PBLQ
HEC

Het versterken van de informatiepositie van de burger

Verkenning naar nieuwe (verplichte) functionaliteiten van MijnOverheid

Eindrapport

Ellen Boschker
Theo Hooghiemstra
Mano Radema
Dirk Schravendeel
Cornelis van der Werf

project 2395
versie 1.0
datum 12 september 2012

voor een sterke publieke sector

Samenvatting

Beleidscontext
In het rapport iOverheid van de WRR[1] wordt ingegaan op de inzet van ICT door de overheid en de ontwikkelingen van een elektronische overheid naar een informatie-Overheid of iOverheid.
De WRR constateert dat digitale datastromen een centrale rol zijn gaan vervullen in het verkeer tussen burgers, overheid en private partijen. Deze ontwikkeling heeft vele positieve gevolgen en biedt veel kansen voor het sneller en goedkoper uitwisselen van gegevens en informatie. Daarnaast staat de overheid voor de uitdaging om zorg te dragen voor de juistheid, zorgvuldigheid en veiligheid van de digitale informatiestromen waar de overheid zelf gebruik van maakt. De WRR bepleit dat het inzage- en correctierecht van burgers, geregeld in de Wet Bescherming Persoonsgegevens, verder gefaciliteerd moet worden.

In de kabinetsreactie op het rapport iOverheid geeft het kabinet aan dat *zij de weerbaarheid van burgers wil vergroten door versteviging van het inzage- en correctierecht*. Het kabinet wil daarmee de informatiepositie van de burger versterken en heeft in haar reactie een verkenning aangekondigd waarin zij wil onderzoeken hoe de informatiepositie van de burger door verdere uitbreiding van de functionaliteiten van de site MijnOverheid.nl en mogelijke verplichting daarvan kan worden versterkt. In opdracht van het ministerie van BZK heeft PBLQ HEC (Het Expertise Centrum) in samenwerking met PBLQ Zenc dit verkennend onderzoek uitgevoerd. De centrale vragen daarbij zijn:

1. Welke additionele functionaliteiten van MijnOverheid kunnen bijdragen aan het versterken van de informatiepositie van de burger?
2. Kunnen, en zo ja op welke wijze, overheidsorganisaties verplicht worden aan te sluiten op de functionaliteiten van MijnOverheid?
3. In hoeverre kunnen de additionele functionaliteiten van MijnOverheid en verplichtstelling daarvan invulling geven aan artikel 18 van de Wet algemene bepalingen burgerservicenummer?

Nieuwe functionaliteiten
In het kader van dit onderzoek zijn de volgende nieuwe functionaliteiten, die de informatiepositie van de burger zouden kunnen versterken, onderzocht:

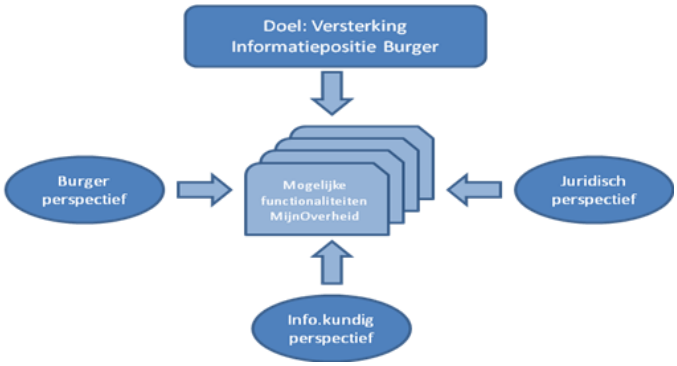
1. Inzage in gegevens
2. Inzage in gegevensverkeer
3. Verzoeken om correctie
4. Mogelijkheid tot actief delen van gegevens
5. Vermelding verwijderingstermijn
6. Een module met contactgegevens

---

[1] Wetenschappelijke Raad voor het Regeringsbeleid (2011). *iOverheid.* Den Haag / Amsterdam: WRR/Amsterdam University Press

Onderzoeksopzet
Kern van dit verkennend onderzoek is de vraag of en hoe de informatiepositie van de burger versterkt kan worden door nieuwe functionaliteiten toe te voegen aan de site MijnOverheid. Daarbij worden drie perspectieven gehanteerd:

- Het perspectief van de burger (wensen en verwachtingen);
- Het juridisch perspectief (rechten en principes);
- Het informatiekundig perspectief (mogelijkheden en consequenties).



Via vier burgerpanels is onderzocht of burgers van mening zijn of nieuwe functionaliteiten van MijnOverheid hun informatiepositie versterkt. Daarnaast is via interviews en literatuurstudie nagegaan wat zowel de mogelijkheden als de implicaties op juridisch, organisatorisch, technisch en financieel gebied zijn van de in de kabinetsreactie genoemde nieuwe functionaliteiten van MijnOverheid. Het onderzoek gaat tevens in op de vraag of, en zo ja, op welke wijze, overheidsorganisaties verplicht kunnen worden om via MijnOverheid een of meer van de hierboven genoemde mogelijke functionaliteiten aan te bieden en of de nieuwe functionaliteiten invulling kunnen geven aan artikel 18 Wabb.

MijnOverheid en relatie met de MijnDomeinen
MijnOverheid biedt momenteel inzage in persoonlijke gegevens, een berichtenbox en de lopende zaken van een tiental organisaties (waaronder 4 gemeenten) en registraties, zoals de Gemeentelijke Basis Administratie (GBA), Donorregistratie, het persoonlijke pensioenoverzicht en het kentekenregister.
Mijnoverheid heeft zo'n 250.000 accounts en het aantal unieke bezoeken ligt rond de 50.000 per maand.

MijnOverheid is gepositioneerd naast de zogenaamde MijnDomeinen van verschillende uitvoeringsorganisaties, zoals MijnDUO en MijnSVB. Deels biedt MijnOverheid inzage in gegevens die niet op andere MijnDomeinen zijn te vinden (voorbeeld: Gemeentelijke Basisadministatie Gegevens). MijnOverheid biedt tot nu toe ook een overzicht van een beperkte set gegevens die een aantal uitvoeringsorganisaties van de burger hebben, en is een 'doorverwijzer' naar de MijnDomeinen voor meer detailinformatie. De uitvoeringsorganisaties zelf registreren een veelvoud aan detailinformatie, die ze voor een deel via hun MijnDomeinen aanbieden, en burgers kunnen bij de uitvoeringsorganisaties terecht voor digitale transacties met de betreffende uitvoeringsorganisatie. De MijnDomeinen dan wel andere digitale voorzieningen bieden voor dit laatste de juiste context (bijvoorbeeld de genoemde relevante detailinformatie zoals persoonsgebonden proces- en statusinformatie en daarnaast informatie over wet- en regelgeving). Bovendien is de Wet bescherming persoonsgegevens – waarin inzage, correctie en verwijdering is geregeld – van toepassing op de relatie tussen burger en de verantwoordelijke voor de verwerking van persoonsgegevens en is er voor deze functionaliteiten geen juridische basis om dit (uitsluitend) via MijnOverheid te regelen.

Uitkomsten burgerperspectief
Voor dit onderzoek zijn vier burgerpanels georganiseerd, op basis waarvan zeer bruikbare informatie naar voren is gekomen omtrent de houding en verwachtingen van burgers. Deze kwalitatieve resultaten zijn vanzelfsprekend niet zondermeer generaliseerbaar. Het blijkt dat de burgers in het onderzoek het belangrijk vinden te weten welke gegevens en informatie de overheid over hen registreert. Hoewel het begrip informatiepositie vrij abstract is, blijken de meeste burgers hier wel degelijk een beleving bij te hebben. Over het algemeen hebben ze het beeld dat de overheid veel van hen weet, maar dat zij lang niet altijd weten wat de overheid van hen weet.

Daarom vinden vrijwel alle burgers in de burgerpanels inzage in gegevens en gegevensverkeer en verwijderingstermijnen van belang om hun informatiepositie ten opzichte van de overheid te versterken. Ook de mogelijkheid om een correctieverzoek te kunnen doen past daarbij. Burgers geven aan dat inzage in hun persoonlijke kerngegevens handig is, maar dat het eventueel verstrekken van gegevens op een te gedetailleerd niveau waarschijnlijk tot een informatie-overload zou leiden. Over een eventuele module met contactgegevens en het actief delen van gegevens met derden zijn de burgers minder positief. De meerwaarde voor hun informatiepositie wordt minder gezien.

Idealiter is er enige voorkeur voor het tonen van de gegevens in MijnOverheid. De panelleden ondersteunen echter zowel een ‘dikke’ als een ‘dunne’ variant van MijnOverheid, waarbij MijnOverheid in de ‘dikke’ variant het unieke loket is en in de ‘dunne’ variant MijnOverheid naast de MijnDomeinen functioneert.

Burgers die ervaringen hebben met het (laten) aanpassen van onjuiste gegevens of informatie geven aan dat ze in aanvulling op de inzage- en correctiemogelijkheid eigenlijk liever een soort ‘accountmanager’ hebben die voor hen uitzoekt wat de oorzaak is van het probleem, en hen begeleidt met het oplossen van het probleem. Hier is met name sprake van wanneer er meerdere overheidsinstanties bij betrokken zijn, en het voor de burger niet altijd duidelijk is waar de oorzaak van het probleem zit, of wie de beheerder is van het ‘onjuiste’ gegeven.

Uitkomsten juridisch perspectief
De Wet bescherming persoonsgegevens (Wbp) regelt het recht van de burger op inzage, correctie en verwijdering van persoonsgegevens in registraties van overheidsorganisaties. Op grond van de Wbp dient aan burgers in ieder geval inzicht gegeven te worden in het doel van de gegevensverwerking en de overige ontvangers c.q. gebruikers van persoonsgegevens, aangevuld met gepersonaliseerde gegevens op kerngegevensniveau waarop een besluit is gebaseerd. Op grond van jurisprudentie dient de specifieke wens van een burger om op meer gedetailleerd niveau inzage te krijgen gehonoreerd te worden.

Overheidsorganisaties zijn niet verplicht om (bijvoorbeeld via MijnOverheid) actief, uit eigen beweging, gegevens uit hun registratie(s) aan burgers te verstrekken. Ook mogen zij op basis van goede argumenten (bijv. onevenredig hoge kosten) een verzoek om inzage, correctie of verwijdering weigeren. Het CBP, en in uiterste instantie de rechter, bepaalt zo nodig of het echt om goede argumenten gaat. Daarnaast is het verplicht om een bewaartermijn vast te stellen of de bewaartermijn te volgen van een toepasselijke sectorwet. Dit betekent dat ontsluiting van persoonlijke gegevens in de MijnDomeinen en aansluiting bij MijnOverheid op dit moment gebeurt op eigen initiatief en overtuiging van de individuele overheidsorganisaties.

