: het ecosysteem van de Personal Data Store in relatie tot andere trends (bron: WEF 2013)

PDS's zijn gerelateerd aan een aantal andere bestaande of verwachte trends. Dit geldt met name voor het *internet of things*, omdat dit een relevante toename in het aanbod aan data belooft. Aan de andere kant doen big-, fast- en smart data de vraag naar data toenemen. PDS's ondersteunen smart technologie; context-afhankelijke automatisering van persoonlijke informatie kan worden gebruikt om real-time te informeren en corrigeren. De ontwikkelingen op het gebied van digitale identiteiten zijn ook van invloed op PDS's vanwege de spilfunctie die digitale identiteiten hebben in het fungeren van de PDS. Immers moet een gebruiker zich betrouwbaar kunnen identificeren als rechtmatige gebruiker.

Ten slotte ligt de PDS in lijn met het *semantic web* en *software defined anything* omdat het een sleutelfunctie in digitale transacties, namelijk het regelen van toegang tot data, centraliseert. Op zijn beurt vereist het doel van PDS's, namelijk de efficiëntie van al je data op één plaats, standaardisatie en mapping. Het semantische web (het formaliseren van data om één holistisch interoperabel web te creëren) draagt hieraan bij, zoals bijvoorbeeld de OWL-taal om nieuwe data te mappen op bestaande data.

4.2 INSPIRERENDE VOORBEELDEN

De markt voor PDS's is gefragmenteerd: er zijn nog geen dominante spelers, maar wel heel veel initiatieven (40+). Enkele tot de verbeelding sprekende voorbeelden zullen hier nader worden beschouwd. De status van deze projecten varieert.

Het eerste concept voor een PDS stamt nog van voor de digitalisering. In 1945 had Vannevar Bush al een idee voor een individu-centrisch data archief: Memex. Dit extern geheugen was gebaseerd op het menselijk brein. Het moest vooral makkelijk zijn om gegevens op te slaan en op te vragen. Daarom zouden individuen allerlei apparaten op zich dragen, waaronder een camera, en met gebaren hun informatie opvragen.

Figuur 13: de Memex

Mydex (Verenigd Koninkrijk)

Mydex is een Britse social enterprise die het sinds 2007 veiliger en makkelijker maakt voor individuen om persoonlijke data te beheren, maken en hergebruiken op een effectieve en veilige manier. Het is een voortzetting van het Midata traject van de Britse overheid. Het Midata traject beoogde de controle over persoonlijke informatie terug te geven aan burgers, waaronder het recht om persoonlijke data terug te trekken. Daarnaast streefde het naar inzicht in relaties tot data. Banken, energiemaatschappijen en mobiele telefonie-aanbieders geven volgens de regels van het Midata traject klanten toegang tot hun persoonlijke gegevens. Overigens heeft de Britse overheid van tevoren gedreigd de beoogde effecten bij wet af te dwingen. In Mydex wordt persoonlijke data door de gebruiker en toegestane organisaties aangemaakt in de PDS en

wanneer de gebruiker het wenst kan hij deze de data delen met organisaties. Daarnaast kunnen er 'proofs of claims', of officiële documenten in worden opgeslagen, zoals een paspoort. Bovendien biedt Mydex de functie om je eigen persoonlijke data te analyseren. Ten slotte is Mydex ook een platform waarop middels API's nieuwe applicaties kunnen worden gebouwd. Voor meer informatie zie deze video.

ProjectVRM (Verenigde Staten)

ProjectVRM (VRM staat voor Vendor Relationship Management, dus voor relaties met aanbieders onderhouden) is een ontwikkelings- en onderzoeksproject van het Berkman Center for Internet & Society aan de Harvard Universiteit en heeft twee doelen:

1. Het stimuleren van de ontwikkeling van tools waardoor individuen controle krijgen over de relaties die ze hebben met organisaties – vooral gericht op commerciële markten.
2. Het stimuleren van onderzoek naar 'Vendor Relationship Management'-gerelateerde theorieën, het gebruik van VRM tools en effecten van adoptie.

Intussen is er een community ontstaan die naast deelnemers in ProjectVRM bestaat uit andere ontwikkelingsprojecten en allerlei organisaties, verenigingen en individuen.

Qiy (Nederland)

De Qiy Foundation streeft ernaar dat iedereen zijn eigen persoonlijke plek op het internet krijgt: een Qiy Domein. Vanuit dit individuele Qiy Domein heeft de consument niet alleen toegang tot zijn of haar data waarover aangesloten partijen beschikken (zoals banken, overheden en scholen); hij of zij bepaalt ook zelf met wie deze informatie gedeeld mag worden. Belangrijk is dat Qiy niet een software-dienst of platform is, maar een trust-framework. Een trust-framework is een geheel van afspraken en principes dat wordt beheerd door aangewezen partijen, en technisch is ingebed in toepassingen. Voor meer informatie zie deze video. DigitalMe is een PDS gebaseerd op Qiy. De verwachting is dat er in de nabije toekomst ook andere omgevingen dan DigitalMe komen gebaseerd op het Qiy framework.

OpenPDS (Verenigde Staten)

OpenPDS is een door MIT ontwikkelde open-source architectuur voor PDS-toepassingen. Open source betekent dat de software code voor iedereen beschikbaar is en zonder beperking mag worden hergebruikt. OpenPDS volgt aanbevelingen van het WEF, de US NSTIC en US Consumer Privacy Bill of Rights. Het stelt gebruikers in staat om hun data te verzamelen en op te slaan, en fijnmazige toegang te geven in de Cloud. OpenPDS verspreidt alleen doelgebonden reeds samengestelde en verwerkte data, en beschermt dus de privacy van gebruikers door alleen anonieme antwoorden in plaats van ruwe data te communiceren. Een mechanisme om applicaties van derden te installeren in een gebruikers PDS beperkt privacy-gevoelige dataverwerking tot de PDS. OpenPDS kan ook data aggregeren voor groepen zonder gevoelige informatie te delen met derden. MIT en Denmark Technical University draaien pilots voor een open architectuur gebaseerd op OpenPDS.

DataPlaza (Nederland)

DataPlaza biedt een platform waarop iedereen achter een beveiligd portaal zijn digitale dossier kan bewaren, en klant en kantoor informatie kunnen uitwisselen. Bovendien kan iedereen kosteloos een digitale kluis aanmaken om zaken als inlogcodes, pincodes en documenten online te bewaren. Ook kunnen notarissen diensten verlenen via DataPlaza, denk hierbij bijvoorbeeld aan een Digitale Erfenis. Een notaris is ook een betrouwbare bron van identiteitsverificatie, zoals zij dat nu ook doen voor notariële aktes. De notaris biedt rechtszekerheid, een landelijke dekking en ziet jaarlijks 1 miljoen bezoekers. Data van of over een consument kan door of onder toezicht van een notaris worden ingevoerd. Met toestemming van de consument (of firma) kunnen derden van deze data gebruik maken. Hoewel het gratis is voor de klant, kost het een kantoor € 1,49 per dossier. Van Brug Software is sinds januari 2014 actief met DataPlaza, en is op 1 april 2015 overgenomen door Total Specific Solutions (TSS). Nu is DataPlaza nog een digitaal notarisdossier, maar de visie is dit uit te breiden naar data-uitwisseling, een digitale kluis, diensten voor de digitale erfenis, en een digitale identiteit in de vorm van NotarisId.

DataCoup (Verenigde Staten)

In 2012 werd deze start-up gesticht door Matt Hogan uit New York City. DataCoup voorziet een marktplaats waar individuen hun persoonlijke data, zoals sociale media activiteit of creditcard- transacties, kunnen verhandelen tegen een maandelijkse beloning tot $8. Nadat een klant heeft geselecteerd welke data hij/zij zou willen verhandelen en met wie, laat DataCoup zien wat de waarde van die data is. Deze data wordt dan gecombineerd met de data van andere DataCoup gebruikers, geanonimiseerd, en geaggregeerd tot algemene datasets. DataCoup verkoopt deze datasets aan afnemers als data-makelaars, adverteerders en marketeers. De gebruikers ontvangen hiervoor in ruil een maandelijkse beloning die zij kunnen verzilveren in DataCoup. In 2014 deed DataCoup een trial waar zo'n 1500 mensen aan meededen die gemiddeld iets minder dan $5 verdienden aan hun persoonlijke data. In de toekomst wil DataCoup ook andere data verhandelen, zoals van FitBit, de draagbare fitness meter, en zoekgedrag op internet. Momenteel is DataCoup alleen op de Amerikaanse markt actief. DataCoup maakte een interessante videoserie over persoonlijke data, te zien op http://pd-16.com/.

Personal.com (Verenigde Staten)

Deze online dienst werd gesticht in 2009, en komt ook als mobiele app. In dit schoolvoorbeeld van een PDS kunnen gebruikers al hun persoonlijke gegevens opslaan, zodat deze niet elke keer opnieuw hoeven te worden opgezocht. Vanuit deze online Cloud-dienst kun je de gegevens vervolgens delen met allerlei partijen. Personal.com biedt diensten voor een persoonlijke Cloud, een veilige datakluis, het automatisch invullen van online formulieren, en een online notitieblok. Sinds 2013 is Personal.com niet langer gratis, en zijn zij een partnership aangegaan met FileThis, de online veilige brievenbus en dossierkast voor al je documenten.

Blue Button (VS)

In de VS is er een initiatief, gestart in 2010, dat het voor patiënten eenvoudig mogelijk maar om hun medische gegevens elektronisch op te halen. Dat initiatief heet Blue Button en is genoemd naar een duidelijk herkenbare blauwe download-knop op de website van je zorgaanbieder. Met die knop kun je diverse informatie ophalen over je medische dossier, behandelingen, medicatie etc.

Blue Button is begonnen in 2010 bij de Amerikaanse Veterans Administration en werd daarna uitgebreid naar de overheidsprogramma's Medicare en Medicaid. Inmiddels zijn ook private partijen aangesloten. Het Blue Button initiatief lijkt effectief (Nictiz, 2015): Uit een onderzoek onder gebruikers van het webportaal van het Department of Veteran Affairs blijkt dat een derde van de ondervraagden gebruik maakt van Blue Button, waarvan 73 % vond dat het hen hielp om hun medische historie beter te begrijpen. Een vijfde van de gebruikers deelde de informatie met zorgaanbieders buiten Veteran Affairs.

De adoptie van Blue Button in Nederland is nog beperkt. Eind 2015 worden de eerste diensten op basis hiervan verwacht.

Philips health vault (Internationaal)

Het HealthSuite digital platform is een samenwerking tussen Philips en Salesforce.com. HealthSuite is een open, cloud-based platform, die klinische en andere data van verschillende apparaten en bronnen verzamelt, samenstelt en analyseert. Zorgverleners en de patiënt hebben toegang tot deze persoonlijke, medische data. Voor zorgverleners is er ook data beschikbaar over de hele populaties. Zorgverleners kunnen patiënten monitoren wanneer zij thuis zijn en kunnen daarmee de zorg aanpassen als het nodig is. HealthSuite is ontwikkeld als een open eco-systeem voor derde partijen (app ontwikkelaars). Toegankelijk door een publieke API, is dit platform schaalbaar, en kan het platform worden gebruikt voor applicaties van derden en applicaties van Philips.

Verder heeft het ingebouwde privacy en data beveiliging. Het Platform wordt aangeboden als een “Platform-as-a-Service” (pay per use).

Poliskluis

De Poliskluis is een initiatief van de verzekeraars om tot een online platform te komen dat verzekerden een integraal overzicht moet bieden van al zijn of haar polisgegevens, vergelijkbaar met zaken als het pensioenoverzicht waarin de opgebouwde pensioenrechten zijn in te zien. De Poliskluis is er nog niet, maar moet in 2016 gereedkomen om verzekeraars aan te sluiten. Het Verbond van Verzekeraars is in 2014 met dit initiatief begonnen. Realisatie hangt mede af van de beschikbaarheid van een universeel authenticatiemechanisme voor consumenten, zoals het beoogde Indensys of BankID.

MijnOverheid

MijnOverheid is een combinatie van digitale post (BerichtenBox), diensten voor lopende zaken tussen burger en overheid, en inzicht in persoonlijke gegevens; en in die zin dus een Personal Data Store van de Nederlandse overheid. Denk bij deze gegevens aan data over financiën, werk en loopbaan, of zorg en gezondheid. Deze data stamt uit de databanken van bijvoorbeeld de basisregistratie persoonsgegevens (BRP), het Kadaster, de Rijksdienst voor het Wegverkeer, gemeenten, of de Belastingdienst, en zijn via een webservice gekoppeld aan MijnOverheid. Daarnaast zijn een aantal andere PDS’s via een hyperlink toegankelijk vanuit MijnOverheid, zoals het donorregister; de mijnomgevingen van DUO, de SVB, het pensioenregister, en de Belastingdienst (mijntoeslagen.nl); en het klantdossier van Werk & Inkomen.

Je logt in op MijnOverheid met DigiD. MijnOverheid wordt maandelijks zo’n 200.000 tot 450.000 maal geraadpleegd. Het is gereed voor 13 miljoen gebruikers en 800.000 berichten via de BerichtenBox. Vanaf oktober 2015 is MijnOverheid verplicht voor alle Nederlanders vanaf 14 jaar. De Belastingdienst is dan ook verplicht dit te gebruiken voor elektronisch berichtenverkeer. Nu is de focus vooral op de BerichtenBox, maar het zal worden doorontwikkeld met nieuwe functionaliteiten (een digitale kluis, het voorzien in transacties) en kanalen (apps). Ook wil de overheid toe naar co-creatie met MijnOverheid, het zou zelfs een platform kunnen worden voor inspraak van burgers.

4.3 WET EN REGELGEVING

Aanbieders van PDS’s moeten zich natuurlijk aan de Wet houden; in Nederland is de WBP (wet bescherming persoonsgegevens) het meest relevant in deze context, alsmede de Europese opvolger, de Data Protection Directive 95/46/EC. Maar wetgeving is ook een belangrijke driver voor PDS’s. Overheden oefenen steeds grotere druk uit op organisaties om transparant te zijn over de verwerking van persoonlijke informatie en dreigen met wetgeving. Dit zorgt ervoor dat er steeds transparanter met gegevens om wordt gegaan.

Juridisch gezien is de WBP van toepassing op Nederland en data die bewaard wordt in Nederland. Echter worden de gegevens van de populaire social media, o.a. Facebook, bewaard buiten Nederlandse grenzen. Dit betekend dat de WBP geen grip heeft op deze platformen en de gebruikers dan ook geen bescherming kan bieden. Zij hoeven alleen rekening te houden met de lokaal geldende regels, die anders kunnen zijn dan de WBP.

> De WBP samengevat is gericht op het bieden van waarborgen dat *bij verwerking van persoonsgegevens de juiste persoonsgegevens, voor het juiste doel, op de juiste gronden, voor de juiste mensen op het juiste tijdstip beschikbaar zijn*. De WBP stelt daarbij de volgende uitgangspunten/privacy beginselen:

1. Transparantie	De betrokkene moet voorafgaand aan de (eerste) registratie op de hoogte worden gesteld van de identiteit van de organisatie en het doel waarvoor de gegevens worden verwerkt.
2. Doelbinding	De verzamelde persoonsgegevens worden alleen verder verwerkt als dit verenigbaar is met het doel waarvoor ze zijn verkregen.
3. Rechtmatige grondslag	De Wbp geeft limitatief aan in welke gevallen persoonsgegevens mogen worden verwerkt. Voor gevoelige gegevens - de bijzondere gegevens als bedoeld in de Wbp – geldt dat verwerking onrechtmatig is tenzij aan specifieke voorwaarden is voldaan.
4. Kwaliteit	Voor het doel behoren de persoonsgegevens toereikend, terzake dienend en niet bovenmatig te zijn.
5. Rechten betrokkenen	De betrokkene heeft recht op inzage, verbetering, aanvulling, verwijdering of afscherming van diens persoonsgegevens.
6. Beveiliging	De verantwoordelijke treft passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
7. Verstrekking aan niet EU-landen	Doorgifte van persoonsgegevens aan landen buiten de EU is niet toegestaan als er geen vergelijkbaar privacyregime heerst.

Figuur 14: Privacy beginselen van de WBP

In Nederland diende kamerlid Omtzigt in 2011 een motie in om in de Wet op te nemen dat burgers hun medisch dossier ook elektronisch moeten kunnen inzien (motie Omtzigt 27 529, nr. 70). Deze motie werd door de Tweede Kamer aangenomen, evenals de hierop volgende wetswijziging (33509, nr 26), en is op het moment van schrijven in behandeling door de Eerste Kamer. Deze wetswijziging werd overigens op verschillende punten kritisch beoordeeld door onder andere Vrijbit, KDVP, VPHuisartsen en Privacy First.