Vanuit juridisch perspectief vergt vrijwillig gebruik van de functionaliteiten van MijnOverheid – zowel van de zijde van de burger als van de bestuursorganen – geen aanpassing van wetgeving. In dat geval is de positie van MijnOverheid met de minister van BZK als verantwoordelijke – slechts beperkt tot de enkele persoonsgegevens die MijnOverheid zelf bijhoudt op verzoek van de burger. De inzage-, correctie- en verwijderingsverzoeken hebben in de praktijk echter meestal betrekking op de bestanden van de uitvoerende bestuursorganen. Deze bestuursorganen zijn zelf verantwoordelijke in de zin van de Wbp en mogen binnen de bestaande wettelijke kaders hun eigen afweging maken. Indien, via het toevoegen van functionaliteiten aan MijnOverheid, de bestuursorganen verplicht worden tot medewerking aan verzoeken van burgers, is aanvullende wetgeving vereist. Ook indien MijnOverheid zonder toestemming van de burger persoonsgegevens wil verwerken is aanvullende wetgeving vereist.

Uitkomsten informatiekundig perspectief
In het (landelijke) informatiebeleid is de afgelopen jaren weinig expliciet aandacht gegeven aan het versterken van de informatiepositie van burgers. Dit perspectief, geconcretiseerd in mogelijke nieuwe functionaliteiten van MijnOverheid, werd door een aantal respondenten ervaren als een geheel nieuwe invalshoek waar men ter plekke een oordeel over moest vormen. Mede daardoor konden zij alleen heel globaal uitspraken doen over de informatiekundige, technische, organisatorische en financiële consequenties van de voorgestelde functionaliteiten.

De consequenties die het bieden van inzage in gegevens heeft, verschilt sterk met het detailniveau waarop inzage geboden dient te worden. Om de burger in staat te stellen zelf vast te stellen waar foute gegevens zijn gebruikt, is inzage op een gedetailleerd gepersonaliseerd niveau nodig. Dit vergt bij de uitvoeringsorganisaties ingrijpende organisatorische en technische aanpassingen met daarmee samenhangende prohibitief hoge kosten. Inzage bieden in de kerngegevens waarop een besluit is gebaseerd sluit aan bij de transactiegerichte of zaakgerichte benadering die in het beleid (iNUP) en door partijen zelf wordt gehanteerd. De wenselijkheid en haalbaarheid verschilt per organisatie. De ene organisatie is veel verder met de invoering daarvan dan de andere. Ook zal nader moeten worden onderzocht wat wordt verstaan onder kerngegevens. Inzage bieden in de gebruikte gegevens is verder in de ogen van de uitvoeringsorganisaties onvoldoende om burgers in staat te stellen mogelijke problemen die ze ondervinden zelf op te lossen. De overheid zal in hun ogen daartoe met een vorm van accountmanagement en aangescherpte verantwoordelijkheden de burgers dienen te ondersteunen.

Inzage bieden in gegevensstromen lijkt voor basisregistraties en voor organisaties die gegevensverkeer faciliteren (zoals bijvoorbeeld BKWI) haalbaar te zijn. De gegevens zijn beschikbaar en de benodigde inspanningen hebben betrekking op het ontsluiten via MijnOverheid. Uitvoeringsinstellingen en mede-overheden zijn echter in het geheel niet bezig met het bieden van inzage in het gegevensverkeer en zullen daarvoor verstrekkende, complexe en daardoor prohibitief dure aanpassingen moeten doorvoeren.

Naar de mening van de respondenten dient een burger op een eenvoudige wijze een correctieverzoek te kunnen indienen op de gegevens die getoond worden in MijnOverheid, dan wel in de MijnDomeinen door de uitvoeringsorganisaties zelf. Dit correctieverzoek zou (wellicht met MijnOverheid als doorgeefluik) bij de betreffende dienstverlener ingediend moeten worden. Daarbij is het ook zaak geen valse verwachtingen te wekken: bijna altijd dient de uitvoeringsorganisatie bestaande regels te volgen bij het vaststellen van gegevens en kan niet zondermeer tegemoet gekomen worden aan het verzoek van de burger.

In de bestaande dienstverleningspraktijk is er nauwelijks sprake van enige sense of urgency als het gaat om verwijderen van gegevens. Men ondervindt zelf nauwelijks problemen en wijst erop dat voorbeelden om het

belang van tijdige verwijdering van gegevens te adstrueren meestal op de domeinen zorg en controle betrekking hebben. Gericht aanpakken van de wel bestaande problemen in de dienstverlening heeft de voorkeur boven een generieke aanpak.

De mogelijke functionaliteit van een module met contactgegevens wordt over het algemeen benaderd vanuit het perspectief en het belang van de overheid zelf. Er zijn bijvoorbeeld besparingen mogelijk wanneer de burger verplicht is één rekeningnummer in haar relatie met de overheid te gebruiken. Verondersteld wordt dat de burger het ook prettig zal vinden om één keer op één plaats contactgegevens te verstrekken die vervolgens door de hele overheid worden gebruikt.

Op de mogelijke functionaliteit actief delen van gegevens wordt soms positief, soms negatief gereageerd. In ieder geval is het zaak het onderscheid tussen publiek en privaat gebruik van gegevens scherp te houden. Sommige uitvoeringsinstellingen en mede-overheidsorganisaties veronderstellen dat burgers voordelen van de functionaliteit zullen hebben, anderen vrezen dat hun informatiepositie er eerder door zal verzwakken.

Om te bereiken dat de nieuwe functionaliteiten gerealiseerd worden door *alle* uitvoeringsinstellingen – via MijnOverheid en/of de MijnDomeinen -en de decentrale overheden is een (wettelijke) verplichting noodzakelijk. Vooraf dient in het bestuurlijke besluitvormingsproces geborgd te worden dat de verplichting ook praktisch uitvoerbaar is.

Het is mogelijk en het heeft voordelen om via MijnOverheid te voldoen aan de verplichting van de staat om het gebruik van het burgerservicenummer inzichtelijk te maken (artikel 18 Wabb).

Conclusies en beantwoording onderzoeksvragen

1. *Welke additionele functionaliteiten van MijnOverheid kunnen bijdragen aan het versterken van de informatiepositie van de burger?*

Wanneer de juiste voorwaarden voor succes gehanteerd worden is het mogelijk om met behulp van nieuwe functionaliteiten via MijnOverheid en/of de MijnDomeinen de informatiepositie van burgers te versterken.

   a. Het gaat dan om *'inzage in gegevens'*, *'inzage in gegevensverkeer'*, *'verzoeken om correctie'* en *'het vermelden van de verwijderingstermijn'*.
   b. De functionaliteiten *'module met contactgegevens'* en het *'actief delen van gegevens met derden'* dragen niet zondermeer bij aan het versterken van de informatiepositie van de burger.
   c. Burgers geven aan dat zij ook de mogelijkheid willen hebben om *gegevensuitwisselingen te stoppen* of *vooraf toestemming te geven* voor een gegevensuitwisseling. De juridische en informatiekundige consequenties van een dergelijke functionaliteit zijn niet onderzocht, maar zijn naar verwachting omvangrijk.

Voor het versterken van de informatiepositie van burgers volstaat het presenteren van de door overheidsorganisaties gehanteerde kerngegevens op persoonsniveau. De huidige Wbp biedt hiervoor de wettelijke basis, zij het dat hierin geen verplichting voor overheidsorganisaties zit om gegevens actief en voor alle burgers inzichtelijk te maken. Om burgers in staat te stellen zelf gegevensproblemen op te lossen is een gedetailleerder inzicht nodig in de onderliggende gegevens en gegevensstromen waarop de kerngegevens gebaseerd zijn. Dit laatste is echter buitengewoon complex en kostbaar en niet op korte termijn te realiseren.

Informatie alleen is niet voldoende voor versterking van de informatiepositie van de burger. Met name in situaties waarin de burger een (gegevens)probleem heeft met de overheid, is het voor de burger van belang

een eventuele onjuistheid in de registraties te laten corrigeren. Het onderzoek wijst uit dat inzage in gegevens en verzoek tot correctie niet afdoende zijn om (gegevens)problemen op te lossen. Een soort accountmanager en/of een gegevensautoriteit (een partij die ervoor zorg draagt dat alle partijen in de keten hun verantwoordelijkheid waarmaken) kan hierbij behulpzaam zijn. De wenselijkheid en haalbaarheid daarvan vraagt nader onderzoek.

Indien MijnOverheid en/of de MijnDomeinen een belangrijke rol en plaats krijgen in het versterken van de informatiepositie van burgers ontstaat een nieuwe serviceconcept. De burger heeft *inzage* in hoe hij bij de overheid geregistreerd staat, wat er over hem wordt uitgewisseld en wanneer gegevens verwijderd worden. De burger heeft *invloed* / *regie* door correctieverzoeken in te dienen, toestemming voor het uitwisselen van gegevens te geven en berichten met de overheid uit te wisselen. De burger kan in probleemgevallen geholpen worden door duidelijk te maken bij welke organisatie hij daarvoor terecht kan. MijnOverheid functioneert als portaal voor de zogenaamde MijnDomeinen waarlangs burgers transacties met overheidsorganisaties verrichten. Belangrijke aandachtspunten hierbij zijn:

a. Een dergelijk service-concept is informatiekundig zeker niet van de ene op de andere dag te realiseren.
b. Het dient volstrekt helder te blijven dat MijnOverheid als ontsluitingsmechanisme en ‘doorverwijzer’ fungeert maar op geen enkele manier in de verantwoordelijkheid van de organisaties treedt voor de kwaliteit van de gegevens, het doorvoeren van correcties en het oplossen van problemen. Dat is ondermeer nodig om de relatie tussen verantwoordelijke en betrokkene die centraal staat in de Wbp ondubbelzinnig in stand te houden.
c. Er dient aandacht te zijn voor een voldoende hoog authenticatie-niveau; het moet onomstreden duidelijk zijn dat alleen de burger inzage heeft in zijn *eigen* gegevens en dat gegevens niet voor andere doeleinden gebruikt worden.
d. Verdere definiëring van kerngegevens en detailgegevens en de vraag welke van deze gegevens in MijnOverheid dan wel in de MijnDomeinen dan wel in beide worden gepresenteerd.
e. De mate waarin diversiteit in oplossingen bij de verschillende uitvoeringsorganisaties mogelijk en/of gewenst is. De vraag naar mogelijke variatie moet afgewogen worden langs burger-informatiekundig en juridisch perspectief.

Verder geldt dat binnen de domeinen zorg en controle en binnen de controleactiviteiten die onderdeel zijn van de dienstverlening, de informatieprocessen anders van aard zijn. Niet alleen juridisch, maar ook qua betekenis voor burgers. De bevindingen uit het rapport zijn niet zondermeer toepasbaar op deze domeinen.

Ook ontstaat door het combineren en bewerken van gegevens de mogelijkheid van ‘profiling’. Als het gaat om profiling, heeft een burger niets aan inzage in gegevens en verzoeken om correctie. In het onderzoek is de vraag naar voren gekomen hoe de informatiepositie van de burger in deze gevallen beschermd en versterkt kan worden.

2. Kunnen, en zo ja op welke wijze, overheidsorganisaties verplicht worden aan te sluiten op de functionaliteiten van MijnOverheid?

Voor het versterken van de informatiepositie van burgers is het van belang dat *alle* overheidsorganisaties inzage geven in gegevens, gegevensverkeer en de verwijderingstermijn en tevens de mogelijkheid bieden tot het digitaal indienen van een correctieverzoek, ongeacht de vraag of dit gerealiseerd wordt via MijnOverheid en/of de MijnDomeinen. Het huidige juridische en wettelijke kader kent daartoe geen verplichting. Uit het onderzoek komt naar voren een verplichting in enigerlei vorm, met bestuurlijke afspraken over de wijze van

realisatie ervan, nodig is om de gewenste resultaten te boeken.

3. *In hoeverre kunnen de additionele functionaliteiten van MijnOverheid en verplichtstelling daarvan invulling geven aan artikel 18 van de Wet algemene bepalingen burgerservicenummer?*

Het is mogelijk en het heeft voordelen om via MijnOverheid te voldoen aan de verplichting van de staat om het gebruik van het burgerservicenummer inzichtelijk te maken.

Succesfactoren voor het vervolg

Deze verkenning biedt een perspectief op de mogelijkheden om de informatiepositie van burgers te versterken door een aantal nieuwe of verbeterde functionaliteiten in MijnOverheid en/of de MijnDomeinen ter beschikking te stellen aan burgers. Daarmee is niet gezegd dat een en ander eenvoudig te realiseren is. Alvorens gekomen kan worden tot een uitvoerbaar implementatieplan dient enerzijds een afweging gemaakt te worden tussen de drie verschillende perspectieven (burger, juridisch, informatiekundig) en anderzijds nog veel uitgezocht en verkend te worden, waarbij deze verkenning als uitgangspunt kan dienen. Op basis van het onderzoek en de gevoerde gesprekken met stakeholders kunnen de volgende factoren benoemd worden die bepalend zullen zijn voor een succesvol vervolg:

1. **Uitwerking en implementatie van functionaliteiten**
   - Deze verkenning geeft een globaal beeld van de nieuwe functionaliteiten. Tijdens het onderzoek viel op dat respondenten vaak heel verschillende beelden hebben van de nieuwe functionaliteiten. Het is noodzakelijk dat deze eerst conceptueel, functioneel en technisch verder worden uitgewerkt. Die uitwerking is zowel nodig per functionaliteit, als in samenhang. Er zijn aanzienlijke verschillen tussen de functionaliteiten waar het de partijen betreft die betrokken zijn, de technische en juridische vraagstukken die opgelost moeten worden, en de startpositie van betrokken partijen.
   - De praktische uitvoerbaarheid van de functionaliteiten en een eventuele verplichting daarvan, dient vooraf door middel van pilots en uitvoeringstoetsen te zijn vastgesteld.
   - Er dient helderheid geschapen te worden over de financiële haalbaarheid en de financiering van de eenmalige ontwikkelkosten en de structurele beheerkosten van de eventuele nieuwe functionaliteiten.

2. **Positionering MijnOverheid en MijnDomeinen**
   - MijnOverheid en de MijnDomeinen zullen meer in samenhang beschouwd moeten worden, waarbij een zorgvuldige positionering van MijnOverheid ten opzichte van de MijnDomeinen noodzakelijk is. Op dit moment is MijnOverheid een voorziening (‘doorverwijzer’) die een (beperkt) overzicht biedt en toegang geeft tot (een aantal) MijnDomeinen. Er is flexibiliteit nodig in het tempo, en wellicht ook qua functionaliteiten, waarmee organisaties hun gegevens ontsluiten via de MijnOverheid en/of de MijnDomeinen. Sommige organisaties zullen aanzienlijke investeringen in hun gegevenshuishouding en de realisatie van hun MijnDomein moeten doen om goed aan te kunnen sluiten op MijnOverheid.
   - Essentieel is het uitgangspunt dat MijnOverheid geen verantwoordelijkheden overneemt van de uitvoeringsinstellingen en basisregistraties. Dat is nodig om de relatie tussen verantwoordelijke en betrokkene die centraal staat in de Wbp intact te laten. Wanneer partijen hun verantwoordelijkheid niet waarmaken dienen ze daarop te worden aangesproken door een bevoegde instantie.

3. **Bestuurlijk draagvlak**
   - Het is van belang dat het ministerie van BZK en de betrokken uitvoeringsorganisaties en decentrale overheden binnen de bestaande governance-structuur van MijnOverheid (ondermeer de

Programmaraad e-Overheid voor burgers en het Bestuurlijk Overleg MijnOverheid) een gezamenlijke afweging maken tussen de drie onderscheiden perspectieven (burger, juridisch, informatiekundig).

- Omdat er, zowel bestuurlijk als juridisch, op dit moment op geen verplichting bestaat om de functie “persoonlijke gegevens” van MijnOverheid te gebruiken is het van belang dat er bestuurlijk draagvlak ontstaat voor de realisatie van eventuele nieuwe functionaliteiten in, MijnOverheid en/of de MijnDomeinen. Daartoe dient het versterken van de informatiepositie van de burger de nodige politiek-bestuurlijk prioriteit te krijgen.
- Daarbij dient wel rekening gehouden te worden met de reeds bestaande bestuurlijke afspraken die lopen tot 2015. De onderzochte organisaties richten zich momenteel op het nakomen van de prestatie-afspraken die in de Bestuurlijke Regiegroep Dienstverlening en e-Overheid zijn gemaakt en in het iNUP zijn gespecificeerd. Daarin zijn ook prestatie-afspraken opgenomen over MijnOverheid (met name het onderdeel Berichtenbox).

1. Inleiding

1.1 Aanleiding

Sinds jaar en dag verzamelen overheidsorganisaties informatie over burgers en ondernemers om publieke taken te kunnen uitvoeren. De toenemende inzet van ICT maakt dat er een overheid is ontstaan die wordt gekenmerkt door informatiestromen en –netwerken: de iOverheid. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) beschrijft de iOverheid als een geheel van actoren die ICT gebruiken om processen uit te voeren, gericht op dienstverlening, het bieden van zorg en het uitvoeren van controle. Daarbij worden gegevens verzameld bij burgers, maar ontstaan ook informatiestromen tussen organisaties. Gegevens worden verrijkt, gebruikt in andere contexten dan waarin ze verzameld zijn en vormen de basis voor het maken van profielen.

Deze informatiestromen bepalen de nieuwe mogelijkheden, maar ook de afhankelijkheden en de kwetsbaarheden voor zowel de overheid als haar burgers. Binnen de iOverheid zoals die nu functioneert vervuilt informatie, is niet altijd duidelijk wie verantwoordelijk is voor informatiestromen en raken burgers, bedrijven en ook instanties binnen de overheid zelf, verstrikt in de datakluwen van de overheid (WRR, 2011: 13-14). De WRR bepleit een betere afweging tussen enerzijds stuwende beginselen als efficiency en veiligheid en verankerende beginselen als privacy en keuzevrijheid. Deze balans moet bewaakt worden vanuit procesmatige beginselen als accountability en transparantie. Als één van de te nemen maatregelen bepleit de WRR het inzage- en correctierecht voor burgers verder te faciliteren.

In het pakket maatregelen dat het kabinet in haar reactie op het rapport aankondigt, zet het stevig in op maatregelen om de burgers zelf zo goed mogelijk toe te rusten tegen problemen die voortvloeien uit de verwerking van hun persoonsgegevens in digitale datastromen in de publieke sector, opdat deze daadwerkelijk voor zichzelf kunnen opkomen. De weerbaarheid van burgers zal worden vergroot door versteviging van het inzage- en correctierecht (Kabinetsreactie, 2011: 6)). Daarbij wordt gedacht aan het uitbreiden van de inzagemogelijkheden en functionaliteiten van de huidige website MijnOverheid.nl. Het kabinet verwacht dat mede daardoor een verschuiving zal optreden in de “checks and balances” in de relatie tussen overheid en burger, en daarmee de informatiepositie van de burger versterkt zal worden.

Op dit moment biedt MijnOverheid – dat gepositioneerd is naast verschillende MijnDomeinen van verschillende uitvoerings-organisaties, zoals MijnDUO en MijnSVB - inzage in persoonlijke gegevens, de zogenaamde berichtenbox, en een overzicht van lopende zaken Op dit moment kunnen ruim tien administraties worden ingezien, denk hierbij aan de Gemeentelijke Basis Administratie, het pensioenoverzicht en het kentekenregister. Daarnaast plaatsen momenteel de RDW, SVB, en UWV berichten in de berichtenbox, en bieden enkele gemeenten de mogelijkheid ‘lopende zaken’ via MijnOverheid in te zien. MijnOverheid heeft zo'n 250.000 accounts en het aantal unieke bezoeken ligt rond de 50.000 per maand. Het aantal berichten dat naar de berichtenbox wordt verstuurd ligt rond 90.000 per maand. Met de aansluiting van de Belastingdienst en uitbreiding van de het aantal berichten zal het aantal berichten naar 6 miljoen kunnen groeien eind 2013.

Dit onderzoek, met het voorliggende rapport als uitkomst, dient geplaatst te worden in de context van het WRR-rapport iOverheid en de kabinetsreactie daarop. In opdracht van het ministerie van Binnenlandse Zaken

en Koninkrijksrelaties is onderzocht of de informatiepositie van de burger versterkt kan worden door verdere uitbreiding van de inzage- en correctiemogelijkheden en andere nieuwe functionaliteiten van MijnOverheid.

1.2 Onderzoeksopdracht

Voor dit onderzoek zijn drie onderzoeksvragen meegegeven. Hieronder wordt elk van de drie onderzoeksvragen toegelicht en afgebakend.