Vanuit de Europese Commissie zijn inmiddels verdere stappen gezet om de rechten omtrent privacy te versterken met de Algemene Verordening gegevensbescherming (AVG) (Informatie, 2015). Met het oog op economische groei is het namelijk van belang dat personen vertrouwen hebben in online diensten. Volgens de Europese Commissie zorgen online diensten namelijk voor een groot deel van de groei in productiviteit. Echter is dit vertrouwen nog niet gewaarborgd, daarom wordt er moeite gedaan het tij te keren. Op 25 januari 2012 is vanuit dit oogpunt een nieuw voorstel gedaan voor regulering van data. Dit voorstel is op 12 maart 2014 goedgekeurd. Zoals de Europese commissie het zelf stelt: *"The European Commission has adopted proposals for updating data protection rules to meet the challenges of the digital age. In particular, the proposals will strengthen protection of your personal data online."*

Maar wat betekent het aannemen van deze nieuwe regulering vanuit de EU? In een rapport van de Europese commissie wordt duidelijk dat het om de volgende punten gaat:

- Versterken van het 'recht te worden vergeten'.
- Garanderen van gemakkelijke toegang tot eigen data.
- Het recht om data vrij te verplaatsen van de ene dienst naar de andere.
- Verzekeren dat personen expliciet toestemming moeten geven wanneer dit nodig is voor bepaalde manier van dataverwerking.
- Striktere regels voor internationaal gegevenskeer.
- Meer verantwoordelijkheid voor degenen die data verwerken door: een data officer voor organisaties met >250 werknemers, privacy is standaard (bijvoorbeeld van een account), meldplicht voor datalekken (binnen 24 uur) en privacy in het design.

De implementatie ervan laat echter op zich wachten en zou sterk verzwakt kunnen worden door compromissen die het bedrijfsbelang moeten veiligstellen. De definitieve tekst wordt medio 2016 verwacht, onder het Nederlandse voorzitterschap van de EU. Databescherming moet veranderen, omdat zij nu niet de rol van de gebruiker als actieve beheerder van zijn eigen persoonlijke data erkent, wel als eigenaar (Informatie, 2015). De eindverantwoordelijkheid ligt bij de bewerkende partij. Wat gebeurt er als ik naast eigenaar ook de bewerker word van mijn eigen gegevens? Ben ik dat ook in alle opzichten verantwoordelijk? Belangrijk is wel dat zodra de regulering in de EU is aangenomen, ze direct geldig is in alle lidstaten en dus niet nationaal hoeft te worden geïmplementeerd. Er ontstaat dan dus direct een heldere situatie in de gehele Europese Unie!

Gezien de toenemende wettelijke eisen ten aanzien van persoonlijke informatie, groeien dus de kansen voor PDS's. Daarnaast zijn mensen eerder bereid om gegevens te delen, wanneer de wet erom vraagt. Een bepaalde verplichting stellen rondom het gebruik van een PDS zou daarmee een groot deel van de mensen over de streep trekken om een dergelijke dienst te gebruiken. Aan de andere kant, eigenaarschap van persoonlijke data is bepalend voor het functioneren van PDS's, maar vaak onduidelijk. De (wettelijke) verantwoordelijkheid voor PDS's moet worden vastgesteld, met name bij een gedistribueerde architectuur.

Wetgeving in finance

Als er een trend is die zijn stempel heeft gezet op wetgeving in de financiële dienstverlening, dan is het wel die van grotere transparantie. Onduidelijke kostenstructuren bij producten leidden tot neologismen als "woekerpolis", beruchte kleine lettertjes deden vertrouwen teniet, gemaskeerde risicoprofielen lagen aan de basis van de bankencrisis. Onvoldoende transparantie speelde in al deze situaties een rol.

De standaard reactie van de politiek bij misstanden is meer regels. En die zijn er dan ook gekomen. De wet op het financieel toezicht, WFT, uit 2007 verving acht oudere toezichtswetten. De AFM werd belast met het toezicht op het gedrag van banken en verzekeraars. In Europa werd in 2007 de Markets in Financial Instruments Directive (MiFID) geïntroduceerd die onder meer "Het bevorderen van eerlijke, transparante, efficiënte en geïntegreerde financiële markten" als doelstelling heeft. In Nederland is sinds 1 januari 2014 een algemene zorgplicht toegevoegd in de WFT. Een zorgplicht bestond er al, zowel in maatschappelijke als in juridische zin. Dit betekent dat een financieel dienstverlener zich "in ieder geval onthoudt van enig handelen of nalaten van dat kennelijk nadelige gevolgen voor de consument kan veroorzaken." Niet wijzen op een voordeliger product is een voorbeeld van nalaten, maar ook in onvoldoende mate signaleren dat er ontwikkelingen zijn die bijvoorbeeld het rendement van een aanvullend pensioen in gevaar brengen. Een enorme impact in de branche. Voor een dienstverlener geldt dus zeker niet meer "u vraagt wij draaien": je bent verplicht de (potentiële) klant te behoeden voor onverstandige keuzes. En de onderbouwing daarvan moet je vijf jaar bewaren, zo is het voorstel.

In dat opzicht kan een PDS een mooie rol vervullen om de dialoog tussen financieel dienstverlener en klant vast te leggen: niet alleen welke gegevens gebruikt zijn, maar ook welke adviezen zijn uitgebracht en welke transacties zijn uitgevoerd. Voor beide partijen inzichtelijk, transparant en duurzaam opgeslagen.

Een andere ontwikkeling is die van de Payment Service Directive 2 (PSD2), die gericht is op het versterken van de concurrentie in het betalingsverkeer te vergroten en nieuwe toetreders kansen te geven, geïnitieerd door de Europese Commissie in 2013 (Spellier, 2015). In de PSD2 worden traditionele financiële instellingen onderscheiden (account servicing payment service providers, AS PSP) en zijn er daarnaast 'payment initiation service providers' (PISP) en 'account information service providers' (AISP). Die laatste twee hebben geen bankvergunning (nodig). De belangrijkste verandering die PSD2 bewerkstelligt is dat de AISP toegang kan krijgen tot de rekeninginformatie, als de eigenaar van de rekening daar toestemming voor geeft ('access to account', XS2A). Ook mogen payment initiation service providers betalingen doen in opdracht van een rekeninghouder. Ook zijn de maximale kosten voor een interbancaire transactie vastgesteld.

Het gevolg van deze maatregelen is dat er een interessant speelveld ontstaat voor intermediairs op financieel gebied. Die intermediairs kunnen voor consumenten (of bedrijven) informatie over meerdere rekeningen integreren, zorgen voor een optimale rente of opbrengst, noem maar op. Typisch een rol zoals die past bij het beeld van een Personal Data Store zoals geschetst.

De directive is inmiddels aangenomen in oktober 2015,[1] maar moet nog nationaal worden geïmplementeerd. Lidstaten hebben daar in principe twee jaar de tijd voor. Ook zullen de banken ervoor moeten zorgen dat er een infrastructuur komt om toegang te krijgen tot de rekeninggegevens, dus dat XS2A mogelijk wordt. De ervaring leert dat banken daar niet heel snel in zijn, gegeven de gevoeligheid van de deze toegang, zowel wat betreft concurrentieoverwegingen als wat betreft technologie en privacy. Voordat de markt dus echt in kan zetten op deze mogelijkheden zitten we als snel in 2018…

Dat een dergelijke ontwikkeling welkom is in de markt, blijkt onder meer uit de problemen die AFAS Personal had in 2014. Dit pakket maakte het mogelijk om namens de klant in te loggen bij eigen bank om zo automatisch de bankmutaties in te lezen; een logische functie, zou je zeggen. ING heeft deze mogelijkheid echter met succes bij de rechter bestreden en AFAS heeft de koppeling moeten verwijderen, waarbij ze een beroep deed op de leveringsvoorwaarden waar in staat dat je inloggegevens niet mag delen.

Daar waar banken misschien genegen zijn om de PSD2 te zien als de zoveelste regulering om het leven van banken moeilijker te maken, is het bij uitstek ook een kans: ook banken en verzekeraars kunnen de rol van PSIP en AISP nemen in de richting van andere banken en zo een totaalomgeving bieden voor bankzaken. De bank die dat het snelst, best en meest klantvriendelijk doet kan een sterk concurrentievoordeel zijn. Dat kan een van de bestaande banken zijn, maar net zo goed een disruptieve nieuwe bank, zoals Bunq.[2]

[1] Zie http://ec.europa.eu/finance/payments/framework/index_en.htm

[2] http://fd.nl/ondernemen/1120680/banken-maken-dingen-die-de-klanten-niet-willen

5 PDS in specifieke contexten

Personal Data Stores als concept zijn heel generiek. In die genericiteit zit kracht, maar zeker ook een valkuil. Onderzoek naar wat Nederlanders denken van dergelijke concepten laten sterk zien dat zo'n concept nog onbekend is (zie hoofdstuk 7). Je mag verwachten dat toepassingen in specifieke sectoren, met een duidelijker afgebakend doel, eerder in de markt gaan doorbreken. Maar wat loopt er dan in verschillende sectoren en wat is de status ervan? En hoe kansrijk zijn die initiatieven? We kijken naar de ontwikkelingen in de zorg, verzekeringen en de overheid. Ook geven we aan op welke kwaliteitsaspecten in die sectoren een PDS een toegevoegde waarde kan leveren.

5.1 HET PERSOONLIJK GEZONDHEIDSDOSSIER

De rol van de zorgconsument verandert in toenemende mate van passieve patiënt naar een actieve agent. Zorgconsumenten willen en kunnen steeds meer invloed uitoefenen op "hun" zorg, mede door technologische ontwikkelingen. Ze zijn beter geïnformeerd door de grote hoeveelheid medische informatie die via het internet beschikbaar is. Een groeiende groep maakt ook graag gebruik van slimme apparaten om de eigen gezondheid te bewaken. Neem het voorbeeld van de Scanadu Scout gezondheidsmonitor: een apparaatje dat je vitale functies meet en doorgeeft aan een app op je smartphone.

Om de zorg optimaal te laten verlopen is het uitwisselen van (medische) informatie van cruciaal belang. Tussen de betrokkenen in de zorg vindt al een veelvoud aan gegevens-uitwisselingen plaats, vaak zonder dat de zorgconsument hier zicht op heeft. Het Persoonlijk Gezondheidsdossier (PGD) is een ICT-oplossing welke tot doel heeft deze data-uitwisseling inzichtelijk te maken voor en de zeggenschap hierover te beleggen bij de zorgconsument. De patiëntenfederatie NPCF definieert het PGD als volgt:

> *"Een universeel toegankelijk, voor leken begrijpelijk, gebruiksvriendelijk en levenslang hulpmiddel om relevante gezondheidsinformatie te verzamelen, te beheren en te delen, en om regie te kunnen nemen over gezondheid en zorg en zelfmanagement te ondersteunen via gestandaardiseerde gegevensverzamelingen voor gezondheidsinformatie en geïntegreerde digitale zorgdiensten."(NPCF, 2013)*

Het PGD wordt beheerd door de patiënt of diens wettelijke vertegenwoordiger, en is op een zodanige wijze beveiligd dat de vertrouwelijkheid van de gegevens en privacy van de gebruiker worden beschermd. De databronnen die worden verenigd in een PGD kunnen heel verschillend zijn. In hoofdlijnen zijn ze in te delen in: medische bronnen afkomstig van zorgverleners, informatie opgegeven door de gebruiker zelf, of data van andere bronnen (waaronder smartphone-apps). Naast het ontsluiten van gegevens kan het PGD ook diensten aanbieden ter ondersteuning van het zorgproces en zelfmanagement. Een dergelijk instrument gaat over meer dan alleen medische gegevens; het gaat namelijk ook over gezondheid (denk bijvoorbeeld aan preventie van ziekte) en interactie met het zorgnetwerk.

PGD's zijn relevant omdat zorgconsumenten steeds meer betrokken zijn bij hun eigen zorg en gezondheid. Maar de zorg is ook complexer geworden: rond patiënten is een heel zorgnetwerk ontstaan van zorgverleners, mantelzorgers en andere betrokkenen die allemaal moeten worden geïnformeerd. Een PGD kan bovendien de risico's van verkeerde informatie beperken; gegevens zijn soms verouderd, incompleet of onjuist, en door actief beheer van de zorgconsument wordt de kwaliteit van de informatie gewaarborgd. Ook voorziet een PGD in het integreren van allerlei losstaande digitale diensten en databronnen. Voor de zorgconsument en zorgverlener zijn vooral gemak, veiligheid en efficiëntie belangrijk.

Bekende voorbeelden van PGD's zijn Apple Health, Microsoft Healthvault en Dossia. De Nationale Patiënten Consumenten Federatie (NPFC) deed onderzoek naar het gebruik van PGD's (NPCF, 2015). Hieruit bleek dat het gebruik van PGD's beperkt is; in 2015 betrof dit slechts 9% van hun achterban, vergeleken bij 7% in 2013. De PGD's bevatten voornamelijk documenten van zorgverleners, en worden door gebruikers aangewend om overzicht te houden. Motivatie voor het gebruik van PGD's is een chronische aandoening, als men bemerkt dat zorgverleners niet alles van elkaar weten, of als zorgverleners wijzen op PGD's. Gebruikers zien vooral meerwaarde in het terugdringen van fouten, het afstemmen van medicatie, en het aanvullen van gegevens. Bovendien vinden ze het een goed hulpmiddel om hun eigen gezondheid te monitoren. Hoewel gebruikers

bereid zijn voor een PGD te betalen, vindt ruim de helft dat dit vanuit de zorgverzekering vergoed moet worden.

Relatie tot andere zorgsystemen

De meeste zorgverleners en zorginstellingen maken gebruik van een elektronisch patiëntendossier (EPD) om het medisch dossier van hun patiënten bij te houden. Denk aan huisartsen, apothekers, zorggroepen, ziekenhuizen en verpleegkundigen. Het PGD en EPD kunnen elkaar versterken, maar niet vervangen. Zo is het PGD juridisch gezien geen dossier dat valt onder de dossierplicht van de zorgverlener. Het moet worden gezien als een aanvulling op het EPD, dat de patiënt vrijwillig kan bijhouden. Vanuit het PGD zou informatie die niet beschikbaar is via het EPD, zoals het daadwerkelijk medicijngebruik, kunnen worden gedeeld met de zorgverlener.

Wanneer patiënten hiervoor toestemming hebben gegeven, kunnen zorgverleners via het Landelijk Schakelpunt (LSP) medische gegevens bij andere zorgverleners op een veilige en betrouwbare manier inzien, uitsluitend wanneer dit voor de behandeling noodzakelijk is. In het LSP staan het Burger Service Nummer (BSN) en welke aangesloten zorgverleners een bijbehorend medisch dossier beschikbaar hebben. Momenteel zijn alleen huisartsenpraktijken (89%), apothekers (94%), huisartsenposten (96%) en ziekenhuizen (81%) aangesloten op het LSP. Het medisch dossier blijft de verantwoordelijkheid van de zorgverlener en staat niet in het LSP. Het LSP heeft een mijn-omgeving waarop burgers kunnen inloggen met DigiD om een inzage-overzicht te bekijken van welke zorgverleners welke medische gegevens hebben opgevraagd. Ook biedt de mijn-omgeving gebruikers de mogelijkheid om zich te abonneren op een melding bij inzage van gegevens. Zorgverleners kunnen alleen een vereiste selectie van persoonlijke en medische gegevens inzien. Bovendien kan men in overleg met zorgverleners vragen bepaalde gegevens af te schermen. In wezen fungeert het LSP als een PDS voor het inzien en delen van medische gegevens, maar is hierin beperkt. Zo kunnen gebruikers in het LSP nog niet de eigen medische dossiers inzien. Door verschillende partijen wordt gesproken over een koppeling tussen het Landelijk Schakelpunt en Persoonlijke Gezondsheidsdossiers. Een koppeling met het PGD zou het mogelijk maken om via het LSP de eigen medische informatie in te zien, op te slaan en te kopiëren. Het LSP blijft echter omstreden, vooral om redenen van veiligheid en privacy. Recentelijk presenteerde de Huisartsenkring Amsterdam in samenwerking met de Universiteit van Amsterdam een decentraal alternatief systeem voor het centrale LSP dat een deel van deze zorgen zou kunnen wegnemen.

Veel zorginstellingen beschikken over een patiëntenportaal; een digitaal platform waarop patiënten kunnen communiceren met zorgverleners en informatie kunnen inzien, zoals instructievideo's of een Individueel Zorgplan. Dergelijke portalen zijn vaak gebonden aan een zorginstelling, of in sommige gevallen aan een regio waarbinnen zorgverleners zijn verenigd. Het resultaat is dat een zorgconsument die op verschillende plekken zorg afneemt, te maken heeft met verschillende portalen. Een koppeling met een PGD maakt het mogelijk om informatie uit diverse portalen uit te lezen en te delen met andere zorgaanbieders.