1. Welke additionele functionaliteiten van MijnOverheid kunnen bijdragen aan het versterken van de informatiepositie van de burger? Onderzoek daarbij ten minste de volgende zes functionaliteiten:
   I. inzage in gegevens;
   II. inzage in gegevensverkeer;
   III. verzoeken om correctie;
   IV. mogelijkheid tot actief delen van gegevens
   (en hierbij de vraag of dit van een overheidsautorisatie kan worden voorzien);
   V. vermelding verwijderingtermijn;
   VI. een module met contactgegevens.

In hoofdstuk twee worden deze functionaliteiten nader beschreven. In het onderzoek is ook onderzocht of er naast de genoemde zes functionaliteiten, andere functionaliteiten zijn die de informatiepositie van de burger kunnen versterken. Naast de wenselijkheid van deze functionaliteiten (vanuit het perspectief van de burger en het versterken van zijn informatiepositie) wordt ook gekeken naar de haalbaarheid van de functionaliteiten (vanuit het perspectief van de overheidsorganisaties). Het gaat daarbij om de organisatorische, technische, juridische en financiële implicaties van de additionele functionaliteiten. De additionele functionaliteiten hebben ook consequenties voor de rol die MijnOverheid vervult. In het onderzoek is bekeken in hoeverre deze verandert.

De vraag aan Het Expertise Centrum is om onderzoek te doen en gegevens en informatie aan te dragen op basis waarvan de beleidsverantwoordelijken zelf een beleidslijn kunnen formuleren en waar ze beleidsmatige keuzes op kunnen baseren. Het rapport heeft daarom een sterk feitelijk karakter. In de hoofdstukken die het burgerperspectief, het juridisch perspectief en het informatiekundig perspectief schetsen worden sec de resultaten van de gevoerde gesprekken en uitgevoerde analyses gepresenteerd. De factsheets in hoofdstuk 6 geven inzicht hoe de verschillende perspectieven zich tot elkaar verhouden. Ook de conclusies in hoofdstuk 7 zijn feitelijk van aard en geven de bevindingen op basis van de inbreng van de respondenten weer.

2. Kunnen, en zo ja op welke wijze, overheidsorganisaties verplicht worden aan te sluiten op de functionaliteiten van MijnOverheid?

Onderzocht is of, en zo ja, op welke wijze (verschillende typen) overheidsorganisaties, verplicht kunnen worden om aan te sluiten op de functionaliteiten van MijnOverheid en wat de consequenties daarvan zijn.

3. In hoeverre kunnen de additionele functionaliteiten van MijnOverheid en verplichtstelling daarvan invulling geven aan artikel 18 van de Wet algemene bepalingen burgerservicenummer?

Artikel 18 betreft de verplichting van de minister tot “de instandhouding van een voorziening met behulp waarvan voor een ieder algemene informatie beschikbaar wordt gesteld met betrekking tot a. het gebruik van

burgerservicenummers en b. de gegevensverwerkingen van gebruikers, waarbij burgerservicenummers worden gebruikt".

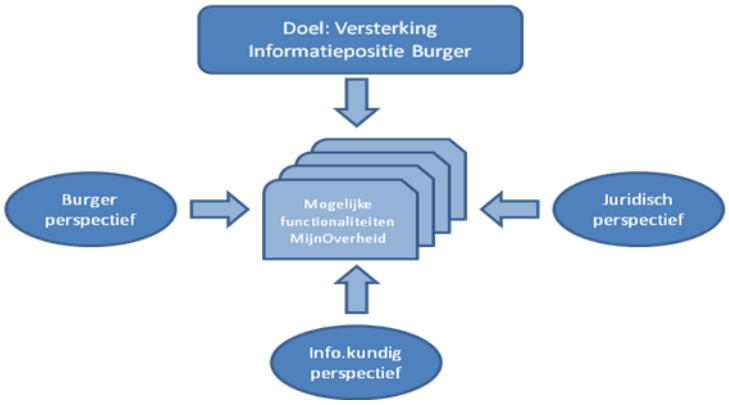
Tot slot is onderdeel van de onderzoeksopdracht dat in de beantwoording van de verschillende onderzoeksvragen zo mogelijk voorbeelden uit binnen- en buitenland meegenomen worden.

Dit onderzoek is onafhankelijk uitgevoerd door Het Expertise Centrum. Voor het faciliteren van reflectie vanuit expertise, en op de voortgang van het onderzoek, is door het ministerie van BZK een begeleidingscommissie ingesteld met experts afkomstig van relevante overheidsorganisaties.

1.3 Werkwijze en onderzoekskader

Het versterken van de informatiepositie van de burger wordt door zowel de WRR als het kabinet gezien als van strategische betekenis binnen de verdere ontwikkeling van de iOverheid. Daarbij worden bij het onderzoeken ven de mogelijke nieuwe functionaliteiten van MijnOverheid drie verschillende perspectieven onderscheiden.

- Het perspectief van de burger (wensen en verwachtingen);
- Het juridisch perspectief (rechten en principes);
- Het informatiekundig perspectief (mogelijkheden en consequenties).



Figuur 1: Onderzoeksperspectieven

Het onderzoek is langs de lijn van deze drie perspectieven opgezet:

- **Het burgerperspectief**
  Het toevoegen van functionaliteiten aan MijnOverheid is alleen zinvol wanneer de functionaliteiten daadwerkelijk de informatiepositie van de burger versterken en burgers zich herkennen in de functionaliteiten en de wijze waarop ze worden aangeboden. Dit perspectief is onderzocht in vier burgerpanels.
- **Het juridisch perspectief**
  Het uitbreiden van de functionaliteiten van MijnOverheid betreft deels het invullen van bestaande rechten, maar wellicht vereisen andere functionaliteiten ook een nieuwe juridische onderbouwing. In het onderzoek zijn de mogelijkheden en eventuele juridische barrières in kaart gebracht.
- **Het informatiekundig perspectief**

Achter een functionaliteit in MijnOverheid zit een keten van informatiestromen en processen om de functionaliteit te laten werken, die op verschillende manieren kan worden vormgegeven. Afhankelijk van de gemaakte keuzen vallen de organisatorische, financiële, technische en juridische consequenties anders uit. Hiervoor zijn (duo-)interviews met vertegenwoordigers van de betrokken organisaties op bestuurlijk en tactisch niveau gehouden. In een later stadium is nogmaals met een aantal sleutelfiguren gesproken om enkele ‘witte vlekken’ in het rapport te dichten en kritische succesfactoren voor de (implementatie van) functionaliteiten te benoemen. Ook is een quick scan uitgevoerd naar vergelijkbare sites in andere landen. Denemarken, Estland, Duitsland, Frankrijk en Slowakije zijn in deze scan meegenomen. De (e-)strategie en de websites van deze landen zijn bekeken.

Hieraan voorafgaand is een korte verkenning op het onderzoek uitgevoerd en een analysekader opgesteld. In dat verband zijn gesprekken gevoerd met de WRR, het College Bescherming Persoonsgegevens (CBP) en zijn relevante documenten bestudeerd, waaronder het WRR-rapport iOverheid, de kabinetsreactie daarop en de impactanalyse van MijnOverheid, uitgevoerd door het Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Dit rapport start met het beeld dat burgers zelf hebben van hun informatiepositie en het belang dat zij daaraan hechten. Vanuit dat perspectief wordt besproken wat de meerwaarde zou kunnen zijn van nieuwe functionaliteiten van MijnOverheid. Vervolgens komt aan de orde wat het huidige juridische kader is rond de informatiepositie van burgers (met name de Wbp) en wat de mogelijkheden en eventuele beperkingen zijn ten aanzien van de nieuwe functionaliteiten van MijnOverheid. Tenslotte bespreekt het rapport de informatiekundige consequenties van het eventueel toevoegen van de genoemde functionaliteiten aan MijnOverheid.

Daarmee biedt deze verkenning een breed overzicht en maakt de samenhang tussen de geschetste perspectieven zichtbaar. Gezien het verkennende karakter van het onderzoek en de ervaring dat, met name bij de gesprekken vanuit het informatiekundig perspectief, veel respondenten hun impliciete beelden moesten bijstellen en creatief moesten meedenken om de vragen te beantwoorden, blijft het onderzoek op sommige punten betrekkelijk globaal. Zo bleek het voor hen niet mogelijk om in deze fase reeds in detail in te gaan op de vraag wat de financiële en organisatorische consequenties zijn van de eventuele invoering van de nieuwe functionaliteiten.

1.4 Leeswijzer

Het rapport start in hoofdstuk 2 met een afbakening van de onderzoeksopdracht en een beschrijving en toelichting op de functionaliteiten die zijn onderzocht. Hoofdstuk 3, 4 en 5 bevatten vervolgens de bevindingen van het onderzoek vanuit de verschillende perspectieven. Wat zegt het burgerperspectief, het juridisch perspectief en het informatiekundig perspectief over de wenselijkheid en haalbaarheid van de verschillende functionaliteiten? In hoofdstuk 6 worden de bevindingen per functionaliteit ten opzichte van elkaar in samenvattende factsheets gepresenteerd. In hoofdstuk 7 worden de onderzoeksvragen beantwoord en staan de conclusies op hoofdlijnen.

2 Afbakening onderzoek

2.1 Inleiding

In dit hoofdstuk wordt het onderzoek nader afgebakend. Als het gaat om de informatiepositie van burgers, waar gaat het dan eigenlijk over? En, wat wordt precies bedoeld met de zes functionaliteiten?

2.2 De informatiepositie van burgers

Het onderzoek betreft de vraag hoe de informatiepositie van de burger versterkt kan worden. Vanuit het perspectief van de burger wordt onderzocht of en hoe met een bepaalde functionaliteit zijn informatiepositie wordt versterkt. Hierbij staat de relatie tussen de burger en de organisaties die wettelijke taken uitvoeren centraal: gemeenten, agentschappen, ZBO's, onderdelen van departementen, maar ook private partijen met een wettelijke taak. Iedere organisatie verzamelt gegevens om haar processen te kunnen uitvoeren, legt deze vast, voert bewerkingen uit en verstrekt gegevens aan andere organisaties.

De burger heeft met tal van uitvoeringsorganisaties te maken. Hij verstrekt soms gegevens zonder direct een dienst te krijgen: een voorbeeld is gegevensverstrekking aan een basisregistratie die de gegevens verstrekt aan andere organisaties die het gegeven in hun dienstverlening betrekken. De dienst kan gevraagd of ongevraagd zijn. De burger is actief op Internet en laat daar digitale sporen (gegevens) na. Uitvoeringsorganisaties plaatsen geen persoonsgegevens betreffende burgers op het Internet, maar maken wellicht wel gebruik van gegevens die daar te vinden zijn. De diverse informatieprocessen (verzamelen en vastleggen, verrijken, verstrekken, profileren) vinden binnen de organisaties plaats.

De organisaties voeren hun werkprocessen uit waarbij ze ICT inzetten om de informatie te gebruiken en te bewerken. De WRR noemt een aantal informatieprocessen die van belang zijn:

- **Dienstverlening**
  Het eenvoudigste geval betreft een burger die aan één organisatie een dienst vraagt, die de benodigde gegevens verstrekt, waarna de dienst geleverd wordt. De dienstverleningstransactie vindt plaats tussen de burger en één verantwoordelijke organisatie. Op basis van de gegevens die de burger zelf verstrekt en de geldende wettelijke regels neemt de organisatie een besluit dat aan de burger kenbaar wordt gemaakt. Het is (in principe) voor de burger helder wie de verantwoordelijke is, hoe het proces verloopt en welke gegevens worden gebruikt.
- **Vernetwerking**
  Steeds vaker is er niet langer sprake van een één op één relatie tussen een burger en een organisatie, waarbij een burger gegevens verstrekt in het kader van een (dienstverlenings-, opsporings- of zorg)proces. Om beleidsvraagstukken op te lossen werken uitvoeringsorganisaties samen in ketens en netwerken, wisselen zij onderling gegevens uit en gebruiken die in hun processen. De overheid heeft basisregistraties ingesteld die wettelijk verplicht gebruikt moeten worden. Om te kunnen volgen hoe een besluit van de overheid tot stand komt heeft een burger niet alleen inzicht nodig in het proces en de door hem zelf verstrekte gegevens, maar ook in de gegevensstromen tussen organisaties.

- **Profiling**
  De WRR karakteriseert de informatiesamenleving waarin de iOverheid functioneert als een omgeving waarin het verzamelen van gegevens niet zozeer het vraagstuk is (gegevens zijn er in overvloed, verzamelen gaat als het ware vanzelf), maar het omzetten van gegevens in betekenisvolle informatie en overdraagbare kennis. Daar wordt een belangrijke nieuwe ontwikkeling zichtbaar. Met behulp van ICT kunnen (zeer) omvangrijke datasets worden bewerkt met wiskundige technieken. Daarmee worden correlaties tussen data zichtbaar zonder dat deze per se op een oorzaak – gevolgrelatie duiden. Met het gebruik van (risico)profielen die op deze manier worden opgesteld kan de effectiviteit van overheidshandelen worden vergroot. De profielen voorspellen gedrag en worden door de overheid ingezet om wetsovertredingen te voorkomen in plaats van ze achteraf te vervolgen en bestraffen.

De informatiepositie van de burger wordt extra relevant op het moment dat er sprake is van onjuiste informatie over de burger in de systemen van overheidsorganisaties. Immers op dat moment worden mogelijk onjuiste of onterechte besluiten genomen, die ten nadele kunnen zijn van de burger. De WRR wijst er in haar rapport iOverheid op dat juist in die situaties het van belang is dat de informatiepositie van burgers wordt versterkt.

2.3 Accenten in het onderzoek

Vernetwerking en profiling
De bestaande praktijk in de dienstverlening heeft met name betrekking op wat de WRR vernetwerking noemt. Vernetwerking komt in de dienstverlening op grote schaal voor. Profiling wordt in de dienstverlening wel toegepast, maar nog niet of nauwelijks in de vergaande vorm die de WRR schetst. In de gevoerde gesprekken is het vrijwel uitsluitend over vernetwerking gegaan. In de algemene juridische en informatiekundige analyse is het onderwerp profiling wel meegenomen, zodat duidelijk gemaakt kan worden in hoeverre de onderzoeksuitkomsten ook toepasbaar zijn op profiling.

Zorg en controle
Hetzelfde geldt voor de domeinen waarop MijnOverheid betrekking heeft. Tot nu toe wordt MijnOverheid voornamelijk gebruikt om burgers inzage te geven in de geregistreerde gegevens bij overheidsdienstverlening, onder aansturing van de Bestuurlijke Regiegroep dienstverlening en e-overheid. De risico's voor burgers zouden echter in domeinen van zorg en controle weleens groter kunnen zijn. Wanneer er iets mis gaat bij het gebruik van controle- en opsporingsgegevens kan dat heel ernstige gevolgen voor de betreffende burger hebben. Zorggegevens hebben een intiem karakter en levensbedreigende situaties kunnen het gevolg zijn van verkeerd gebruik. Vanuit de ernst van de problematiek en het belang voor burgers verdienen het zorgdomein en het controledomein zeker zoveel aandacht als de dienstverlening. De scheiding tussen de domeinen is geen waterscheiding: controleprocessen maken onderdeel uit van veel dienstverleningsprocessen.
De gesprekken die gevoerd zijn, hebben met name plaatsgevonden met partijen die in de dienstverlening actief zijn. Aanvullend is met één partij in de zorg gesproken.

2.4 Beschrijving van de functionaliteiten

Over functionaliteiten spreken zonder het doel dat ze moeten dienen en de context waarin ze moeten functioneren steeds voor ogen te houden, leidt niet tot bruikbare resultaten. Met de begeleidingscommissie van dit onderzoek zijn daarom in een vroeg stadium de te onderzoeken functionaliteiten besproken en gedefinieerd.

Bij inzage in gegevens en gegevensstromen, correctierecht en verwijderen van gegevens maakt het beoogde detailniveau veel verschil voor de toegevoegde waarde van de functionaliteit voor burgers, maar ook voor de gevolgen die het gebruiken ervan heeft voor de uitvoeringsinstellingen. We onderscheiden drie relevante detailniveaus:

- **Een algemeen niveau**
  Dat bestaat uit een algemene beschrijving van de taken die een uitvoeringsinstelling verricht, de partijen waarmee gegevens worden uitgewisseld en categorieën van gegevens die het betreft. De website www.burgerservicenummer.nl bevindt zich op dit niveau.
- **Een "kerngegevens" niveau**
  Uitvoeringsorganisaties verzamelen op allerlei manieren gegevens, bewerken die, en interpreteren ze conform de eigen sectorwetgeving. Op basis daarvan nemen ze een besluit: deze auto staat op uw naam, u krijgt wel of niet een invalidenparkeervergunning, u hebt recht op dit bedrag aan AOW. Deze besluiten worden begrijpelijk voor de burger en zijn gebaseerd op wat wij noemen "kerngegevens". Op het kerngegevensniveau biedt een instelling inzage in deze, aan het besluit / de zaak / de transactie gerelateerde gegevens.
- **Een gedetailleerd gepersonaliseerd niveau**
  Op dit niveau worden ook de gegevens en de bewerkingen die zijn uitgevoerd om de kerngegevens te bepalen inzichtelijk gemaakt voor de burger die het betreft. Gegevensverkeer wordt per bericht gespecificeerd (datum, verzendende partij, ontvangende partij, inhoud van het bericht, doel van het bericht).

Omdat het onderscheid in detailniveau een heel cruciaal element in de uitkomsten van het onderzoek blijkt te zijn, verduidelijken we dit met een voorbeeld. Gemeenten verlenen parkeervergunningen aan invaliden. Het besluit is: u krijgt (en vervolgens u hebt) wel of geen parkeervergunning. De kerngegevens betreffen zaken als: u bent inwoner van deze gemeente, u bent eigenaar van een auto, u bent gehandicapt, de parkeerplaats is wel/niet in te passen in het ruimtelijk beleid. Kerngegevens zijn de uitkomst van de bewerkingen die zijn uitgevoerd om het verzoek te behandelen. De GBA en de Kentekenregistratie zijn geraadpleegd, de burger heeft op een manier die aan de gestelde eisen voldoet aangetoond dat hij gehandicapt is, de betreffende gemeentelijke dienst heeft een onderzoek naar ruimtelijke inpasbaarheid uitgevoerd. Op gedetailleerd niveau wordt in het verloop van de bewerkingen (in principe volledig) inzage gegeven.

2.4.1 Inzage in gegevens

Uitvoeringsorganisaties leggen bij het uitvoeren van hun processen gegevens over burgers vast. Burgers hebben op grond van de Wet bescherming persoonsgegevens (Wbp) het recht op inzage in deze gegevens. Ze kunnen dat recht uitoefenen bij alle uitvoeringsorganisaties door de organisatie te benaderen en inzage te vragen. Het bestaande MijnOverheid heeft als belangrijke doelstelling inzage voor burgers sterk te vereenvoudigen. Een aantal overheidsorganisaties biedt al inzage via MijnOverheid. De kabinetsreactie op het WRR-rapport stelt dat door elektronisch inzichtelijk te maken welke gegevens overheidsorganisaties van burgers gebruiken, deze burger in staat wordt gesteld daar toezicht op te houden en zelf regie te voeren. Inzage zou ook moeten gelden voor dossiers waarin gegevens van meerdere instellingen worden samengebracht, inclusief de herkomst van de gegevens en gegevens die gebruikt zijn voor pro-actief handelen.

2.4.2 Inzage in gegevensverkeer

Uitvoeringsinstellingen delen gegevens met elkaar, zo ontstaan de informatiestromen die de WRR zo typerend acht voor de iOverheid. Uitwisselingen vinden plaats:

- Vanuit een basisregistratie naar uitvoeringsinstellingen en andere (basis)registraties;
- Door uitvoeringsinstellingen die gegevens bij hun collega's opvragen;
- Binnen ketens waarin uitvoeringsinstellingen samenwerken, vaak worden daarbij dossiers of portalen gebruikt.

2.4.3 Verzoeken om correctie

In de kabinetsreactie staat dat verkend zal worden of, náást de mogelijkheid tot het indienen van correctieverzoeken direct bij de gegevenshouder, een uitbreiding van MijnOverheid met een correctievoorziening wenselijk, mogelijk en haalbaar is (Kabinetsreactie, 2012: 12). Verondersteld wordt dat inzage in gegevens en het gegevensverkeer een burger duidelijk maakt hoe een gegeven door de keten gaat, waar een fout gemaakt wordt en hoe die doorwerkt bij andere organisaties in de keten. Met een gemeenschappelijke correctiefaciliteit kan de burger bij alle partijen tegelijk een verzoek indienen om de fout en de gevolgen daarvan recht te zetten.