Een noemenswaardige ontwikkeling is het Blue Button initiatief, een idee uit Amerika van de nationale coördinator voor gezondheids-ICT. Blue Button is een open standaard voor een knop op een website van een zorgverlener die patiënten in staat stelt hun medisch dossier te downloaden, om dit vervolgens te bekijken en eventueel te delen met anderen. Het inlezen en delen van deze informatie zou ook via een PGD kunnen verlopen. Inmiddels is de Blue Button in Amerika erg populair en bieden steeds meer zorgpartijen deze optie, zijn er apps ontwikkeld op basis van de Blue Button, en zijn er andere industrieën die dit initiatief kopiëren (zoals de Red Button voor onderwijs of de Green Button voor energie).

De uitdagingen

PGD-initiatieven zullen echter pas succes hebben als zij worden gestimuleerd vanuit overheid (en verzekeraars) of door de grote technologie-ontwikkelaars als Apple en Microsoft worden aangeboden. Overheden oefenen steeds grotere druk uit op organisaties om transparant te zijn over de verwerking van persoonlijke informatie en dreigen met wetgeving. In Nederland diende kamerlid Omtzigt in 2011 een motie in om in de Wet op te nemen dat burgers hun medisch dossier ook elektronisch moeten kunnen inzien (motie Omtzigt 27529, nr. 70). Deze motie werd door de Tweede Kamer aangenomen, evenals de hierop volgende wetswijziging (33509, nr. 26), en is op het moment van schrijven in behandeling door de Eerste Kamer. Deze wetswijziging werd overigens op verschillende punten kritisch beoordeeld door onder andere Vrijbit, KDVP, VPHuisartsen en

Privacy First. Naar aanleiding van een deskundigenbijeenkomst op 13 April 2015 is de geplande behandeling van 26 Mei door de Eerste Kamer wegens overweldigende kritiek uitgesteld.

Typisch zal de software voor een Persoonlijk Gezondheidsdossier worden aangeboden als web-gebaseerde applicatie. De technische randvoorwaarden voor een PGD zijn connectiviteit, betrouwbare authenticatie van gebruikers, adequate databeveiliging, en integratie van datasets. Een belangrijke technische uitdaging is standaardisatie van processen, informatie en systemen. Nictiz, het orgaan voor standaardisatie voor IT in de zorg, werkt aan ontwikkelingen op dit gebied.

Er zijn ook een aantal juridische afwegingen, zoals aansprakelijkheid voor en geheimhouding van de inhoud van het PGD. Wanneer een PGD genetische informatie zou bevatten, rijzen er een aantal vragen die voortkomen uit de bijzondere eigenschappen van deze informatie, onder andere omdat genetische informatie ook informatie over familie bevat. Met een PGD verschuift een stukje verantwoordelijkheid naar de zorgconsument. Dit hoeft geen risico te vormen voor het zorgproces zolang de consument voldoende wordt ondersteund, bijvoorbeeld door begrijpelijke taal te gebruiken en uit te leggen welke informatie belangrijk is voor welke behandelaar. Bilaterale communicatie en data-uitwisseling tussen zorgverleners, buiten de patiënt om, zullen blijven bestaan omdat de patiënt niet altijd kan intermediëren en behandelaars vrijuit over de patiënt moeten kunnen praten. Een remmende factor is de discussie over het eigenaarschap van data. Zorginstellingen en verzekeraars voelen zich eigenaar van data; ze spreken van 'company assets'. De consument claimt echter steeds nadrukkelijker "zijn data". Ten slotte zijn er ook nog ethische vraagstukken die een rol spelen: waar mag data wel en niet voor worden gebruikt?

5.2 POLISMAPPEN EN –KLUIZEN

De financiële sector kent al een lange geschiedenis van experimenten met digitale kluizen en mappen. In 2004 introduceerde de ABN AMRO al een digitale kluis, primair er op gericht om documenten veilig op te slaan, tot 1MB (in het totaal) gratis. Dit volgde op initiatieven als "lockertje.nl", opgericht na de vuurwerkramp in Enschede door een betrokken politieman. Dit soort digitale kluizen heeft her en der navolging gekregen, maar is nooit een echt succes geworden.[3] Bijna een jaar na introductie had de digitale kluis van de ABN AMRO pas 4000 aanmeldingen. Voor alle duidelijkheid: Dropbox werd pas opgericht in 2007, dus dit alles speelt jaren voordat document sharing eenvoudig in de markt beschikbaar kwam.

Na dit soort generieke voorzieningen zijn er ook producten geïntroduceerd die specifiekere dienstverlening ondersteunen. Elke bank en verzekeraar heeft zijn eigen mijn-omgeving, waarin transacties kunnen worden afgehandeld en contracten kunnen worden ingezien. Het delen van die gegevens of combineren wordt niet ondersteund. Een uitzondering daarop is het pensioenregister, dat met DigiD kan worden bekeken op MijnPensioenregister.nl dat in 2011 werd geïntroduceerd. Ook zijn er initiatieven in de markt, zoals de Polismap van Voogd&Voogd verzekeringen, die dit aanbiedt aan verzekeringsintermediairs. Hierin worden de verzekeringen van een verzekerde, voor zover ze via Voogd & Voogd lopen, ontsloten en kunnen andere polissen worden bewaard als pdf. Ook kunnen verzekerden hierin zelf mutaties doorgeven.

Het Verbond van Verzekeraars heeft besloten tot een dergelijk initiatief voor de hele markt, de Poliskluis. De Poliskluis moet verzekerden een integraal overzicht bieden van al zijn of haar polisgegevens, vergelijkbaar met zaken als het pensioenoverzicht waarin de opgebouwde pensioenrechten zijn in te zien. De Poliskluis is er nog niet, maar moet in 2016 gereedkomen om verzekeraars aan te sluiten. Het Verbond van Verzekeraars is in 2014 met dit initiatief begonnen. Realisatie hangt mede af van de beschikbaarheid van een universeel authenticatiemechanisme voor consumenten, zoals het beoogde Indensys of BankID. De indentificatie van een consument over verschillende verzekeraars en verzekeringen is nog een belangrijk knelpunt in de realisatie van de Poliskluis.

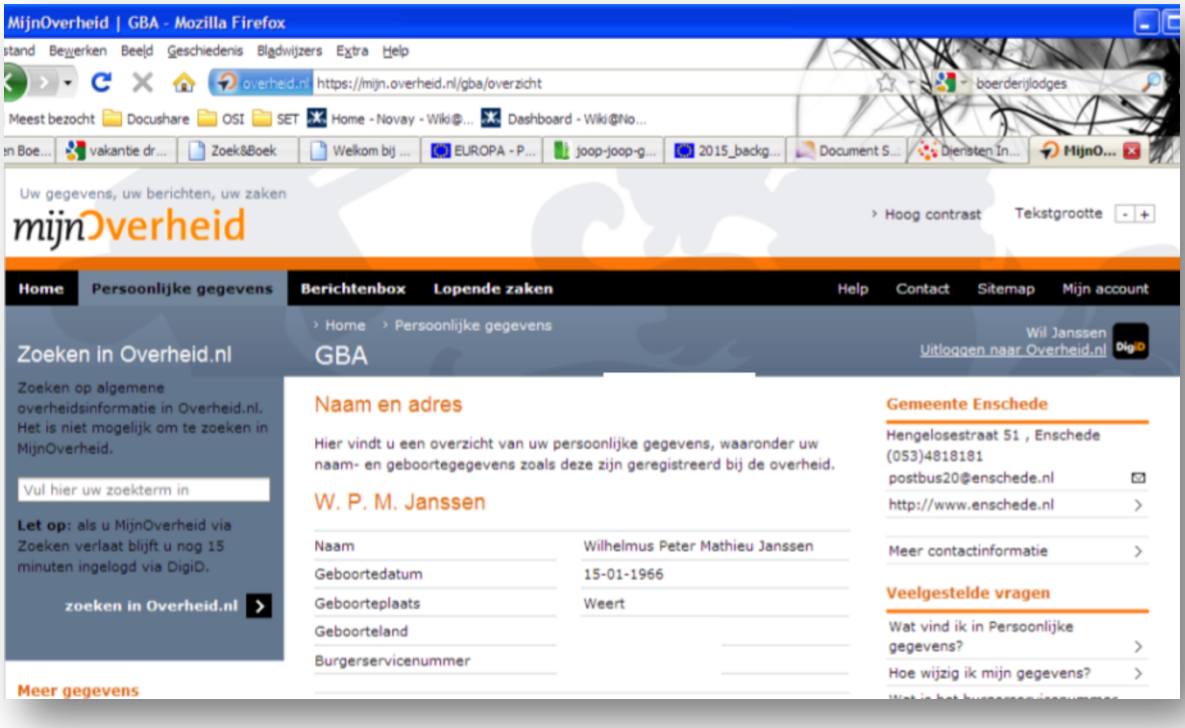
5.3 MIJNOVERHEID EN MIJNGEMEENTE

MijnOverheid is in 2006 ontstaan vanuit een onderzoek door de Manifestgroep naar digitale dienstverlening vanuit de overheid. In opdracht van de Manifestgroep is toen door het toenmalige Telematica Instituut een

[3] Veilig virtueel opgeborgen, NRC, 2 september 2009. Te raadplegen via http://vorige.nrc.nl/economie/article1834812.ece

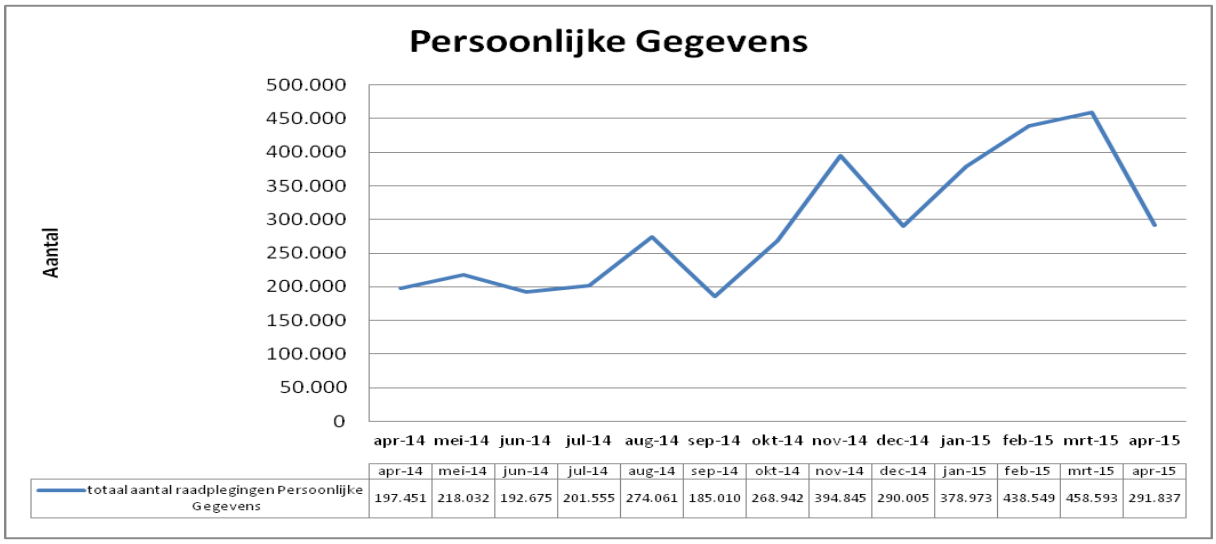
visie ontwikkeld en gevisualiseerd van mogelijkheden voor een e-overheid, het e-dossier. Hierin werd zelf gekeken naar een publiek-private opzet van een dergelijk e-dossier.

Discussies destijds tussen Ministeries (Rijksbrede ICT Agenda, 2005) gaven aan dat het privaat gebruik van publieke infrastructuur zoals DigiD te controversieel was. Vanuit de ontwikkelde visie werd uiteindelijk in twee wegen verder gewerkt, om onderzoek en ontwikkeling naar een publiek-private e-dienstverlening en eerste implementaties van de e-overheid te scheiden. Er ontstond een initiatief vanuit het Ministerie van Binnenlandse Zaken om een integraal portaal voor de overheid te ontwikkelen in de stijl van het E-Dossier. Daartoe werd een werkgroep opgericht die uiteindelijk in het ICTU programma het E-Dossier / Persoonlijke Internet Pagina ontwikkelde. Een grote horde in de lancering van MijnOverheid.nl bleek uiteindelijk niet te liggen bij de technologie of bij de burger: met name de overheid zelf had grote moeite om aan te sluiten op MijnOverheid.nl. Gebrek aan kennis, menskracht en prioriteit speelden daarbij een grote rol. Juist in die tijd kwam een aantal probleemsituaties rondom overheid en ICT naar boven die het inzetten op innovatieve nieuwe diensten tot een moeizaam verhaal maakten. Uiteindelijk heeft dit geleid tot de lancering van MijnOverheid.nl in april 2008.



Figuur 15. MijnOverheid in 2008

Inmiddels is MijnOverheid sterk gegroeid, zowel in aangesloten diensten, beschikbare gegevens, als gebruik. Geregistreerde en te bekijken gegevens zijn de gegevens uit het basisregister personen (NAW), gegevens rond identiteitskaarten, kadaster, WOZ etc. Daarnaast ontsluit MijnOverheid ook de mijn-omgevingen van andere instellingen, zoals DUO, SVB en gemeenten.



Figuur 16. Groei gegevensraadplegingen in MijnOverheid (bron: programma MijnOverheid)

Op dit moment ligt de nadruk op de uitrol van de BerichtenBox als onderdeel van MijnOverheid. Met name de Belastingdienst zet sterk in op elektronisch berichtenverkeer, als vervanging van de blauwe enveloppe. De bedoeling is dat ook andere overheden gebruik gaan maken van de berichtenbox. Wetgeving die deze mogelijkheid verplicht maakt, de Gemeenschappelijk Digitale Infrastructuur, is in de maak in samenwerking tussen de ministeries van economische en binnenlandse zaken en wordt in 2016 in concept verwacht.

Met deze ontwikkelingen wordt MijnOverheid voor de ontsluiting van gegevens en de communicatie met de burger een dominant kanaal. Dat wil nog niet zeggen dat MijnOverheid een succes is, vanuit het perspectief van een Personal Data Store. MijnOverheid is primair inzage. Correctie is niet of beperkt mogelijk, delen van gegevens is niet mogelijk en aanvullen met andere gegevens is niet mogelijk, laat staan privaat gebruik. Daarmee staat het nog ver af van de visie zoals die bij het ontstaan in 2004 is neergezet. In 2016 ontstaat er ruimte voor het verrijken van de visie van MijnOverheid in relatie tot overheid.nl, de mijn-omgevingen en mogelijke marktwerking. Nieuwe kansen voor een beweging richting een overheids-PDS met wezenlijke toegevoegde waarde.

5.4 DE KANSEN VOOR PERSONAL DATA STORES IN SECTOREN

De strategie canvas is een grafische weergave van de huidige en potentiele concurrentie omgeving van een organisatie. Deze weergave is kenmerkend voor de ‘blue ocean strategy’: het verder kijken dan de huidige markt door het creëren van nieuwe markten. De strategie canvas heeft twee doelen:

- De huidige toestand van de markt visualiseren; inzicht in de factoren waarop een industrie concurreert en waarin de concurrentie investeert.
- Actief nadenken over de heroriëntering van de focus van een bedrijf; de focus kan verschuiven naar andere factoren.

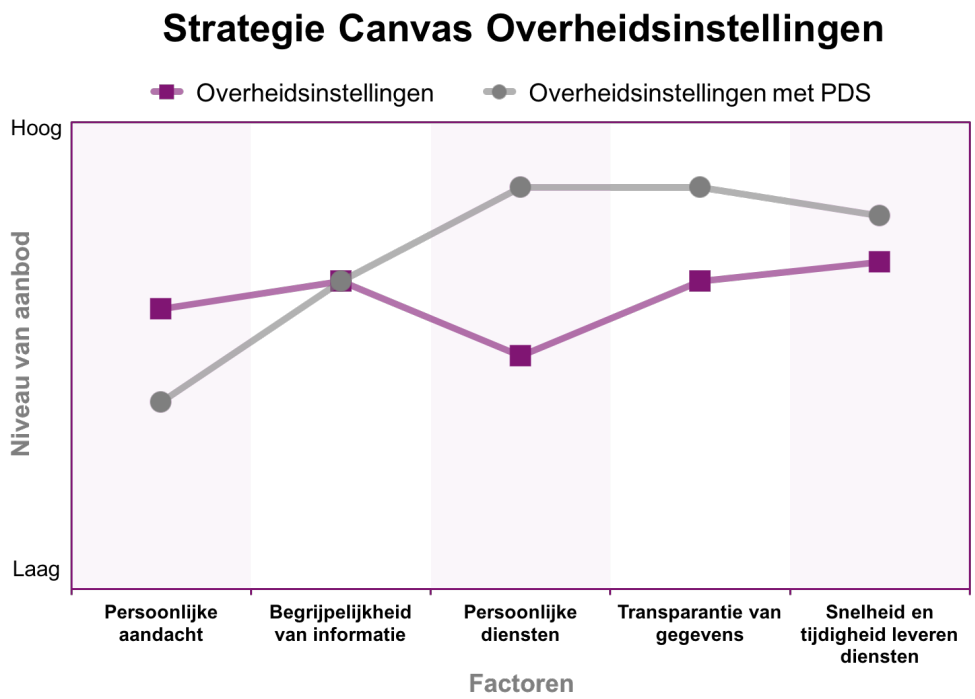
Om een strategie canvas te maken moet er worden bepaald wat de belangrijkste factoren zijn en hoe een organisatie/industrie presteert op deze factoren. De strategie canvas heeft twee assen. Op de horizontale as zijn de factoren weergegeven die bepalend zijn voor een organisatie/industrie; de kenmerken waar de klant belang aan hecht. Op de verticale as wordt het niveau van de factoren weergegeven; dit zijn de prestaties van de kenmerken vanuit het oogpunt van de klant. Met deze informatie wordt de waardecurve van een organisatie/industrie bepaald. De waardecurve is het belangrijkste component van de strategie canvas. Het geeft weer hoe de organisatie/industrie scoort op de factoren bepalend voor de industrie. Aan de hand van deze waardecurve kan er afgelezen worden hoe goed een industrie gemiddeld presteert. Daarnaast kunnen individuele organisaties vergeleken worden met elkaar of met het gemiddelde van de industrie.

In deze analyse worden de belangrijkste factoren voor drie sectoren bepaald: overheid, zorgverzekering en financieel. Elke sector heeft een gemiddelde waardecurve en de impact van een Personal Data Store op deze

waardecurves wordt zichtbaar gemaakt. De factoren voor de drie sectoren zijn bepaald dankzij de input van de consortium leden van Digital We, en informatie uit jaarverslagen en websites. Met deze input is tevens de gemiddelde score van een sector op de factoren vastgesteld, waardoor de gemiddelde waardecurve zichtbaar wordt. Met behulp van een expertgroep, bestaande uit betrokkenen van Digital We vanuit InnoValor, is er bekeken wat de impact van een Personal Data Store is op de waardecurves. Deze impact is weergegeven met een aparte waardecurve. Vervolgens zijn de huidige waardecurves vergeleken met de waardecurves na invoering PDS. Met deze vergelijking wordt de impact van een PDS op een sector beschreven.

Impact op de overheidsinstellingen

De overheid stuurt bewust op kwaliteit (zie, bijvoorbeeld: i&o research, 2014; Desan Research, 2015). Daaruit komen met name Persoonlijke Aandacht, Begrijpelijkheid, Persoonlijke dienstverlening, Transparantie en Snelheid en tijdigheid naar voor als prestatie indicatoren. Zodra de Personal Data Store een rol gaat spelen binnen het netwerk van overheidsinstellingen dan zullen ze het met name beter gaan doen op het leveren van persoonlijke diensten en het bieden van transparantie over gegevens. Tevens zullen er minder fouten worden gemaakt dankzij complete en juiste gegevens, waardoor diensten sneller en op tijd geleverd kunnen worden. In hoeverre de burger de aangeboden informatie begrijpelijk vindt zal niet veranderen door de PDS. Echter, door de automatisering van interactie die dankzij de PDS mogelijk wordt zal de mate van persoonlijke aandacht voor de klant afnemen.



Figuur 17: Strategie canvas van overheidsinstellingen

Persoonlijke aandacht

Een element waar overheidsinstellingen aandacht aan besteden is het geven van persoonlijke aandacht aan klanten om de klanttevredenheid te waarborgen. Een Personal Data Store zal de interactie met de klant verder automatiseren en mogelijk wel personaliseren. Dit kan gedaan worden via het internetkanaal en daarmee in plaats van persoonlijke aandacht komen. Alhoewel er op maat gemaakte diensten geleverd kunnen worden, is er niet meer persoonlijke aandacht.

Begrijpelijkheid van informatie

Overheidsinstellingen verschaffen een veelheid aan informatie aan de burgers. Dat deze informatie duidelijk is voor iedereen spreekt niet voor zich. Overheidsinstanties zijn actief bezig met het verduidelijken van informatie. Er al heel wat verbeterd aan de begrijpelijkheid waardoor de sector boven gemiddeld scoort. Een

Personal Data Store zal zorgen dat gegevens en informatie gemakkelijk ontsloten wordt, maar het zal niets veranderen aan de kwaliteit van deze informatie. Het verduidelijken van informatie zal niet ondersteund worden door de PDS, daarom heeft de PDS geen impact op de begrijpelijkheid van informatie.

Persoonlijke diensten

Het personaliseren van de dienstverlening is voor vele overheidsinstanties een aandachtspunt. Diensten worden immers aan de gehele bevolking beschikbaar gesteld, waardoor een persoonlijke benadering lastig is. Overigens zit er wel verschil tussen de overheidsinstanties. Desalniettemin scoren overheidsinstellingen onder de maat op het aanbieden van persoonlijke diensten. De Personal Data Store maakt het mogelijk om op basis van persoonlijke gegevens een persoonlijk aanbod te doen. Met deze mogelijkheid zal de sector beter persoonlijke diensten aan kunnen bieden.

Transparantie van gegevens

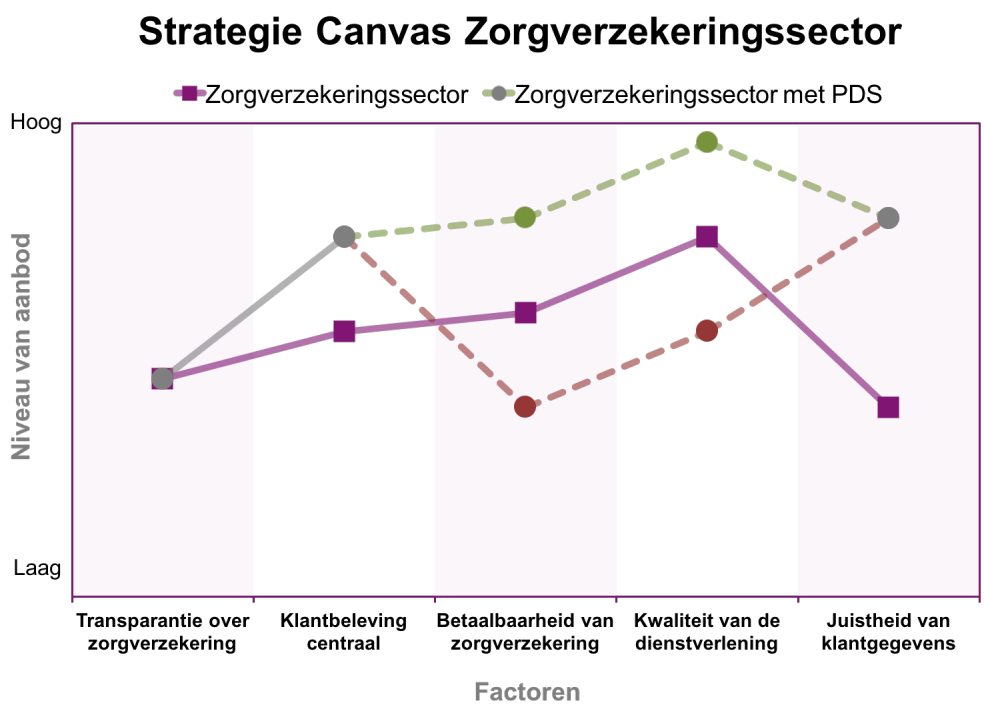
Overheidsinstanties proberen transparanter te zijn over de gegevens die ze over de burgers bezitten. Een belangrijke reden hiervoor is het winnen van het vertrouwen van de burger. Met Mijn Overheid wordt transparantie van gegevens bevorderd, waardoor overheidsinstellingen boven gemiddeld hierop scoren. Mijn Overheid is vooralsnog beperkt in de hoeveelheid aangesloten organisaties, met een PDS moet er een volledig beeld ontstaan van de persoonlijke gegevens. Zo zullen alle overheidsinstellingen worden aangesloten, en zal er meer transparantie van gegevens zijn binnen deze sector.

Snelheid en tijdigheid leveren diensten

De snelheid waarmee overheidsinstellingen reageren op aanvragen en een dienst leveren verschilt per overheidsinstelling. De overheid streeft ernaar om zo spoedig mogelijk de burgers te voorzien van diensten. Overheidsinstellingen scoren dankzij duidelijke doelstellingen boven gemiddeld op deze factor. Een Personal Data Store kan het aantal fouten terugbrengen doordat gegevens meer compleet en juist zijn. De tijd verdaan met het corrigeren van fouten zal afnemen waardoor diensten sneller geleverd kunnen worden.

Impact op de verzekeringssector

Zodra zorgverzekeraars gebruik gaan maken van een Personal Data Store zullen er minder fouten worden gemaakt doordat de gegevens van klanten accurater zijn. De impact van een PDS op de juistheid van gegevens is groot. Het is tevens gemakkelijker om de klantbeleving centraal te stellen dankzij de hoeveelheid gegevens beschikbaar over de klant. Opvallend is dat er voor zorgverzekeraars een aantal scenario's ontstaan. Deze scenario's zijn het resultaat van de macht die zorgverzekeraars krijgen door middel van de PDS.



Figuur 18: Strategie canvas van de zorgverzekeringssector

Transparantie over zorgverzekering

De klant wil van zorgverzekeraars weten welke zorgverzekering ze kunnen krijgen en wat er wel/niet verzekerd is. Om aan deze vraag te voldoen streeft de sector naar meer transparantie over de zorgverzekering. Zorgverzekeraars worden steeds transparanter over de zorgverzekering en wat er wel/niet onder valt. Er zijn echter nog verbeteringen te maken, daardoor scoort de sector gemiddeld op deze factor. Een Personal Data Store zal ervoor zorgen dat de klant beter bij bestaande gegevens en informatie kan. Echter, het zorgt er niet voor dat zorgverzekeraars meer informatie of betere informatie vrij gaat geven. De PDS heeft hier geen impact op.

Klantbeleving centraal

De klant staat steeds meer centraal bij de zorgverzekeraar. Zo is het niet verliezen van bestaande klanten en het aantrekken van nieuwe klanten van essentieel belang. Bij klantbeleving centraal moet er vanuit de behoefte en ervaring van de klant worden gekeken wat de beste dienst is en hoe die geleverd moet worden. Zorgverzekeraars kunnen hier nog op verbeteren en scoren nu net geen voldoende. De Personal Data Store zorgt voor meer en betere gegevens over (potentiële) klanten. Hiermee kan de vraag en behoefte van de klant beter worden bepaald. De PDS kan de klantbeleving meer centraal zetten dankzij persoonlijke aanbiedingen.

Betaalbaarheid van zorgverzekering

Een belangrijke reden voor het verliezen van een klant is dat de concurrentie een betere premie biedt. Daarnaast is voor een bepaalde groep de zorg simpelweg niet betaalbaar. Dankzij de Personal Data Store zal er meer en betere persoonlijke gegevens beschikbaar zijn. Dit geeft de zorgverzekeraars macht, aangezien ze beter weten wie hun doelgroep is en welke zorg er nodig is. Aan de ene kant kan de zorgverzekeraar de potentiële kosten beter doorberekenen en inschatten. Zo is er minder buffer nodig en kan de premie hierop afgesteld worden, wat de betaalbaarheid zal doen toenemen. Daarnaast zullen er minder fouten gemaakt worden dankzij juiste gegevens, waardoor er bespaard kan worden op het corrigeren van deze fouten. Aan de andere kant geldt er in de zorgverzekering een collectiviteitsprincipe dat de zorg voor een groot gedeelte van de bevolking betaalbaar houdt. Zodra zorgverzekeraars verzekeringen op maat gaat maken, met name voor de gezonde bevolking, zal voor een groot gedeelte van de bevolking de zorg minder betaalbaar worden. Denk aan een hogere premie voor rokende klanten. Daarnaast kunnen de zorgverzekeraars ervoor kiezen om

besparingen te investeren in plaats van ze door te berekenen naar de klant. Afhankelijk van de keuzes van zorgverzekeraars zal de betaalbaarheid toenemen of juist afnemen.

Kwaliteit van dienstverlening

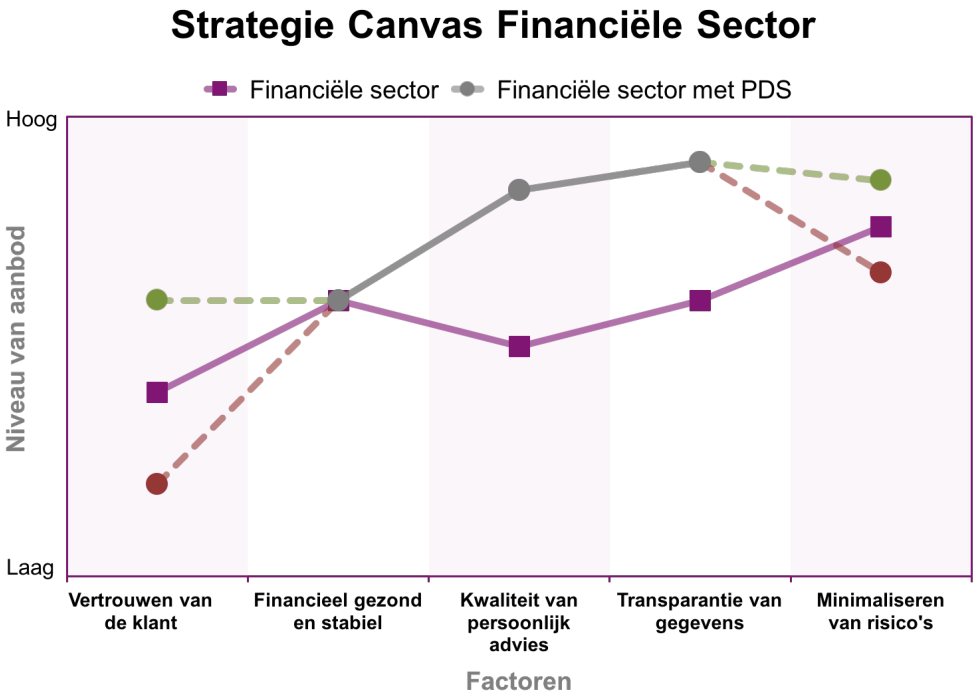
De kwaliteit van dienstverlening gaat onder andere om het aanvragen van de verzekering, en de bereikbaarheid en gemak bij indienen van vragen en declaraties. Op dit moment doet de zorgverzekeraar het goed op deze punten, er is veel aandacht voor het contact met de klant. Door de Personal Data Store is er meer informatie beschikbaar over personen en deze informatie is tevens beter. Er zullen minder fouten voorkomen en persoonlijke aanbiedingen op basis van de informatie wordt mogelijk. In het eerste opzicht zal de kwaliteit van de dienstverlening verbeteren. Echter, door de hoeveelheid macht van de zorgverzekeraars dankzij de PDS kan de kwaliteit juist verminderen. Zorgverzekeraars hebben meer inzicht in persoonlijke gegevens en kunnen op basis hiervan de zorgverzekeringen aanpassen. Zo kunnen risico gevallen uitgesloten worden van een goede zorgverzekering. De kwaliteit van de dienstverlening wordt tevens bepaald door de keuzes van de zorgverzekeraars, deze keuzes zullen bepalen of de kwaliteit verbetert of juist verslechtert.

Juistheid van klantgegevens

Het corrigeren van onjuiste informatie is een kostbare en tijdrovende klus. Dit is in feite een verspilling voor de zorgverzekeraars. Het is lastig om na te gaan of de gegevens van de klant juist en volledig zijn. De verzekeringssector scoort in het algemeen onder de maat op deze factor. De Personal Data Store zal juist voor deze factor een grote verbetering teweegbrengen. Dankzij een eenmalige uitvraag aan informatie en de mogelijkheid om informatie te delen en corrigeren is een compleet en up-to-date overzicht van de klantgegevens mogelijk. Door meer en betere gegevens van klanten zal de juistheid van klantgegevens dermate toenemen.

Impact op de financiële sector

Voor financiële organisaties zal een Personal Data Store voornamelijk een positieve impact hebben op de kwaliteit van persoonlijk advies en de transparantie van gegevens. De PDS biedt klanten inzicht in welke gegevens er worden gedeeld of gebruikt waardoor er meer transparantie ontstaat. Daarnaast worden er met toestemming van de klant meer en juiste gegevens gedeeld; hierdoor neemt de kwaliteit van het persoonlijk advies toe. Het vertrouwen van de klant in de financiële organisaties hangt af van het vertrouwen van de klant in de Personal Data Store. Mocht er wantrouwen zijn in het gebruik van een PDS dan zal dit wantrouwen overslaan op financiële organisaties op het moment dat deze gebruik maken van een PDS.