2.4.4 Vermelden van verwijderingstermijn

Voor allerlei gegevens bestaan bewaar- en verwijderingstermijnen, maar deze worden niet altijd nageleefd. De functionaliteit houdt in dat, bij gegevens waarvoor een bewaartermijn geldt en die via MijnOverheid inzichtelijk gemaakt worden, tevens vermeld wordt wanneer het gegeven moeten worden gewist. De achtergrond van deze functionaliteit is dat gegevens 'doorgeleverd' worden aan derde overheidspartijen. Het kan bijvoorbeeld voorkomen dat in de zorg iemands psychiatrisch verleden al uit het dossier gewist is, maar in de dossiers / datasets van andere partijen nog bestaat.

2.4.5 Een module met contactgegevens

Niet genoemd in de kabinetsreactie, maar wel onderdeel van het onderzoek is het verkennen van de mogelijkheid om in MijnOverheid een module met contactgegevens op te nemen. Het betreft bankrekeningnummer, email, mobiele telefoon en tijdelijk correspondentieadres. Deze module kan op twee manieren ingevuld worden:

- Vanuit het belang van de overheid die op deze wijze processen kan vereenvoudigen en efficiënter en effectiever kan werken.
- Vanuit het belang van de burger die zelf de contactgegevens beheert en regisseert die hij gebruikt in het digitaal verkeer met de overheid.

2.4.6 Actief delen van gegevens

Dit betreft de mogelijkheid om eigen gegevens op eigen verzoek actief te delen met derde partijen. De kabinetsreactie geeft als voorbeeld dat nu al op papier een uittreksel uit de GBA of een inkomensverklaring van de Belastingdienst moet worden verstrekt. Het voorstel wordt ingrijpender wanneer de burger bepaalt aan

welke private partijen zij zelf de gegevens uit MijnOverheid verstrekt. Beide varianten zijn in de verkenning meegenomen.

3 Bevindingen burgerperspectief

3.1 Inleiding

In dit hoofdstuk staan de bevindingen van het burgerperspectief: de resultaten van de kwalitatieve burgerpanels. In paragraaf 3.2 wordt de opzet van de burgerpanels beschreven. Gelijk aan deze opzet worden in paragraaf 3.3. de algemene bevindingen over het versterken van de informatiepositie van de burger en MijnOverheid beschreven en in paragraaf 3.4. de bevindingen per functionaliteit. In paragraaf 3.5 worden de consequenties beschreven voor het beantwoorden van de onderzoeksvragen vanuit het burgerperspectief.

Het is van belang op te merken dat het in dit hoofdstuk gaat om de meningen en wensen van burgers in reactie op de vraag hoe zij aankijken tegen hun informatiepositie. Daarbij is met name ingegaan op de vraag wat het toevoegen van de nieuwe functionaliteiten aan MijnOverheid zou betekenen voor hun informatiepositie. Daarmee zijn de bevindingen in dit hoofdstuk nog niet geconfronteerd, c.q. afgewogen, ten opzichte van de mogelijkheden en eventuele beperkingen die voortkomen uit het juridische en informatiekundige perspectief. Dat betekent dit dat enkele van de onderstaande weergegeven citaten van panelleden niet noodzakelijk overeenkomen met de technische mogelijkheden of juridische werkelijkheden.

De burgerpanels zijn een kwalitatief onderzoeksinstrument waarmee gedetailleerd inzicht wordt verkregen in ervaringen en wensen van de aanwezige burgers. Het betreft hier geen kwantitatieve studie die representatief aangeeft wat de ‘algemene ervaringen en wensen’ van de Nederlandse bevolking zijn.

3.2 Opzet burgerpanels

Voor het burgerperspectief zijn vier kwalitatieve burgerpanels georganiseerd. Deze panels zijn ingedeeld naar drie leeftijdscategorieën: 18 – 35 jaar, 35 – 60 jaar en 60 jaar en ouder, en een groep zzp’ers. Via het respondentenbestand van PanelClix zijn panelleden uit verschillende leeftijdscategorieën geworven. Middels een korte vragenlijst konden respondenten aangegeven of zij mee wilden doen aan het panel of niet. In de vragenlijst is ook de vraag gesteld of zij bekend zijn met MijnOverheid en zo ja, hoe vaak ze gebruikmaken van de site. Hiernaast is een burgerpanel voor zzp’ers georganiseerd. Voor deze panels zijn eenmanszaken uitgenodigd, de zogenoemde burgers ‘plus’, die vanuit hun eigen persoon ook zakelijk contact hebben met de overheid. Dit is met medewerking van de Vereniging Amersfoort Zelfstandigen gedaan. Voorafgaand aan deze vier panels is een testpanel met medewerkers van Het Expertise Centrum gehouden. Ook dit testpanel is in de analyse meegenomen. Over het algemeen waren er weinig tot geen verschillen tussen de doelgroepen. Waar dat wel zo was, wordt dit aangegeven. Aan de panels hebben in totaal zo’n 35 mensen deelgenomen. Dit relatief beperkte aantal respondenten heeft vanzelfsprekend consequenties voor de generaliseerbaarheid van de uitkomsten. Bij het verbinden van conclusies aan de resultaten dient hier rekening mee te worden gehouden.

In de panels is als eerste stilgestaan bij het beeld en de ervaringen van respondenten met het gebruik van informatie door de overheid. Dit leverde over het algemeen veel concrete ervaringen op, soms negatief, soms positief. Op die manier zaten de panelleden in de ‘juiste modus’ om MijnOverheid en de extra functionaliteiten te bekijken. Wat verwachten de panelleden van de site en hoe zou het hun moeten helpen?

De extra functionaliteiten zijn aan de hand van nagebootste screenshots besproken. Aan het eind van elke bespreking is de balans opgemaakt en is de deelnemers gevraagd op een post-it te schrijven of en waarom ze (n)iets aan de functionaliteit hebben.

3.3 Algemene bevindingen

3.3.1 Het versterken van de informatiepositie

Willen weten wat de overheid weet
De panelleden weten precies waar het over gaat als het om hun informatiepositie gaat. Over het algemeen vinden zij dat de overheid veel over hen weet, maar dat zij niet weten wat de overheid allemaal over hen weet en wat er met die informatie gebeurt. Zij zouden meer controle willen hebben over iets dat van henzelf is.

> *"Ik weet niet wat de overheid allemaal van mij registreert en wat ze daar mee doen. Dit mag wel wat transparanter. Ik hoef dit niet tot in de details te weten, maar wel op hoofdlijnen. Welke overheidsdiensten communiceren op welk niveau met elkaar?"*

> *"Waar gebruiken ze de informatie precies voor? Dat is mij niet altijd even duidelijk. Ik weet ook niet of de gegevens allemaal correct zijn. Als de mogelijkheid er is, dan zou ik het wel controleren."*

> *"Ze mogen alles weten, maar ik wil wel weten wat ze weten en wat ze aan elkaar koppelen."*

Privacy en grenzen aan het verzamelen van informatie
De panelleden leggen in dit verband ook snel de relatie met privacy. Eén van de panelleden definieert privacy als volgt:

> *"Dat je het gevoel hebt dat je aan het stuur zit. Dat je zelf kiest welke gegevens wel en niet gedeeld worden."*

In dit verband vinden de panelleden ook dat er een grens zit op datgene wat de overheid over hen mag verzamelen en koppelen:

> *"Ik wil wel wat meer weten over bestandskoppelingen, bijvoorbeeld met de Belastingdienst, de zorgverzekering en de RDW. Dat zijn griezelige combinaties, er komen veel extra gegevens vrij. Ik heb het gevoel dat je een stukje macht kwijtraakt. Mijn grootste nachtmerrie is dat je ineens als crimineel gezien wordt, omdat er iemand is met vrijwel dezelfde naam. Dan kom je een hoop ellende tegen."*

> *"Als ze je internet en telefoonverkeer gaan vastleggen, dan bevinden ze zich op een hellend vlak. Ik weet dat ze wellicht mijn hele hebben en houden boven water kunnen halen. Als dat functioneel is om hun service te optimaliseren, dan vind ik dat prima. Maar als ze meerdere dingen aan elkaar gaan knopen, dwarsverbanden leggen en daar conclusies aan verbinden [profiling, red.] dan is het de vraag of dat wenselijk is."*

Omgekeerde bewijslast en actief wijzen op rechten

Verder ervaren sommige panelleden dat de overheid vooral haar eigen administraties vertrouwt en niet naar de burger luistert. De bewijslast ligt al snel bij de burger en niet bij de overheid. Dit voelt als onmacht.

> *"Als een instantie een foutje maakt, luisteren ze niet naar mij maar naar die instantie. Je moet alles bewijzen."*

> *"Het is eindeloos gedoe. Je moet aan heel veel verplichtingen voldoen. De overheid is niet goed in het organiseren van dataverkeer. Je weet niet precies wat er gebeurt."*

De panelleden weten verder niet altijd op welke voorzieningen (bijvoorbeeld zorgtoeslag) men juridisch gezien recht heeft. Volgens een aantal panelleden zou het fijn zijn als de overheid duidelijk en actief communiceert waar burgers recht op hebben.

Redenen waarom de panelleden inzage willen
De panelleden willen dus graag weten welke informatie en gegevens de overheid allemaal van hen heeft. Hier noemen zij verschillende redenen voor. Ten eerste wordt op die manier volgens hen de transparantie en het vertrouwen van de overheid versterkt en ten tweede kunnen zij de overheid controleren op juistheid.

Het belang van een accountmanager
Het controleren van gegevens op juistheid geldt in het bijzonder voor mensen van wie gegevens bij de overheid niet kloppen. Verschillende panelleden hebben dergelijke ervaringen met de overheid. Enkele voorbeelden staan hieronder in de kaders beschreven.

Een tijdje geleden overkwam het Tom dat zijn BSN niet meer klopte. Hij bestond niet meer. Tom ging met zijn probleem naar de gemeente, maar die stuurde hem door naar de IND. Voor Tom voelde het alsof hij uit het buitenland kwam. Na een tijdje kwam Tom gelukkig weer terug in het systeem.

Miranda huurt een appartement in een pand met vier appartementen. Op de een of andere manier wordt zij als hoofdbewoner gezien. Er blijkt maar één adres in de registratie te staan, terwijl het er vier moeten zijn. Door deze verkeerde registratie wordt Miranda voor de gemeentelijke en waterschapsbelastingen aangeslagen voor alle vier de appartementen in plaats van alleen voor haar appartement. Ook ontvangt zij de huurtoeslag van haar medebewoners en moet zij die vervolgens onder hen verdelen. Ze heeft al meerdere keren met de gemeente contact gezocht, maar het is tot nu toe niet gelukt om het aan te passen.