Figuur 19: Strategie canvas van de financiële sector

Vertrouwen van de klant

Het vertrouwen van de klant is dankzij de economische crisis behoorlijk geschaad. Op dit moment scoren financiële organisaties daardoor in het algemeen onder gemiddeld op deze factor. Een Personal Data Store zal inzicht bieden in het gebruik van de gegevens van klanten, zij zullen daarnaast controle en overzicht hebben. Doordat klanten weten wat er met hun gegevens wordt gedaan kan hun vertrouwen in de financiële organisaties toenemen. Echter, een Personal Data Store kan wantrouwen bij klanten oproepen aangezien hierin persoonlijke informatie wordt verzameld. Uit het gebruikersonderzoek blijkt dan ook dat een groot gedeelte sceptisch is over een PDS. Doordat financiële organisaties hierop aansluiten kan het wantrouwen in deze organisaties ook toenemen. Het vertrouwen in financiële organisaties hangt af van de perceptie van de klant en hoe een PDS naar de klant wordt gecommuniceerd.

Financieel gezond en stabiel

Een randvoorwaarde voor het vertrouwen van klanten in financiële organisaties is dat deze financiëel gezond en stabiel zijn. Dankzij de economische crisis is hier een groot behoefte aan. De meeste financiële organisaties verkeren zich weer in rustigere wateren waardoor de sector redelijk scoort op deze factor. Een Personal Data Store zal geen invloed hebben op de gezondheid en stabiliteit van financiële organisaties. Deze organisaties zijn hier zelf verantwoordelijk voor, het zal van andere factoren afhangen zoals de keuzes gemaakt bij investeringen.

Kwaliteit van persoonlijk advies

Voor veel klanten zijn financiële zaken zeer persoonlijk en daarom is er een behoefte aan een persoonlijke benadering. De financiële sector focust zich dus op de kwaliteit van het persoonlijk advies aan de klant. De financiële sector scoort net voldoende op deze factor. De Personal Data Store zal ervoor zorgen dat financiële organisaties meer en betere informatie tot hun beschikking hebben. Hiermee zal de kwaliteit van het persoonlijk advies verbeterd worden; er worden immers minder fouten gemaakt en persoonlijke aanbiedingen worden beter mogelijk.

Transparantie en openheid in informatie

Voor financiële organisaties is het van belang om transparant en open te zijn over wat er gebeurt met de informatie van de klant. Dit onder andere voor het versterken van het vertrouwen van de klant in de financiële organisaties. De sector scoort gemiddeld voor deze factor. De Personal Data Store maakt het voor de gebruiker mogelijk om in te zien wie welke informatie inziet en gebruikt. Hierdoor zal de transparantie van het gebruik van gegevens in grote mate toenemen voor onder andere de financiële organisaties.

Minimaliseren van risico's

Dankzij de turbulente tijd rondom de economische crisis heeft de klant behoefte aan weinig risico nemend gedrag bij de financiële organisaties. Financiële organisaties proberen risico's te minimaliseren, hierdoor scoort de sector boven gemiddeld op deze factor. Een Personal Data Store zorgt ervoor dat organisaties zoals financiële organisaties beter inzicht hebben in hun klanten en ze hebben meer gegevens tot hun beschikking. Met gebruik van deze informatie kan een organisatie betere keuzes maken ten opzichte van investeringen en/of leningen. Echter, dankzij dit inzicht bestaat er de kans dat financiële organisaties overmoedig worden en dankzij dit inzicht juist risicovollere keuzes maken. Hier hangt het er tevens vanaf hoe de organisaties omgaan met de macht en inzicht die ze krijgen dankzij de PDS.

6 Standaarden, patronen en principes

Voor het ontwerpen en ontwikkelen van complexe informatiesystemen zoals Personal Data Stores is een helder kader van belang. Architectuurprincipes, ontwerppatronen en technologiestandaarden bieden een dergelijk houvast.

6.1 PRINCIPES ROND PERSOONLIJKE DATA

Onder meer in de Nederlandse overheid wordt op uitgebreide schaal gewerkt met architectuurprincipes. De NORA (Nederlandse OverheidsReferentieArchitectuur) is een belangrijke bron hiervoor, evenals haar dochterarchitecturen zoals GEMMA, PETRA, WILMA en anderen. De NORA onderscheidt tien basisprincipes (BPxx) en ca. veertig afgeleide principes (APyy). In elk geval zijn de onderstaande principes hieruit relevant voor toepassing van Personal Data Stores in een overheidscontext.

> Architectuurprincipes zijn algemene, stabiele en breed geldende uitspraken die richtinggevend zijn voor de ontwikkeling en inrichting van een organisatie of systeem. Principes worden gebruikt om op een hoog niveau de strategie en uitgangspunten van een organisatie te vertalen in begrijpelijke, toepasbare richtlijnen. Door hun brede geldigheid creëren principes ook inzicht: door grote systemen overal op dezelfde manier in te richten, zijn deze eenvoudiger te begrijpen omdat de achterliggende gedachten steeds herkenbaar zijn.
>
> Een goede verzameling principes voldoet in elk geval aan de volgende eisen:
>
> - De principes zijn begrijpelijk en de gebruikers ervan weten hoe ze deze moeten toepassen.
> - De principes zijn robuust, goed toe te passen in verschillende situaties en leiden tot duidelijke uitspraken.
> - De principes zijn toetsbaar, er kan duidelijk worden vastgesteld of een gegeven situatie aan een principe voldoet of niet.
> - De principes zijn onderling consistent en spreken elkaar niet tegen.
> - De principes zijn stabiel en veranderen relatief zelden.

BP06: Transparant. Afnemers hebben inzage in voor hen relevante informatie.

De dienstverlener geeft afnemers vooraf, tijdens en na het uitvoeren van een dienst informatie over het resultaat, het proces en de gebruikte gegevens. Het gaat om algemene informatie over de dienst en om informatie over de afnemer zelf. In het bijzonder is het van belang om informatie te verschaffen over de betekenis (semantiek) van gebruikte informatie, over de status van het dienstverleningsproces en over de vraag welke informatie van de afnemer wordt bijgehouden.

BP08: Vertrouwelijk. Afnemers kunnen erop vertrouwen dat informatie niet wordt misbruikt.

De dienstverlener garandeert dat informatie alleen toegankelijk is voor bevoegde personen en alleen wordt gebruikt voor het doel waarmee zij is verzameld. Dit principe geldt niet alleen voor informatie over personen, maar ook voor informatie over bedrijven en de overheid zelf. Zo kunnen bedrijfsgegevens waaruit investeringsbeslissingen zijn af te leiden interessant zijn voor de concurrentie. Informatie over overheidsgebouwen kan interessant zijn voor terroristen.

AP13: Bronregistraties zijn leidend: Alle gebruikte informatieobjecten zijn afkomstig uit een bronregistratie.

AP15: Doelbinding: Het doel waarvoor informatie wordt (her)gebruikt is verenigbaar met het doel waarvoor deze oorspronkelijk is verzameld.

AP16: Identificatie informatie-objecten: Informatieobjecten zijn uniek geïdentificeerd.

AP17: Informatie-objecten systematisch beschreven. De aan de dienst gerelateerde informatieobjecten zijn systematisch beschreven en op passende wijze gemodelleerd.

AP37: Identificatie, authenticatie en autorisatie. Dienstverlener en afnemer zijn geauthentiseerd wanneer de dienst een vertrouwelijk karakter heeft.

AP39: Controle op juistheid, volledigheid en tijdigheid. De betrokken systemen controleren informatie-objecten op juistheid, volledigheid en tijdigheid.

Ook in de gemeentelijke wereld wordt gewerkt met principes. De volgende principes uit de GEMMA zijn specifiek relevant:

Onze gemeente biedt de klant een goede informatiepositie. Een goede informatiepositie is voor klanten cruciaal om snel en gemakkelijk hun weg te vinden binnen de overheid. Het zorgt er ook voor dat zij de verantwoordelijkheid kunnen nemen die in toenemende mate van hen wordt verwacht vanuit een nieuw evenwicht tussen samenleving en overheid. Dat gaat niet alleen over het ontvangen van informatie; het gaat ook over het aan het stuur zetten van de klant omtrent het gebruik van zijn gegevens. Klanten moeten in staat zijn incorrecte registratie van hun gegevens te signaleren, zodat ze voor zichzelf op kunnen komen.

Onze gemeente hergebruikt gegevens. Binnen de Nederlandse overheid is afgesproken dat burgers niet wordt gevraagd om gegevens waar de overheid zelf al over beschikt.

Onze gemeente gaat op een vertrouwelijke manier met gegevens om. Klanten verwachten dat de gemeente op een zorgvuldige manier met hun gegevens om gaat en dat deze niet in handen komen van onbevoegden.

Een andere interessante invalshoek zijn de 'rules of engagement' van het Internet of Subjects (een not-for-profit groep individuen en organisaties die het individu meer centraal willen stellen in de ontwikkeling van het internet) en de daaruit volgende architectuurprincipes. Deze geven een zeer specifieke invulling aan een PDS die mogelijk niet in alle contexten van toepassing is, maar zeker interessante aanknopingspunten biedt:

1. Totale scheiding tussen de opslag van persoonlijke gegevens en attributen (in de PDS) en het gebruik van die gegevens en attributen door andere organisaties. Die scheiding is fysiek, functioneel en juridisch gewaarborgd.
2. De PDS's van een persoon kunnen over verschillende providers verdeeld zijn, elk met specifieke diensten aangepast aan het type gegevens waar het om gaat, het benodigde niveau van beveiliging en de gevraagde performance.
3. Alle PDS's van een persoon zijn verbonden door middel van een service bus die de eigenaar in staat stelt al zijn/haar persoonlijke gegevens te beheren en gebruiken, met inachtneming van de beveiligingsniveaus van de verschillende PDS's. Er is geen bovengrens aan het aantal PDS's dat zo verbonden kan worden.
4. De eigenaar van de inhoud van een reeks PDS's heeft een integraal, compleet beeld van al zijn/haar persoonlijke gegevens en heeft volledige controle over het gebruik hiervan en de bijbehorende toegangsregels.
5. Alle PDS's waarmee een organisatie interactie heeft zijn functioneel ontkoppeld om het risico van hackers, incompetente of kwaadwillende personen te beperken. Het is niet mogelijk de inhoud van een PDS te lezen of exporteren zonder de expliciete toestemming van de eigenaar.
6. De interactie met een PDS verloopt via een webservice. Toevoegen van nieuwe services voor het genereren of gebruiken van persoonlijke gegevens wordt gedaan via een federatie van services in een persoonlijke 'circle of trust', onder regie van de eigenaar.

Wanneer meer eigenaren zijn of in geval van beperkingen op de gegevenstoegang (bijv. wanneer informatie vertrouwelijk binnen een bedrijf is) kunnen persoonlijke, groeps- en organisatieregels voor gegevenstoegang worden gecombineerd om toepassing van de relevante regels af te dwingen.

Samenvattend zijn de volgende principes het belangrijkste in de context van Personal Data Stores:

1. **Leg de regie bij het individu**: Degene over wie de data gaan, bepaalt door wie deze mogen worden gebruikt (behoudens wettelijke uitzonderingen, gereguleerd op basis van doelbinding).
2. **Registreer aan de bron**: Vermijd kopieën en vraag niet naar de bekende weg, maar hergebruik reeds vastgelegde gegevens onder regie van de betrokkene.

3. **Bescherm de data**: Zorg dat toegang tot gegevens met voldoende sterke technische, procedurele en juridische waarborgen is omgeven, van sterke encryptie en authenticatie tot screening van personeel (en ketenpartners) en sancties op overtredingen.
4. **Scheid opslag en gebruik**: Maak een scherp onderscheid tussen het vastleggen van gegevens en het gebruik hiervan, op technisch, functioneel, organisatorisch en juridisch vlak.
5. **Geef data betekenis**: Leg niet alleen de data zelf vast, maar beschrijf ook wat deze betekent (bijvoorbeeld met metadata).
6. **Bewaak de datakwaliteit**: Neem technische en organisatorische maatregelen om de kwaliteit van de vastgelegde gegevens te verzekeren, op korte en lange termijn.
7. **Gebruik open standaarden**: Voor de eenvoudige uitwisseling van gegevens en het voorkomen van 'lock-in' is het gebruik van breed gedragen open standaarden essentieel.

6.2 ONTWERPPATRONEN IN PERSONAL DATA STORES

Specifiek voor Personal Data Stores zijn er nog niet veel ontwerppatronen te vinden, omdat dit een relatief nieuw terrein is en dergelijke ontwerpproblemen daarmee nog niet vaak voorkomen. Toch willen we hier een paar interessante voorbeelden noemen van patronen die op dit gebied van toepassing kunnen zijn.

> Ontwerppatronen ('design patterns') geven standaardstructuren voor de oplossing van veelvoorkomende ontwerpproblemen. Dergelijke patronen worden veelal op een standaardmanier beschreven. Een veel gebruikt sjabloon voor patroonbeschrijving (http://hillside.net/patterns/50-patterns-library/patterns/222-design-pattern-definition) heeft de volgende onderdelen:
>
> - **Naam**: een korte, pakkende, betekenisvolle naam.
> - **Probleem**: het ontwerpvraagstuk dat moet worden opgelost.
> - **Context**: de omstandigheden waarin het patroon kan worden toegepast.
> - **Krachten**: de verschillende belangen, eisen en wensen waarmee rekening moet worden gehouden.
> - **Oplossing**: de onderdelen van de oplossing en hoe die samenhangen.
> - **Resulterende context**: de situatie na toepassing van het patroon, waaronder voor- en nadelen ervan.
> - **Rationale**: de achterliggende motivatie voor deze oplossing.

Specifiek voor het "social" aspect in personal data stores hebben we in eerder onderzoek wel een aantal patronen ontwikkeld. Zie daarvoor (Beuger & Janssen, 2014), met onder meer het patroon "In de genen".

Datavirtualisatie

Datavirtualisatie is een nuttige techniek om gegevens uit verschillende bronnen op een eenduidige manier te ontsluiten. Datavirtualisatie is zelf als een groot architectuurpatroon te beschouwen, maar er zijn ook specifiekere patronen voor deelproblemen op dit vlak.

Probleem: Hoe ontsluit je gegevens uit verschillende, heterogene bronnen op een eenvoudige, uniforme manier, zonder bijvoorbeeld lokale kopieën van de data te maken?

Context: Een PDS combineert gegevens uit allerlei verschillende bestaande bronnen, die elk hun eigen technische en andersoortige standaarden hanteren.

Krachten: Technische heterogeniteit en bijvoorbeeld performance-eisen, versus enkelvoudige (en eenvoudige) ontsluiting.

Oplossing: Datavirtualisatie legt een abstractielaag over de verschillende bronnen die de details van de implementatie van die bronnen afschermt voor de gebruiker van de data. Een PDS kan ook worden beschouwd als een vorm van datavirtualisatie: het biedt een gestandaardiseerde manier van toegang tot de achterliggende brongegevens, zonder die data zelf lokaal op te slaan.

Resulterende context: De resulterende virtualisatielaag biedt op een uniforme, gestandaardiseerde manier toegang tot de achterliggende gegevens.

Rationale: Een nuttig whitepaper dat meer achtergronden geeft over datavirtualisatie is geschreven door Cap Gemini.[4]

SafeAnswers

Een interessant architectuurpatroon vormt de kern van het openPDS systeem van MIT. Hoewel zij dit zelf niet in de vorm van een patroon beschrijven, is dit een uitstekend voorbeeld hiervan. Conform het voorgaande sjabloon ziet dit er als volgt uit.

Probleem: Hoe kun je hoogdimensionele data (bijv. geolocatiegegevens) laten gebruiken door derden zonder je anonimiteit op te geven?

[4] https://www.nl.capgemini.com/resource-file-access/resource/pdf/1b-015.13_dutch_version_of_wp_data_virtualization_web.pdf.

Context: Allerlei partijen hebben behoefte aan persoonsgebonden, privacygevoelige informatie voor bijvoorbeeld analysedoeleinden. Een PDS ontsluit dergelijke data op een centrale, eenduidige, gestandaardiseerde manier.

Krachten: Beschermen van de privacy van degene op wie de data betrekking heeft, mogelijkheid tot analyseren van data over groepen mensen.

Oplossing: SafeAnswers brengt niet de data naar de code, maar de code naar de data. De oplossing bestaat uit twee lagen:

1. Gevoelige bewerkingen van data vinden plaats binnen de PDS van de gebruiker en alleen de uitkomsten hiervan worden beschikbaar gesteld aan de vragende partij, niet de data zelf.
2. Data kan anoniem worden geaggregeerd over individuen heen met een privacybeschermende methode voor berekeningen voor dergelijke groepen, zonder deze data zelf met anderen te delen.

Resulterende context: Bij toepassing van SafeAnswers kunnen externe partijen vragen stellen over de data en worden de antwoorden onder regie van de gebruiker terug geleverd. De data zelf verlaat nooit de PDS-omgeving.

Rationale: Beschermen van je privacy wordt steeds moeilijker. Doordat hoogdimensionele data zeer specifiek is, is het vaak toch mogelijk om geanonimiseerde gegevens te herleiden tot de bron. Denk aan locatiegegevens. Uit onderzoek is bekend dat met slechts vier datapunten van plaats en tijd 95% van de mensen uniek te identificeren is. Het beschikbaar stellen van dergelijke data is dan ook vaak ongewenst. Het alleen toestaan vragen te stellen over die data kan de privacy-risico's beperken, omdat de antwoorden onder regie van de gebruiker berekend en gegeven worden zonder de data zelf te hoeven delen met anderen.

Pseudonimiseren

Een ander relevant patroon om de privacy te beschermen is het pseudonimiseren van gegevens. Dit laat nog wel toe om gegevens uit verschillende bronnen te koppelen op persoonsniveau, maar geeft geen (rechtstreekse) identificatie van het individu. Een voorbeeld hiervan is ZorgTTP, dat als vertrouwde derde partij voor de zorgsector gegevens pseudonimiseert.

Probleem: Hoe kunnen gegevens op persoonsniveau worden gecombineerd, zonder de identiteit van personen bekend te maken?

Context: Gegevens uit verschillende bronnen moeten voor bijvoorbeeld onderzoeksdoeleinden kunnen worden gecombineerd.

Krachten: De behoefte aan het combineren van gegevens uit verschillende bronnen op persoonsniveau, om samenhang en correlaties te kunnen onderzoeken (denk aan medische gegevens met woonadres, om te onderzoeken of wonen in de buurt van een snelweg gezondheidsrisico's oplevert). Dit levert echter potentieel grote privacyrisico's op en is in veel gevallen simpelweg wettelijk verboden.

Oplossing: Individuen krijgen door een vertrouwde derde partij een pseudoniem toegekend dat alleen door die partij tot het individu valt te herleiden.

Resulterende context: De gegevens worden via die vertrouwde derde partij gepseudonimiseerd doorgeleverd aan de gebruikende organisaties en systemen.

Rationale: Om gegevens uit verschillende bronnen te kunnen combineren op persoonsniveau is een unieke identificatie van die personen nodig. Door deze identificatie door een vertrouwde derde partij te laten toekennen, kunnen de organisaties die de gegevens gebruiken zelf niet meer die persoon identificeren en is zijn/haar anonimiteit gewaarborgd. Echter, deze anonimiteit is niet absoluut. Als je voldoende gegevens over iemand verzamelt, is uit dat profiel de identiteit vaak ook af te leiden.

6.3 RELEVANTE STANDAARDEN

Personal Data Stores zijn per definitie softwaretoepassingen die niet op zichzelf staan, maar verschillende databronnen en applicaties verbinden. Om te kunnen functioneren in zulk een heterogene omgeving zijn standaarden nodig. Standaarden zijn generieke verzamelingen van voorschriften die een ideale uitvoering van bepaalde activiteiten weergeven, ofwel uitgeschreven normen. Door databronnen, interfaces en applicaties op een eenduidige manier met elkaar te verbinden, i.e. door te standaardiseren, kunnen Personal Data Stores optimaal functioneren. Het liefst zijn gebruikte standaarden open, wat zoveel betekent als publiekelijk ontwikkeld en toegankelijk. Standaarden kunnen zowel technisch, bijvoorbeeld communicatieprotocollen, als organisatorisch, denk aan afspraken over het delen van data, zijn ingestoken. PDS toepassingen maken veel gebruik van verschillende algemene standaarden voor informatiesystemen en software, maar er zijn ook een aantal standaarden die specifiek voor PDS's relevant zijn.

Belangrijk voor PDS's zijn standaarden voor het organiseren van toegang tot persoonlijke data. De gebruiker geeft bijvoorbeeld toegang tot zijn data middels een technische protocol als User Managed Access (UMA). UMA is dus een technische standaard voor gedelegeerde autorisatie, en zelf gebaseerd op een standaard voor toegang, namelijk Oauth. Het werd ontwikkeld door het Kantara initiative, een non profit organisatie voor innovatie op het gebied van digitale identiteitenmanagement, en goedgekeurd in 2015.

Maar behalve de technische standaarden die nodig zijn, is ook een afsprakenstelsel nodig waarin verantwoordelijkheden zijn bepaald. En deze afsprakenstelsels moet zelf weer technisch worden ingebed in de PDS-toepassingen. Twee voorbeelden van standaardisatie op dit gebied zijn Qiy en het Respect Network. Qiy is een open standaard voor een afsprakenstelsel met betrekking tot delegeren van toegangsbeheer van persoonlijke data door de gebruiker. Applicatie-ontwikkelaars die persoonlijke data verwerken kunnen dus door de bepalingen uit de Qiy standaard te verwerken in hun applicaties het beheer hiervan aan de gebruiker overlaten. De Qiy standaard is nog in ontwikkeling en niet publiek beschikbaar. Het is nog geen open standaard.

Voor de structuur, verwerking en opslag van persoonlijke data bestaan ook veel standaarden, die dus relevant zijn in de ontwikkeling van PDS's. Een voorbeeld is de ISO 27018 (2014) norm die beschrijft hoe persoonsgegevens in cloud oplossingen zouden moeten worden beschermd.

Ten slotte bestaan er ook standaarden voor een hele PDS: een voorbeeld van een open-source PDS-toepassing is OpenPDS dat door MIT werd ontwikkeld, zoals hierboven al is geïntroduceerd. OpenPDS maakt zelf weer gebruik van het Funf open-sensing framework waarmee sensordata op Android-smartphones wordt verzameld en stuurt naar de OpenPDS omgeving. Op zijn beurt draait de OpenAnswers applicatie op data uit de OpenPDS software. Voor meer informatie, zie deze video.

7 Het gebruikersperspectief

We hebben gekeken naar het concept, voorbeelden ervan, mogelijke bedrijfsmodellen. Maar wat vinden “we” daar nu van, wij als Nederlandse burgers en consumenten? Zijn we allemaal tegen dit soort praktijken, zoals de privacy fundamentalisten ons willen laten geloven? Of zijn we inderdaad ontzettend naïef en delen we alles, met iedereen, zoals het gebruik van Facebook suggereert? Zo heel veel weten we niet op dit vlak, zeker niet in Nederland. In 2005 is er een groot onderzoek gedaan bij de start van MijnOverheid.nl. Dat was in de tijd dat Hyves pas een jaar bestond en 100.000 leden had. Sinds die tijd is er heel veel veranderd op het internet, de vraag is of dat onze mening en gedrag ook heeft veranderd. In februari van dit jaar heeft het Ministerie van Economische Zaken door TNO een onderzoek laten doen naar de privacybeleving van Nederlanders; daar liggen raakvlakken met dit thema (TNO, 2015).

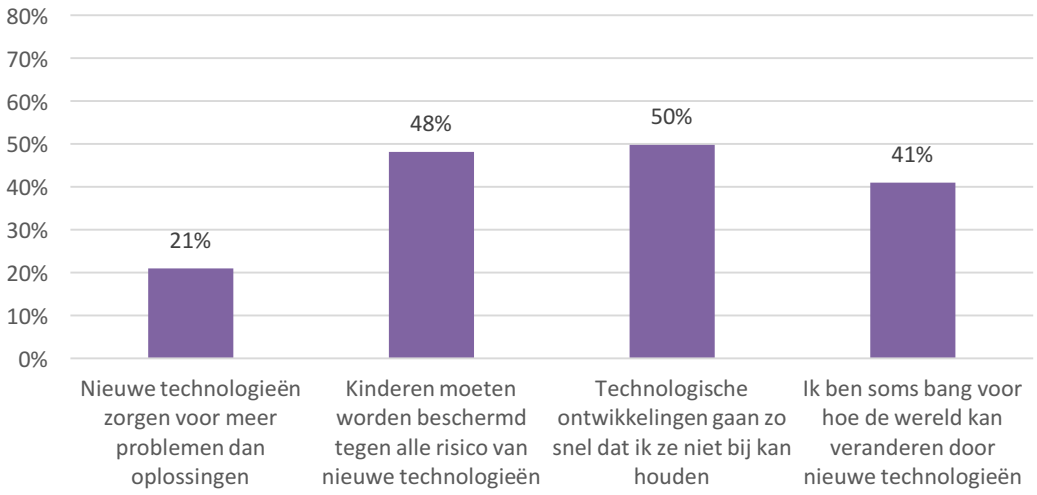
We zijn dus op zoek gegaan naar de mening van Nederlanders over gebruik en delen van persoonlijke data door en met organisaties. In dit onderzoek wordt gevraagd naar de mening van Nederlanders over het gebruik van persoonlijke data door organisaties. Specifieke vragen hierbij zijn: wat is de behoefte om zelf persoonlijke data te beheren en controleren? Welke problemen heeft men met de huidige situatie van persoonlijke data beheer? In welke partijen heeft men het meeste vertrouwen als het gaat om persoonlijke data? En wanneer is men bereid persoonlijke data te delen? Kunnen we daarbinnen verschillende doelgroepen of marktsegmenten herkennen?

Het onderzoek is in juni 2015 voor Digital We uitgevoerd door Newcom Research, in opdracht van InnoValor. De mening van 501 Nederlanders is gemeten (Newcom, 2015).

Technologie is eng, maar handig

Wanneer we meten hoe Nederlanders tegen technologie aankijken, zijn vier groepen te onderscheiden. Aan de ene kant van het spectrum, vinden we de argelozen en de luddites. Zij zijn huiverig voor nieuwe technologieën. Aan de andere kant de adopters en sceptici: enthousiast over nieuwe technologie. De argelozen en adopters maken eerder gebruik van nieuwe technologie dan de sceptici en luddites.

Wanneer we specifiekere vragen gaan stellen over technologie zien we dat de helft van de respondenten de ontwikkelingen zo snel vindt gaan, dat ze het niet allemaal bij kunnen houden. Daarnaast is een groot deels zelfs bang voor de ontwikkelingen die technologie teweeg kan brengen (41%). Dit kan een uiting zijn van bijvoorbeeld de angst om werkeloos te worden door bepaalde ontwikkelingen, of de gevolgen van nieuwe



Figuur 20: Percentages van de respondenten die aangaven het eens te zijn met de stellingen

technologie voor onze omgeving. Daarnaast moeten kinderen ook vooral beschermd worden voor die nieuwe technologieën.

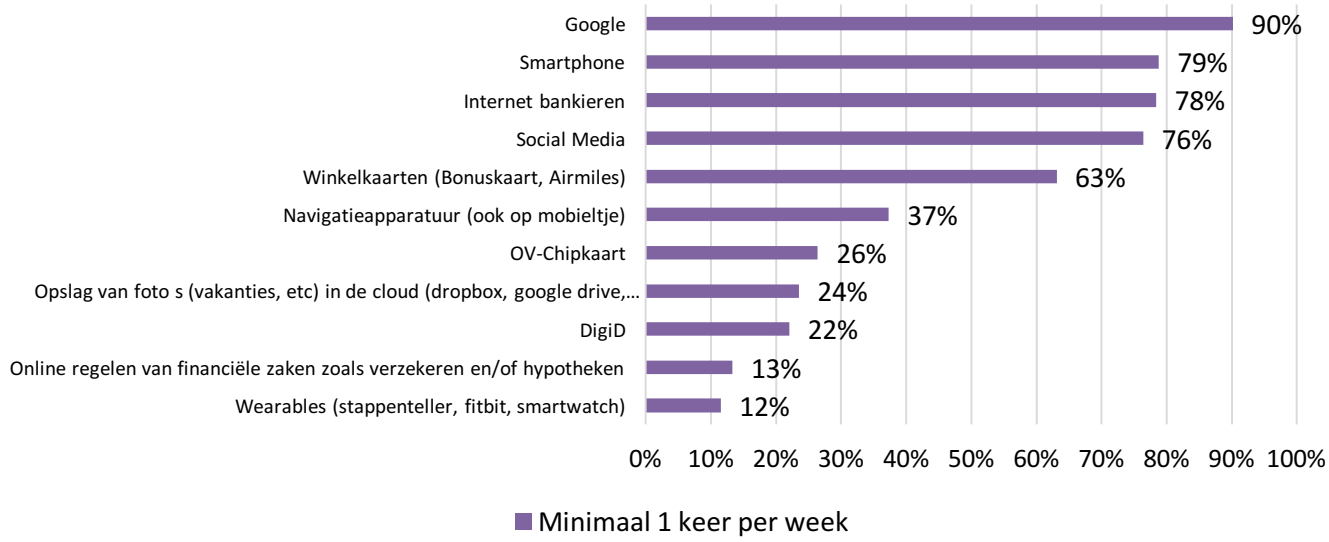
Ondanks die overwegingen zien we toch meer voordelen dan nadelen. We zien dat technologie ons leven toch wel makkelijker kan maken en iets meer dan de helft (54%) van de Nederlanders wordt zelfs enthousiast van nieuwe technologieën.

Toch ziet men ook voordelen van technologie. Het maakt mensen enthousiast (54%) en kan het leven ook beter maken (54%). Dit zien we terug in het daadwerkelijke gebruik van technologie: 90% van de mensen maakt gebruik van Google, en smartphones worden inmiddels door 79% van de Nederlanders gebruikt. Wearables zijn wat minder aanwezig: 12% gebruikt wekelijks een wearable.

We doen het allemaal…

Dat het gebruik van social media wijdverspreid is weten we inmiddels. Het is dan ook geen verrassing dat 76% van de mensen aangeeft social media te gebruiken.

DigiD lijkt hier laag uit te komen, maar als je bedenkt dat hier wordt gevraagd om 'minimaal eens per week' is dit een zeer hoge score: een vijfde van de Nederlanders gebruikt inmiddels wekelijks DigiD. Wearables hebben daarnaast nog wel een lange weg te gaan, maar 12% gebruikt wekelijks een wearable. De smartwatches en stappentellers zijn daarmee nog lang geen concurrentie voor de smartphone die inmiddels door 79% van de Nederlanders gebruikt worden. Daarnaast worden ook zaken als winkelkaarten door wel 63% van de Nederlanders wekelijks gebruikt.



Figuur 21: Percentage van de respondenten dat aangeeft de technologie minstens eenmaal per week te gebruiken

Deze cijfers geven een ander beeld dan eerder geschetst. We geven aan dat we technologische ontwikkelingen lang niet allemaal bij kunnen houden, maar toch wordt er veel meer gebruik van nieuwe technologie gemaakt dan dat sentiment doet vermoeden. We gebruiken allemaal de platformen, waar we soms toch twijfels bij hebben.

De bovenstaande cijfers zijn in lijn met andere onderzoeken. Uit het social media onderzoek van Newcom[5] blijkt dat al 9,4 miljoen Nederlanders Facebook gebruiken, bijna 80% van de Nederlanders maakt gebruik van een of meerdere platformen. Het gebruik van DigiD is, volgens het overheidsonderzoek naar de kwaliteit van dienstverlening in 2014 gestegen naar 52%, met een bijna 100% bekendheid.

[5] http://www.newcom.nl/socialmedia2015

Gegevens, hoezo opslaan?

Nederlanders laten onzekere gevoelens zien als het aankomt op persoonlijke data. Een meerderheid van de respondenten (57%) geeft bijvoorbeeld aan dat ze niet precies weten hoeveel gegevens er over ze zijn opgeslagen. 38% weet ook niet precies hoeveel ze zelf delen. Daarnaast ziet ook twee derde van de mensen het nut niet in van de opslag van gegevens. Het komt erop neer dan Nederlanders niet weten welke gegevens organisaties hebben, waarom ze gegevens hebben en wat ermee gebeurt.