Puck verhuisde onlangs. Er werden verkeerde gegevens door de woningbouw doorgestuurd naar de Belastingdienst. Dat resulteerde erin dat haar zorg- en huurtoeslag werd stopgezet. Meerdere keren belde ze de Belastingdienst. Elke keer kreeg ze het antwoord 'Ja, maar de computer zegt…' of 'De computer heeft dat gedaan'. Soms vindt Puck het fijn dat gegevens worden doorgestuurd, maar als het fout gaat is het moeilijk te herstellen.

Deze groep geeft aan dat MijnOverheid als zodanig hun probleem niet kan oplossen. Het geeft hen wel extra inzicht of bewijsmateriaal (bijvoorbeeld over hoe ze geregistreerd staan en welke informatie over hen wordt uitgewisseld) en wellicht een mogelijkheid tot het doen van een correctieverzoek, maar daarmee is hun probleem niet opgelost. Daarvoor is meer en met name persoonlijk contact nodig. De panelleden vinden het wenselijk als er een accountmanager zou zijn die voor hen uitzoekt wat de oorzaak is en het probleem

(eventueel tussen organisaties) oplost, zodat zij niet van het kastje naar de muur gestuurd worden. Ze refereren daarbij aan bestaande mogelijkheden en ervaringen die ze daarbij hebben.

> *"Als er toen (ik als zelfstandige werkte, red.) problemen (bij de Belastingdienst, red.) waren ging ik er gewoon naartoe. Anders werkt het niet zo goed. Bellen werkt niet om problemen op te lossen."*

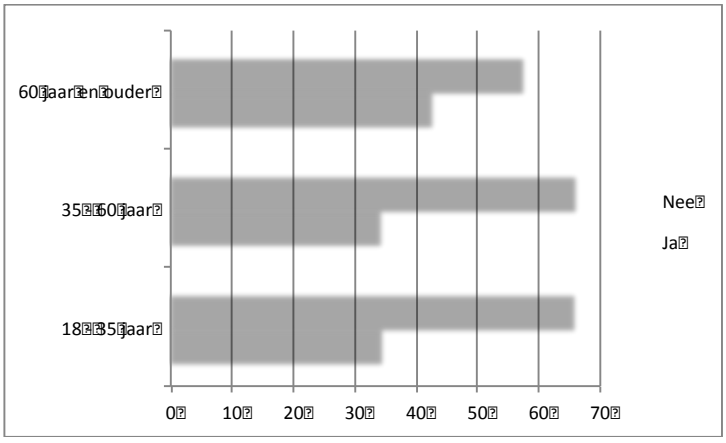
De groep eenmanszaken had beduidend minder probleemsituaties met de overheid. Als ondernemer hebben zij gemiddeld meer contact met de overheid dan als privépersoon. Dat contact is dan met name met de Belastingdienst in verband met de loonaangifte. Dat contact verloopt niet altijd even prettig. De eenmanszaken hekelen de anonieme callcenters en vinden het vreemd dat de Belastingdienst niet bereikbaar is via de e-mail. Ook zij willen bij voorkeur een accountmanager die hun geschiedenis kent en weet wat er speelt, net zoals de huisarts weet wat je medische achtergrond is:

> *"Ik wil graag een lokaal winkeltje van de overheid, met mensen die je echt kunnen helpen."*

Een tussenconclusie is dat MijnOverheid fysiek en persoonlijk contact niet kan vervangen.

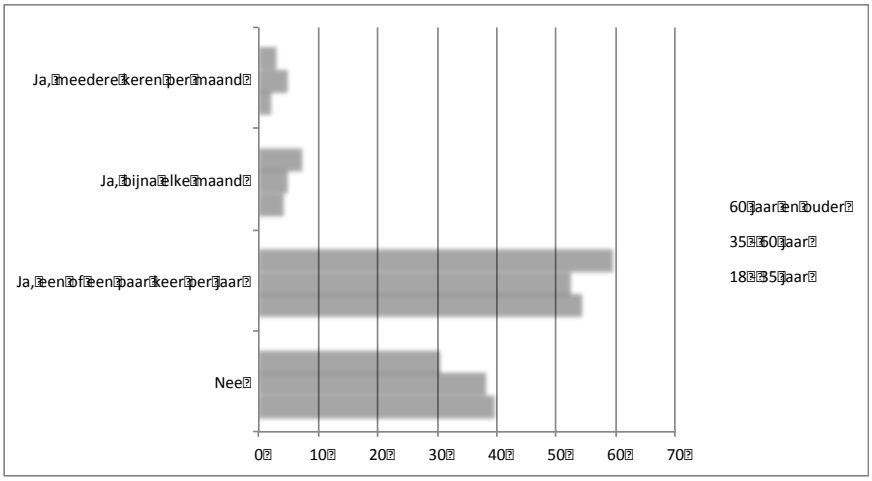
3.3.2 Bekendheid met en gebruik van MijnOverheid

In totaal hebben 425 mensen een korte vragenlijst ingevuld om aan te geven of ze wel of niet mee willen doen aan het burgerpanel. Ongeacht hun deelname heeft iedereen de vraag beantwoord of ze bekend zijn met MijnOverheid en zo ja, hoe vaak ze gebruik maken van de site. Dit geldt voor 140 mensen in de doelgroep 18-35 jaar, 123 mensen in de doelgroep 35 – 60 jaar en 162 mensen in de doelgroep 60 jaar en ouder. Het merendeel van de respondenten is niet bekend met de site, zo'n 35 tot 40 procent wel, zoals onderstaande grafiek laat zien.



Figuur 1: bekendheid met de site MijnOverheid

Vervolgens blijkt dat het merendeel van degenen die de site kennen niet tot nauwelijks gebruik maakt van de site. De onderstaande grafiek met bijbehorende vraagstelling "Maakt u weleens gebruik van MijnOverheid?" laat dit zien. Ruim de helft van de respondenten, ongeacht leeftijdscategorie, maakt één of enkele keren per jaar gebruik van de site.



Figuur 2: gebruik van de site MijnOverheid

3.3.3 Verwachtingen van MijnOverheid

In de burgerpanels is als eerste aan de panelleden die de site niet kennen, het merendeel, gevraagd wat zij van de site verwachten. Wat zou de site volgens hen moeten bieden? De antwoorden op deze vraag kunnen opgedeeld worden in een informatieve functie, een inzagefunctie en een regelfunctie.

MijnOverheid als informatiekanaal
Een aantal panelleden zou het fijn vinden als de site een slimme persoonlijke zoekmachine bevat. Daar kan hij/zij terugvinden welke regels en rechten hij allemaal heeft en kan hij/zij specifieke vragen stellen en antwoorden terugvinden. Een aantal wil ook hun 'probleem' of vraag via de site kunnen aankaarten, waarna zij via persoonlijk contact verder geholpen worden. Ook zou een aantal panelleden zich via de site willen abonneren op een nieuwsbrief om bijvoorbeeld geïnformeerd te worden over wat er in hun wijk gebeurt. Voor degenen die deze verwachting bij de site hadden, was het – na uitleg – echter heel logisch dat deze informatie op www.overheid.nl te vinden is en dat MijnOverheid *alleen o*ver persoonlijke gegevens en contact gaat.

MijnOverheid als mogelijkheid om je gegevens in te zien
De meeste panelleden verwachten op de site hun 'eigen dingen' terug te vinden, bijvoorbeeld met welke organisaties ze contact hebben en welke gegevens zij van hen hebben:

> *"Als ik via DigiD MijnOverheid binnen kom, dan wil ik alles kunnen zien. Alle gegevens tussen mij en de overheid zitten daar in, zodat je gewoon even kan kijken wat er staat. En dat je je bankrekeningnummer kan invullen of je brief kan checken. Als ik MijnOverheid hoor, dan denk ik aan mijn persoonlijke pagina met mijn gegevens en mijn dingen met de overheid."*

MijnOverheid als manier om dingen te regelen
Alleen inzage in gegevens is voor de panelleden niet voldoende. Zij willen hier ook iets mee kunnen doen. Zij willen de gegevens beheren. Bijvoorbeeld door toestemming te geven over welke gegevens je wilt delen of

wijzigen en een verhuizing of een nieuwe baan door te geven. Op die manier hebben ze de regie over hun eigen gegevens. MijnOverheid krijgt dan vooral meerwaarde als het interactief is en je transacties kunt doen, aldus de panelleden.

Degenen die de site kennen, zien de site als een startpunt van waar je overal naartoe kunt. Een aantal ziet de site ook als een archief en zouden het fijn vinden als zij alles niet meer zelf jarenlang in ordnermappen hoeven te bewaren. Ook wordt er aangegeven dat zij via de site verzoeken om gegevens te corrigeren willen kunnen indienen.

Eén overheid, één site
Idealiter zien de meeste panelleden het liefst één overheid en één site. Dat zou MijnOverheid dan zijn.

> *"Alle diensten direct beschikbaar. Niet steeds verschillende sites voor verschillende organisatie. Stel dat je verhuist, dan wijzigt het allemaal in één keer. Als je met zo'n site komt, regel het dan meteen goed. Het zou fijn zijn als deze site alle andere sites vervangt: verzekering, Belastingdienst, DUO, gemeente, etc. Shoppen bij de overheid."*

Naast MijnOverheid hebben diverse overheidsorganisaties ook een zogenaamd MijnDomein. Bijvoorbeeld mijn.svb.nl. In de panels is ook gesproken over de relatie tussen MijnOverheid en de MijnDomeinen van de verschillende organisaties. De panelleden ondersteunen zowel de 'dikke' – MijnOverheid als het unieke loket - als de 'dunne' variant – MijnOverheid functioneert naast de MijnDomeinen - van MijnOverheid, zolang de informatie op beide sites maar beschikbaar is.

> *Persoon x: "Ik heb van de gemeente zelf wel eens een dergelijke pagina geopend. Eigenlijk zou MijnOverheid dan handiger zijn. Anders moet je alsnog naar alle verschillende websites." Persoon y: "Maar als ik een rijbewijs heb, ga ik toch eerst naar de gemeentewebsite toe. Dat is logischer." Persoon z: "Als je het weet, dat er één site is, dan is dat handiger. Twee plekken, MijnOverheid en eigen organisatie, is ook prima."*

MijnOverheid als toegangskanaal voor eenmanszaken
Een specifieke noot ten aanzien van de 'ondernemende burgers' (de eenmanszaken) is dat, hoewel zij wel onderscheid maken in hun privézaken en onderneming, bijvoorbeeld wat betreft bankrekeningnummer - MijnOverheid ook voor hen een logische ingang is. Zodra ze doorgroeien dan is niet de persoon, maar de onderneming relevant en zouden zij op een andere site informatie en gegevens willen zien.