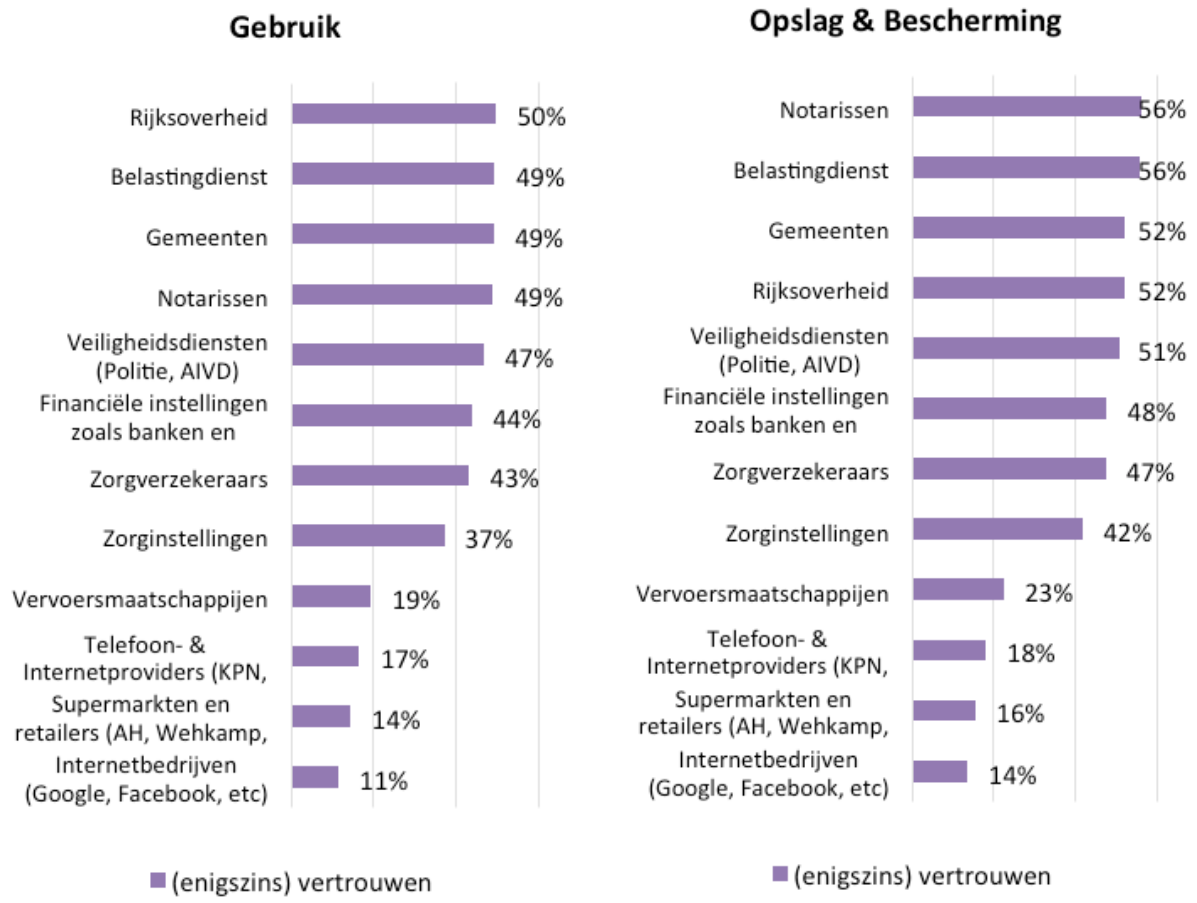
Mensen willen zelf kunnen sturen: er is een grote behoefte om zelf te kunnen bepalen wie er toegang heeft tot gegevens. Dit vertaalt zich in een behoefte naar meer controle: men wil gegevens kunnen bewerken en kunnen verwijderen. Dat men dit graag wil lijkt voort te komen uit het gevoel van onzekerheid en niet weten wat er allemaal opgeslagen is. Er is dus wel degelijk behoefte aan meer inzicht en controle.

Opvallend is dat men in Nederland weinig waarde hecht aan het zelf verkopen van data. Terwijl in de UK 47% van de respondenten besparingen zag als een rede om data te delen. Wellicht is de mogelijkheid nog zo onbekend, dat dit niet als optie gezien wordt. Dit zet vraagtekens bij de ontwikkeling van initiatieven waar persoonlijke data verkocht wordt, zoals Datacoup.[6] Data kunnen verplaatsen, corrigeren of centraal beheren, heeft nog weinig prioriteit. We willen meer controle, maar hoe dat wordt geregeld is (nog) minder belangrijk.

We vertrouwen vooral de overheid

Wanneer we vragen wie we vertrouwen met opslag en gebruik van onze gegevens komt de overheid positief naar voren (tussen de 56% en 52% vertrouwen). Verzekeraars en zorgverzekeraars hebben, net als banken, een achterhoedepositie (tussen de 48% en 40% vertrouwen). De introductiestrategie van bijvoorbeeld de Poliskluis, zal zorgvuldig moeten gebeuren en sterk moeten appelleren aan transparantie en controle om de vertrouwenskant te laten groeien. De Internet Service Providers, TelCo's, retail en internetbedrijven(Google, Facebook) scoren het slechtst.

[6] www.datacoup.com



Figuur 22: Het percentage van de respondenten dat aangeeft de betreffende partij te vertrouwen met het gebruik, dan wel opslag, van hun data

De zorgpartijen staan er in de UK beter voor: 61% van de Engelsen heeft vertrouwen in deze groep. Wanneer we kijken naar de situatie in de UK blijkt dat de variant van het 'EPD' (elektronisch patiëntendossier) daar al eerder dan in Nederland is ingericht en al verder is ingebed in het land. Onderzoek van de NPCF[7] uit 2015 laat zien dat er wel een latente behoefte is: gebruikers van een persoonlijk gezondheidsdossier (zo'n 9%) van de Nederlanders, wil nooit meer zonder en ziet grote voordelen in het gebruik. De aanleiding om tot gebruik te komen ligt dan vaak in chronisch ziek worden of merken dat er veel miscommunicatie is in de zorgketen. Aan de aanbiederskant is deelname aan het Landelijk Schakelpunt (LSP), waar medische informatie uitgewisseld wordt, al meer dan 90%.[8]

Wanneer we dit beeld vergelijken met een onderzoek van NetPanel uit 2005, zien we een ander beeld. De banken stonden toentertijd bovenaan als het ging om vertrouwen. Daarentegen scoorden overheidspartijen in die tijd ook al goed.

Een andere interessante vergelijking op gebied van vertrouwen, is met het onderzoek uit de UK. Daar staan de zorginstellingen juist bovenaan de lijst van vertrouwde organisaties, 60% van de respondenten geeft aan ze te vertrouwen, en staat daarmee ver boven andere publieke partijen. Er zijn ook gelijkenissen te vinden: de telefoon & internet providers staan daar ook laag in de lijst met 34% vertrouwen. De social media organisaties

[7] https://www.npcf.nl/nieuws/nieuws/694-wie-eenmaal-een-pgd-heeft-wil-nooit-meer-zonder
[8] https://www.vzvz.nl/page/Zorgconsument/Links/Over-VZVZ/Feiten-en-cijfers

pakken de onderkant met maar 31%. Daarmee zijn de Nederlanders wel wat sceptischer aangelegd, hier scoren ze respectievelijk 18% en 14%.

Een totaal ander beeld ontstaat als we deze cijfers vergelijken met cijfers uit de VS (GfK 2014). Daarin staan juist zorgverleners en retailers bovenaan, op de voet gevolgd door banken. Verzekeraars staan iets hoger dan in ons onderzoek, maar de overheid staat relatie laag in de vertrouwenspositie. Wie we vertrouwen verschilt dus sterk per land, en per schandaal dat er speelt.

Delen is een kwestie van vertrouwen

Het delen van data doen we met verschillende partijen. Daarnaast doen we het met verschillende beweegredenen. De ene keer vraag je toegang tot een app, de andere keer moet je je inkomensgegevens delen met een hypotheekverstrekker. Maar wat zijn precies de redenen om te delen?

Een basis van vertrouwen is van belang: 43% van de Nederlanders zou gegevens delen als ze een organisatie vertrouwen. Het speelt daarmee een veel grotere rol dan het krijgen van geld of een dienst voor de gegevens. Het blijkt dat 'de wet' en vertrouwen in een organisatie goede motivatoren zijn om gegevens te delen. We zijn daarnaast toch snel bereid data te delen voor nationale veiligheid. Wetgeving kan daarmee een manier zijn om initiatieven te stimuleren. Bijvoorbeeld voor een dienst als MijnOverheid zou een wettelijke verplichting ondersteuning kunnen bieden.

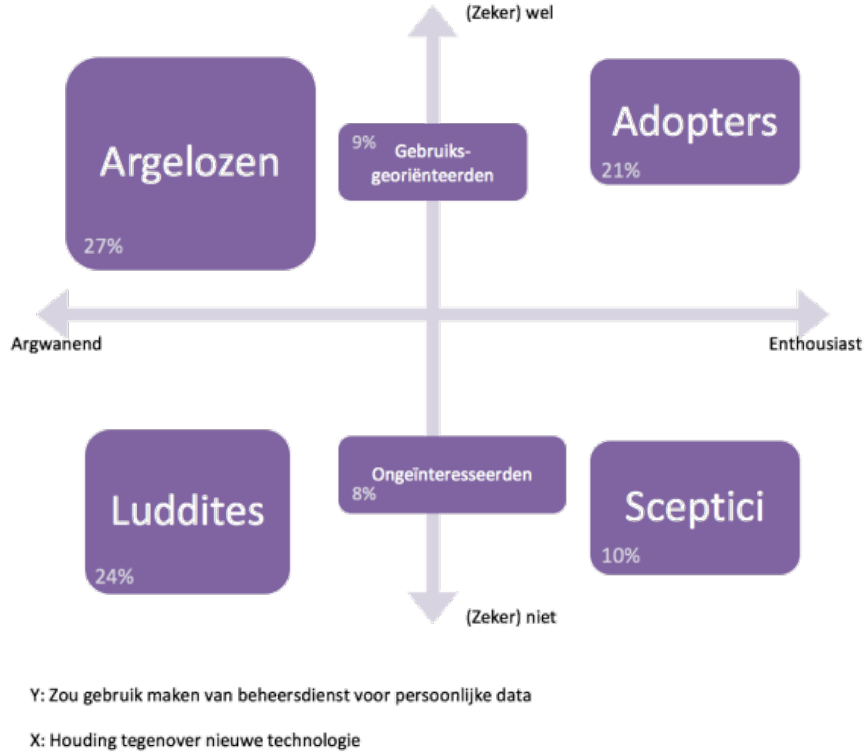
Toch is een behoorlijk deel (14%) van de Nederlanders helemaal niet bereid om persoonlijke gegevens te delen. Het zal altijd lastig blijven om deze groep te verleiden tot gebruik van een dienst wanneer daar persoonlijke gegevens voor gedeeld moeten worden.

Het lijkt erop dat Nederlanders in het algemeen eerder gegevens zullen delen wanneer ze een organisatie vertrouwen of voor de veiligheid, dan dat ze op geld of andere compensatie gericht zijn. Een dienst die zich met persoonlijke gegevens bezighoudt zal zich dus in eerste instantie moeten richten op die vertrouwensbasis. Daarbij kan de wettelijke hand hulp bieden om mensen aan een dienst te binden, maar de vertrouwensbasis is, logischerwijs, van groot belang.

Welke segmenten zien we dan?

Als we al deze kenmerken combineren, ontstaan er duidelijke segmenten. Het belangrijkste onderscheid zit daarbij op twee assen: de houding ten opzichte van nieuwe technologie en de mate waarin we gebruik zouden willen maken van een beheersdienst voor persoonlijke data, een PDS. Uiteraard zijn Nederlanders niet over één kam te scheren. Binnen de respondenten waren vier grote, en twee kleinere segmentaties te onderscheiden. Door te vragen hoe men tegenover technologie staat en hoe men denkt over de mogelijkheden rondom beheer van persoonlijke data, kunnen we identificeren hoe Nederlanders op deze vraagstukken te typeren zijn.

Aan de ene kant van het spectrum, vinden we de *argelozen* en de *luddites*. Beide groepen zijn in het algemeen argwanend ten opzichte van nieuwe technologie. De argelozen zouden echter wel gebruik maken van nieuwe technologie, maar de luddites niet. Onder beide groepen vallen relatief veel lager opgeleiden.



Figuur 23: Segmenten, gecategoriseerd naar gebruik van PDS en houding t.o.v. technologie

Aan de andere kant zien we de *adopters* en de *sceptici*. Beide groepen zijn enthousiast over nieuwe technologieën. In beide groepen vinden we overwegend mannen: 62% van de adopters en 59% van de sceptici is man. Daarnaast zijn er onder de sceptici relatief veel hoger opgeleiden. Een verschil is echter dat de sceptici het idee van een beheerdienst voor persoonlijke data nog niet ziet zitten. De adopters daarentegen, zien er wel toekomst in.

Als we de percentages van de groepen optellen, komen we nog niet tot de volle 100%. Er zijn namelijk nog twee andere groepen te herkennen in de populatie. Dit zijn de *gebruiksgeoriënteerden* en de *ongeïnteresseerden*. Deze twee groepen zijn beide onverschillig over technologie. Ze zijn er niet argwanend over, maar ook niet enthousiast. De gebruiksgeoriënteerden zijn echter wel geneigd diensten voor het beheer van persoonlijke data te gebruiken, terwijl de ongeïnteresseerden dat liever niet doen. Het stereotype gevoel dat vrouwen minder met technologie hebben wordt hier bevestigd: vrouwen zijn relatief sterk vertegenwoordigd in deze twee groepen.

Al met al staat 57% van de ondervraagden positief ten opzichte van het concept PDS. Dat zien we ook terug als we puur en alleen krijgen naar de intentie tot gebruik, later in het hoofdstuk. Het is daarnaast opvallend dat leeftijd in de gehele segmentatie geen rol speelt: in alle groepen is leeftijd divers.

Verder is het interessant om de groepen op meer punten te vergelijken. Bijvoorbeeld tegen verwachting in controleren de luddites en argelozen het minst vaak eigen gegevens (57% resp. 45% doet het nooit). Terwijl ze wel sceptisch tegenover technologie staan. Dit zou voor een deel bij onwetendheid kunnen liggen: ze zijn angstiger om de technologie te leren kennen. Daarnaast zien we dat de adopters een stuk meer vertrouwen hebben: ze delen het vaakst bij vertrouwen in een organisatie (52%) en ze vertrouwen de Rijksoverheid het meest (57%). Wellicht dat dit grotere vertrouwen er ook voor zorgt dat ze eerder vertrouwen hebben in nieuwe technologieën en er dus minder angstig voor zijn.

	Argelozen	Adopters	Luddites	Sceptici
Populatie aandeel	27%	21%	24%	10%
Controleert nooit zijn gegevens	45%	39%	57%	36%

Deelt gegevens bij wettelijke verplichting	52%	66%	44%	40%
Deelt gegevens bij vertrouwen in organisatie	40%	52%	28%	25%
Is nooit bereid gegevens te delen	12%	4%	32%	27%
Vertrouwd in Rijksoverheid met gegevens	48%	57%	33%	23%

Personal Data Stores, ehhh?

Op dit moment roept het beheren van eigen data op een centrale plaats nog weinig beelden op bij mensen. Wanneer we vragen om hier gedachtes bij te omschrijven komt voor terug dat men 'geen idee' heeft. Het is dus van belang om te zorgen dan mensen snappen wat er aangeboden wordt als het om Personal Data Stores gaat. De complexiteit van het concept maakt dat misverstanden op de loer liggen.

Toch zegt 57% van de mensen dat ze gebruik zouden maken van een dienst om persoonlijke gegevens te beheren. De vraag is dus niet zo zeer of er ruimte is voor een PSD, maar vanuit welke toepassingsgebieden de PSD zal opkomen en groeien. Wie specialiseert in het bieden van een overzichtelijk geheel van persoonlijke data zou veel mensen achter zich kunnen scharen.

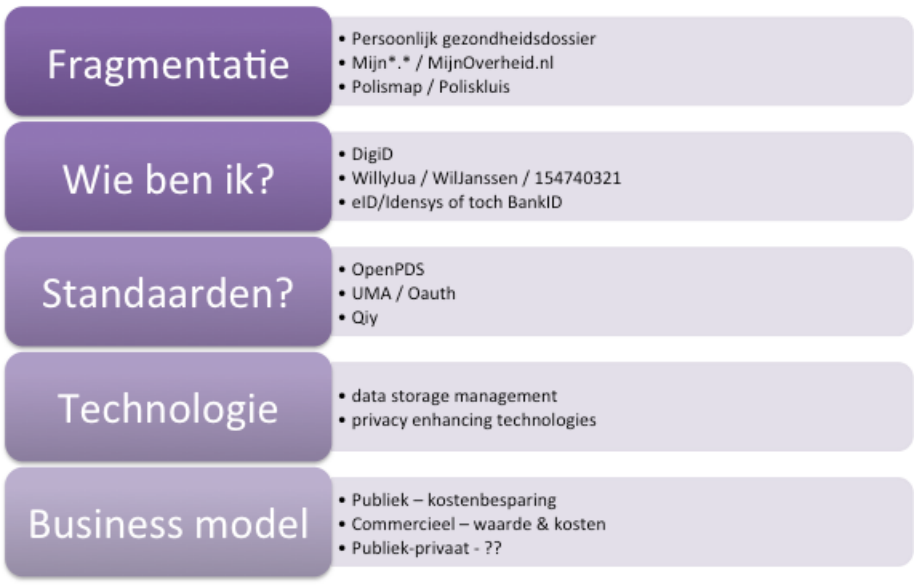
8 Drie stappen vooruit, twee achteruit?

8.1 VAN BELOFTE NAAR BEWAARHEID – DE KNELPUNTEN

We hebben gekeken naar de ontwikkeling van Personal Data Stores, in Nederland en in het buitenland. Daarbij hebben we gezien dat het concept al lange tijd bestaat, maar nog steeds niet echt is doorgebroken. Redenen daarvoor zijn maar beperkt van technische aard. De complexiteit van het concept en het onderliggende business model, met veel afhankelijkheden tussen overheid, bedrijfsleven, regulering en anderen, maakt de introductiestrategie onduidelijk. Ook is eenvoud van gebruik nog vaak ver weg, hetgeen adoptie in de weg staat. Er lijkt niet één weg te zijn die tot een gedragen introductie van Personal Data Stores leidt, al is de behoefte of potentie nadrukkelijk aanwezig. Wat zijn nu ingrediënten van een kansrijke strategie rond Personal Data Stores? En waar liggen de knelpunten?

Gelet op de behoefte aan controle over persoonlijke data en de economische winsten die kunnen worden behaald lijken PDS's veelbelovend. Organisaties kunnen concurreren op privacy en persoonlijke informatie door de juiste middelen te bieden. Naast economische winsten bieden PDS's kansen om vertrouwen van gebruikers te vergroten. Consumenten hebben vaak weinig besef wat er gebeurt met hun data, maar als zij zich hiervan bewust zijn ervaren zij hier meer profijt van. Maar weinig gebruikers beheren actief hun persoonlijke data, maar wanneer zij dit wel doen zijn zij gemiddeld twee keer meer bereid informatie te delen.

Als die kansen zo groot zijn, waar liggen dan de barrières? Die liggen op verschillende terreinen. Vanuit de consument gezien is de versnippering aan initiatieven een probleem. Er zijn veel aanbieders, ook van onderdelen van PDS's, allen met verschillende doelen, aanpakken, en verstrekte informatie. Dat kan een voordeel zijn, omdat kleine nicheoplossingen wellicht makkelijker worden geadopteerd, maar vooralsnog levert het eerder onduidelijkheid. Die onduidelijkheid is er ook rond authenticatie: toegang tot een PDS, met veel gevoelige informatie en diensten, moet met een goed authenticatiemiddel gebeuren. DigiD kan, zeker in combinatie met de veiligheid van een SMS, maar kan alleen voor publieke zaken, zorg en pensioenen. Het grootste deel van de private sector staat buiten spel en gebruikers worden dan ook geconfronteerd met een oerwoud aan identiteiten, wachtwoorden en wachtwoordconventies. Met eID/Idensys is er de belofte dat dit opgelost gaat worden, maar dat is nog maar sterk de vraag. Wellicht dat de banken met een BankID daar een oplossing in gaan bieden.



Figuur 24. Knelpunten in roadmap voor Personal Data Stores

In het algemeen is de hoeveelheid direct toepasbare standaarden op dit vlak beperkt. We zagen eerder OpenPDS en UMA/OAuth als relevante standaarden, en QiY als trust framework in ontwikkeling. Daarmee is de mate van standaardisatie nog zeer beperkt.

Een technische uitdaging is het effectief behouden van zoveel informatie in de tijd, ofwel *data storage management*. Denk hierbij aan opslag

en back-ups, maar ook aan adequate databeveiliging. Een verandering naar een gebruiker-centraal model van datamanagement heeft ook allerlei andere technische gevolgen, zoals een andere ontwikkeling van nieuwe applicaties. Om de privacy van gebruikers zoveel mogelijk te waarborgen, dienen bovendien allerlei technieken (*privacy enhancing technologies*) in PDS's te worden opgenomen.

Mogelijke gevolgen van de opkomst van PDS's kunnen liggen in nieuwe wet- en regelgeving en nieuwe markten, maar ook in een socio-technische revolutie in het datalandschap. Dit laatste verwijst naar een transitie van data- naar gebruiksmanagement, waarbij de gebruiker controle heeft over de eigen data.

Uiteindelijk zal dit moeten leiden tot een duurzaam business model. Dat kan in de publieke sector gevonden worden, al leert DigiD en de Berichtenbox dat ook daar het moeilijk is te komen tot een financieringsmodel. In de private sector zal een betaalde PDS absoluut mogelijk zijn, waarbij in het verdienmodel wel opgepast moet worden met rendement uit datahandel. Al staat de Nederlandse consument daar niet heel negatief tegenover, het kan zeker wel de perceptie kantelen in de media en dan niet naar de positieve kant.

8.2 EN NEDERLAND DAN?

Het laaghangend fruit

Wat de meeste mensen missen als het gaat om persoonlijk gegevens is inzicht, welke de organisaties gegevens hebben, welke type gegevens ze hebben en wat ermee gebeurt. Inzicht geven zou daarmee bovenaan de agenda moeten staan van PDS initiatieven. Bijvoorbeeld in de vorm van een intuïtief dashboard. Wie specialiseert in het bieden van een overzichtelijk geheel van persoonlijke data zou veel mensen achter zich kunnen scharen.

Daarnaast willen mensen kunnen sturen: er is een grote behoefte om zelf te kunnen bepalen wie er toegang heeft tot gegevens. Dit vertaalt zich ook in een behoefte naar meer controle: men wil gegevens kunnen bewerken en graag ook nog kunnen verwijderen.

De functies 'toegang', 'verwijderen' en 'bewerken', gecombineerd met inzicht, zouden de kern moeten zijn van een Personal Data Store. Geld of financieel gewin is geen succesfactor van betekenis. We kunnen dus niet verleiden tot gebruik via voordelen of gratis diensten. Het kan wellicht helpen, maar is niet doorslaggevend. Buiten PDS's zouden deze punten ook voor andere sociale platformen kunnen gelden.

Overheid aan zet?

Naast wetgeving is vertrouwen in een organisatie de belangrijkste drijfveer om gegevens te delen. Vertrouwen realiseren zou daarom hoog op de lijst moeten staan bij aanbieders van een PDS.

De overheidspartijen scoren hoog qua vertrouwen. Daarmee lijkt de rijksoverheid een goede partij om een dergelijk dienst in de markt te zetten, mogelijk voortbouwend op MijnOverheid. Echter is het hier niet altijd makkelijk om een technologisch innovatieve dienst te ontwikkelen. Een snellere weg naar succes zou zijn dat start-ups in deze sector een overheidspartij aan zich weten te verbinden. Dit zou mensen meer vertrouwen kunnen geven in de aangeboden dienst.

Verzekeraars en zorgverzekeraars starten, net als banken, vanuit een achterhoedepositie. Het vertrouwen is nog beperkt. Een trekkende rol vanuit hun positie ligt niet voor de hand. De introductiestrategie van, bijvoorbeeld, de Poliskluis, zal zorgvuldig moeten gebeuren en sterk moeten appelleren aan transparantie en controle om de vertrouwenskant te laten groeien. Mogelijk dat organisaties zoals de NPCF een rol kunnen spelen om het vertrouwen op voldoende niveau te krijgen, daar waar het gaat om het persoonlijk gezondheidsdossier. Een start vanuit een ISP, telco of vanuit retail, bijvoorbeeld bouwend vanuit een loyalty programma, ligt volgens ons onderzoek nog minder voor de hand.

Opmerkelijk is daarbij dat perceptie van vertrouwen sterk verschilt per land. De adoptie van een buitenlands initiatief in Nederland, al is dat concept in het buitenland succesvol, zal niet zonder slag of stoot gaan.

De zorg als springplank?

We hebben gezien hoe een Personal Data Store in de vorm van het Persoonlijk Gezondheidsdossier zorgconsumenten in staat stelt overzicht en controle te krijgen over hun medische gegevens; een typisch voorbeeld van een PDS in de zorg. Enkele voordelen van PDS's komen hierbij naar voren: meer en betere data leidt tot verbeterde dienstverlening, nieuwe inzichten en efficiënter datamanagement realiseert significante kostenbesparing, en het voorziet in een concrete wens van consumenten. Maar er bestaan nog belangrijke uitdagingen op technisch, organisatorisch, cultureel en juridisch vlak. Desalniettemin zou de zorg wel eens één van de eerste sectoren kunnen zijn die de PDS omarmt. Medische informatie ervaren mensen als intiem en belangrijk, wat de consument beweegt dit actief te beheren. Laagdrempelige elementen als de Blue Button kunnen hierin baanbrekend uitwerken. Betere informatie heeft direct effect op de zorgverlening en leidt daarmee tot een hogere kwaliteit van leven. Tenslotte hebben partijen als de overheid, zorgverleners, brancheorganisaties en verzekeraars vanuit hun zorgplicht niet-commerciële drijfveren om het PGD een succes te doen worden. Er zijn dan ook al verregaande initiatieven op dit gebied. De zorg kan daarom de eerste zijn die de belofte van het beheren van persoonlijke data inlost en als springplank dienen voor de revolutie van de PDS.

Een PDS strategie in zes punten

Samengevat kun je stellen dat in een ontwikkelpad voor Personal Data Stores een zestal punten meegenomen zouden moeten worden:

1. De overheid lijkt een sleutelrol te hebben. Profiteer van het voordeel dat de overheid nu geniet en werk samen, ook in private initiatieven.
2. Begin met een doelgroep met een noodzaak. Dat kan in een sector liggen of in een andere segmentatie. Mensen met langdurige zorg hebben baat bij een persoonlijk gezondheidsdossier. Werklozen profiteren van een open variant van hun werkmap. Bijklussende studenten met een lening hebben weer andere behoeften.
3. Pas op met kopiëren uit het buitenland. We halen nogal graag disruptieve voorbeelden uit het buitenland om die hier te introduceren. Net zo min als het japanse iMode een succes werd in Nederland, zal dat hoeven gelden voor Personal Data Stores. Daarvoor verschillen culturen te sterk.

Figuur 25: Zes punten van het ontwikkelpad van de PDS

4. Standaarden zijn op termijn van doorslaggevend belang. De vraag is echter of je er op kunt wachten. In een sector kun je starten en onderling afspraken maken. Hergebruik wat er al is, maar wacht niet op de ultieme open standaard. Dat zou nog wel eens lang kunnen duren.
5. Maak gebruik van de segmentatie die we hebben gezien. We weten dat er een grote groep mensen met een meer latente interesse is. Activeer hen. Behandel ze ook anders dan de adopters. En richt je energie niet op de sceptici.

6. En het allerbelangrijkst: begin met functionaliteit die zin heeft en waar mensen iets aan hebben. Een PDS is een complex concept in totaliteit. Begin dan klein, met nuttige dingen. Een digitale brievenbus valt daar niet onder, dat is een prettig bijeffect. Een inzage en correctiemogelijk is nuttiger, net als proactief attenderen op betere verzekeringsproducten, gewijzigde persoonlijke situaties etc.

Onbekend maakt onbemind

Op dit moment roept het beheren van eigen data op een centrale plaats nog weinig beelden op bij mensen. Het is dus van belang om te zorgen dan mensen snappen wat er aangeboden wordt als het om Personal Data Stores gaat. De complexiteit van het concept maakt dat misverstanden op de loer liggen. Ook al willen mensen wel inzicht in eigen gegevens, als ze niet begrijpen dat deze diensten dat inzicht bieden zullen ze het niet gaan gebruiken.

Daar komt bij dat men nog maar nauwelijks eigen gegevens controleert. Ook al willen we inzicht in gegevens, het daadwerkelijk opzoeken en iets mee doen is een tweede. Er moet dus een duidelijk voordeel zijn om het wèl te gaan doen. Zeker als het moeilijk gemaakt wordt om überhaupt inzicht te krijgen en instellingen vaak verstopt zitten.

Toch zegt 57% van de mensen dat ze wel gebruik zouden maken van een dienst om persoonlijke gegevens te beheren. Er is dus zeker draagvlak voor dit soort diensten. Dat blijkt ook uit de tevredenheid van mensen die een persoonlijk gezondheidsdossier gebruiken en de gebruikers van MijnOverheid. De vraag is dus niet zo zeer of er ruimte is voor een PSD, maar vanuit welke toepassingsgebieden de PSD zal opkomen en groeien.

9 Bronnen en achtergronden

1. Beuger, Bas & Wil Janssen (red). Vorm geven aan de social enterprise. InnoValor. 2014.
2. Boston Consulting Group. The Value of our digital identity, November 2012.
3. CTRL-Shift (2011). The new personal data landscape.
4. CTRL-Shift (2014). Personal information management services – an analysis of an emerging market.
5. De Montjoye, Y. A., Wang, S. S., Pentland, A., Anh, D. T. T., & Datta, A. (2012). On the Trusted Use of Large-Scale Personal Data. IEEE Data Eng. Bull., 35(4), 5-8.
6. Derikx, Sebastiaan. Mobile Insurance - Overcoming Privacy Concerns in the Consumer Use of Insurance Services based on Mobile Technologies. Master Thesis TU Delft, 2015.
7. Desan Research Solution. UWV Klantfgerichtheidsmonitor, 2015.
8. GfK (2014). Survey on data privacy and trust. Zie http://www.gfk.com/Documents/GfK-Privacy-Survey.pdf
9. Hardjono, T., Greenwood, D., & Pentland, A. (2013). Towards a trustworthy digital infrastructure for core identities and personal data stores. In *Global Forum on Identity*.
10. Informatie, Jaargang 57, nummer 6 – augustus 2015. Themanummer Privacy en de Europese Wetgeving.
11. InnoValor. Nederlanders over persoonlijke data. Rapport Digital We, september 2015.
12. I&O Research. De kwaliteit van de overheidsdienstverlening 2014. I&O research i.o.v. Ministerie van BZK en Ministerie van EZ, januari 2015. Rapport 2015-2079
13. Kearns, D. (2009, July 7). Five datasets of the personal data store. *Networkworld.com.* Zie http://www.scientificamerican.com/article/3-projects-prove-privacy-is-not-dead/
14. Leber, J. (2014, July 23). MIT wants you to own your own data, not give it away. *Fastcoexist.com.* Zie http://www.fastcoexist.com/3033414/mit-wants-you-to-own-your-own-data-not-give-it-away
15. Liberty Global (November 2012). The value of our digital identity.
16. Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., & Boneh, D. (2012). A critical look at decentralized personal data architectures. *arXiv preprint arXiv:1202.4503*.
17. Naughton, J. (2015, February 1). Fightback against internet giants' stranglehold on personal data starts here. *The Guardian.* Zie http://www.theguardian.com/technology/2015/feb/01/control-personal-data-databox-end-user-agreement
18. Newcom. Persoonlijke data onder Nederlanders. Neil van der Veel & Bob Sival. Juni 2015.
19. NPCF, Visie persoonlijk gezondheidsdossier. Juni 2013.
20. NPCF, https://www.npcf.nl/Documenten/meldacties/Rapport_PGD_definitief.pdf. April 2015
21. Osterwalder, A., & Y. Pigneur. Business model generation.
22. Owano, N. (2013, October 7). OpenPDS software focuses on control of personal data. *Phys.org.* Zie http://phys.org/news/2013-10-openpds-software-focuses-personal.html
23. Payment Service Directive 2 for Dummies, Pascal Spelier. Emerce, augustus 2015.
24. Social physics (2014, January 18). Open PDS: Privacy through Personal Data Stores. YouTube, https://www.youtube.com/watch?v=JOgwMzF9Zqo
25. Strong, C. (2013, October 8). Cloud it: Barclay's bold move into personal data stores. *Huffington Post.* Zie http://www.huffingtonpost.co.uk/colin-strong/barclays_b_4055856.html
26. The Information Daily (2014, June 17). Personal information management services market to reach 16.5b. *The Information Daily.* Zie http://www.theinformationdaily.com/2014/06/17/personal-information-management-services-market-set-to-reach-165
27. TNO, Privacy beleving op het internet in Nederland. Roosendaal et. al., februari 2015. TNO 2015 R10276
28. Van Kleek, Max and O'Hara, Kieron (2014). The future of social is personal: the potential of the personal data store. In,*Daniele Miorandi, Vincenzo Maltese, Michael Rovatsos, Anton Nijholt & James Stewart (eds.), Social Collective Intelligence: Combining the Powers of Humans and Machines to Build a Smarter Society.* Berlin, DE, Heidelberg, DE,Springer-Verlag, 125-158. (doi:10.1007/978-3-319-08681-1_7).
29. Venkatesh, V.; Morris; Davis; Davis (2003), "User Acceptance of Information Technology: Toward a Unified View", MIS Quarterly 27 (3), pp. 425–478

30. Wired (2012, May 30). Personal data stores will liberate us from a toxic privacy battleground. *Wired.* Zie http://www.wired.co.uk/news/archive/2012-05/30/ideas-bank-personal-data-stores
31. World Economic Forum (February 2013). Unlocking the value of personal data: from collection to usage.
32. World Economic Forum (June 2011) Personal Data the 'new oil' of the 21st century
33. World Economic Forum (May 2014). Rethinking personal data.

Websites:

http://hub.personaldataecosystem.org/wagn/Personal_Data_Store

http://en.wikipedia.org/wiki/Higgins_project

http://wiki.eclipse.org/PDS_Architecture

http://equalsdrummond.name

http://blog.joeandrieu.com/

http://www.gfk.com/trustsurvey

http://www.nu.nl/internet/4062623/miljoenen-overheidsmedewerkers-vs-getroffen-datalek.html

http://www.newcom.nl/socialmedia2015

https://www.npcf.nl/nieuws/nieuws/694-wie-eenmaal-een-pgd-heeft-wil-nooit-meer-zonder

https://www.vzvz.nl/page/Zorgconsument/Links/Over-VZVZ/Feiten-en-cijfers

www.datacoup.com