> *"Als eenmanszaak breng je jezelf in. Als je een BV hebt, dan is het niet meer van jou alleen, maar dan wordt het ook de MijnOverheden van de werknemers. Dan kan je het niet meer aan jou persoonlijk koppelen."*

3.3.4 Eerste ervaringen met MijnOverheid

DigiD
Tijdens de burgerpanels is met DigiD ingelogd op de site en wordt de site bekeken. Vanuit de panels komen direct reacties op het gebruik van DigiD. De meeste panelleden hebben een DigiD, maar vaak worden inlognaam en wachtwoord vergeten of gaat er iets mis.

Verder wordt door sommigen aangegeven dat het vertrouwensniveau van DigiD dat nu voor MijnOverheid gebruikt wordt niet als voldoende veilig wordt ervaren. Als DigiD gebruikt wordt voor MijnOverheid dan moet het volgens de panelleden wel echt veilig zijn.

> *"Als het (MijnOverheid, red.) een centrale site moet worden dan zou er veel meer aan de beveiliging gedaan moet worden. DigiD alleen is niet voldoende."*

Verder willen de panelleden niet telkens opnieuw inloggen als zij naar een andere overheidssite worden doorverwezen. Dit zou in hun ogen automatisch moeten gebeuren.

> *"Ik kreeg een heel overzicht van waaruit je weer verder kan. Maar dan weet ik niet of ik dan nog een keer met DigiD moet inloggen. Als dat zo is, dan voelt het als het water naar de zee dragen."*

Aangenaam verrast

Wat vinden de panelleden vervolgens van de site? De meeste mensen zijn aangenaam verrast door de site. Er staat al meer informatie op dan dat ze dachten. De meesten geven ook aan dat ze de site na afloop van de bijeenkomst thuis willen gaan bekijken. Een aantal personen heeft ook nog bericht dit daadwerkelijk gedaan te hebben.

> *"Ik vind het prachtig. Het is handig als je je gegevens terug kan zien. Zelf aanzetten, uitzetten, zelf regelen."*

> *"Dit had ik niet verwacht. Dat dit er allemaal instaat. Ik ervaar het als positief."*

Weinig persoonlijk

Een algemene reactie die hierna volgt, is dat de site te algemeen en te weinig persoonlijk is. Zo staan er gemeenten op (de Middelsee Gemeenten, red.) waar ze niks mee te maken hebben. Het onpersoonlijke karakter geldt met name ook voor de pagina met persoonlijke gegevens. De meeste panelleden willen alleen de informatie die op hen van toepassing is zien en niet informatie van organisaties waarbij zij niet bekend zijn. Op die manier wordt het ook een stuk overzichtelijker en hoef je minder vaak door te klikken.

> *"Er staan zaken op die niet van toepassing voor mij zijn. Het is te algemeen. Het is lastig dat je zaken ziet waar jij niet mee te maken hebt. Het zou prettig zijn als je de site naar je wens kan inrichten."*

Een enkeling geeft aan dit uitgebreide overzicht juist wel fijn te vinden. Op die manier kan er ook gekeken worden of het klopt dat er bijvoorbeeld geen gegevens staan bij het kadaster als iemand geen huis heeft of, zoals een deelnemer aan het zzp-panel het zei, wordt hij eraan herinnerd dat hij wat aan zijn pensioen moet doen.

Tweerichtingsverkeer

Hoewel de panelleden in eerste instantie positief zijn over de site en de hoeveelheid gegevens die beschikbaar is, verwachten en wensen zij dat zij hier ook iets mee kunnen doen. Zoals gezegd zit de meerwaarde pas echt in de site als er ook via de site gecommuniceerd kan worden en dingen geregeld kunnen worden. De berichtenbox zou tweerichtingsverkeer moeten ondersteunen en ook zouden bijvoorbeeld verhuizingen moeten kunnen worden doorgegeven of gegevens gewijzigd kunnen worden. Dit geldt in het bijzonder voor de groep eenmanszaken die bijvoorbeeld graag via de site een nieuw KvK- nummer willen aanvragen.

Site wekt andere verwachtingen
Hiernaast roept de site direct een andersoortige reactie op. Kan iedereen mijn gegevens inzien? De denkfout wordt regelmatig gemaakt dat wanneer je je eigen gegevens in overzicht via één website gepresenteerd krijgt, dat andere overheidsorganisaties dit ook kunnen zien. Randvoorwaarden voor de site zijn dus dat alleen 'jij' je gegevens kan inzien en dat de veiligheid gegarandeerd is. Hiernaast is onduidelijk welke organisaties allemaal onder de overheid vallen. Valt de gemeente er ook onder? Het zou handig zijn als dit wordt aangegeven.

> *"Welke organisaties vallen er onder 'de overheid'. Het zou handig zijn als vaak gebruikte instanties er allemaal in staan."*

3.4 Bevindingen per functionaliteit

3.4.1 Inzage in gegevens

De panelleden willen allemaal inzage in hun gegevens. Zij willen alles weten wat de overheid over hen weet. Dat betekent ook financiële gegevens van de Belastingdienst (die nu nog niet op de site staan), justitiële gegevens en zorggegevens. Wat betreft zorggegevens gaat het om de ziektekostenverzekering, huisartsgegevens en Wmo-gegevens zoals het PGB dat door het CAK wordt bijgehouden.

> *"Er moet een overzicht zijn van wat er van je wordt verzameld. Financiën, criminaliteitsgegevens, zorggegevens, waar je verblijft."*

Niet iedereen is overigens van mening dat opsporingsgegevens inzichtelijk moeten worden gemaakt. Volgens deze panelleden mag de overheid deze informatie voor zichzelf houden en daar vertrouwen ze de overheid volledig in.

Aangegeven wordt dat men inzage in gegevens hoofdzakelijk gebruikt om gegevens te controleren, in te zien wat de overheid over hem/haar weet, en te beoordelen of dit juist is. Een andere motivatie om inzage in gegevens te hebben is dat het een geheugensteun, een naslagplek of archief is, vergelijkbaar met een fysiek dossier thuis. De vraag die hierna gesteld wordt, is of de gegevens naar een harde lokale schijf kunnen worden gekopieerd. Een aantal panelleden wil graag dat de inzage in gegevens zo wordt gepresenteerd dat het als bewijsmateriaal kan worden gebruikt. Dit speelt met name voor personen die (gegevens)problemen hebben met de overheid.

In de panels is de deelnemers een aantal varianten van gegevensinzage gepresenteerd. Het voorbeeld van geclusterde informatie heeft de grootste voorkeur. Dit geldt voor alle doelgroepen. Het oogt overzichtelijk en gebruikersvriendelijk. Dit komt omdat de clustering, denk hierbij aan de clustering, geld, auto, belasting, verzekering etc. aansluit bij de belevingswereld van de burger. Anderen geven de voorkeur aan een overzichtslijst waarin de informatie onder elkaar wordt gepresenteerd. Dit maakt het volgens de panelleden makkelijk om de overheid te controleren en is makkelijker voor naslag. De panelleden vinden het prettig te weten wie wat van hun weet. Op die manier weten ze bij wie ze moeten zijn als ze wat willen of moeten wijzigen.

De panelleden ervaren het in de huidige manier van presenteren als gebruikersonvriendelijk dat er regelmatig opnieuw moet worden ingelogd als je bij een andere registratie je gegevens wilt inzien. Overigens zou, volgens een aantal panelleden, het mooiste natuurlijk zijn als je zelf je instellingen en 'design' kunt bepalen. Je kunt dan je eigen site inrichten.

3.4.2 Inzage in gegevensverkeer

Het overgrote gedeelte van de panelleden wil inzage in gegevensstromen. De panelleden met een leeftijd boven de 35 jaar willen dit allemaal. Bij de panelleden onder de 35 jaar en de eenmanszaken waren minder respondenten die dit wilden, met name omdat zij inzage in gegevensstromen alleen nuttig vinden als ze problemen hebben met de overheid en omdat ze vraagtekens hebben bij de behapbaarheid en begrijpbaarheid van deze informatie (overload). Deze doelgroep heeft ook minder vaak contact (en eventueel problemen) met de overheid, wat een mogelijke verklaring kan zijn.

De panelleden die inzage in gegevensstromen willen, geven nadrukkelijk aan dat zij toestemming willen geven over wie welke informatie van hen mag gebruiken en uitwisselen. Toestemming verlenen geeft hen een gevoel van controle. Dit gaat eigenlijk nog aan inzage in gegevensstromen vooraf. Sommigen vinden dat het koppelen van bestanden nu al buiten hen om gebeurt. Zij worden hier niet in gekend, terwijl ze dat wel zouden willen. Anderen geven daarentegen weer aan dat het soms wel handig is al dingen gewoon gekoppeld worden. Dat bespaart hen ook het aanleveren van bekende informatie. Ook heeft het verlenen van toestemming volgens enkelen een praktisch bezwaar, namelijk dat je voor veel kleine zaken toestemming moet geven.

> *"Ik vind het ook best handig, koppelen om tot slimmere informatie te komen. Als we het niet goed vinden, moeten we er ook een stop op kunnen zetten. Dan kan bijvoorbeeld via een website."*

> *"Ik zit er niet op te wachten mijn gegevens dubbel in te vullen. Als ik wat moet aanvullen is het prima."*

Er zijn verschillende redenen waarom respondenten inzage in gegevensstromen willen, grotendeels te vergelijken met de motieven waarom zij inzage in gegevens willen hebben. Namelijk: om te controleren, als archief en als bewijsmateriaal.

> *"Openheid en inzicht in gegevensstromen heeft voor mij niet echt een functie, maar het draagt wel bij aan het gevoel van wisselwerking en aan vertrouwen dat de overheid niks te verbergen heeft."*

> *"Je hebt bewijs van wat er gezegd is. Zeker als het fout gaat, is het nuttig. Je hebt een sterkere positie als er iets mis gaat."*

Ook wordt genoemd dat het wellicht een middel is om de kwaliteit van de overheid te verbeteren. Als de gegevensstromen op detailniveau worden gepresenteerd, legt dit een vergrootglas op de overheid. Het overheidshandelen wordt transparanter en de panelleden verwachten dat de kwaliteit mede hierdoor omhoog zou kunnen gaan.

Wederom is de panelleden een aantal varianten van inzage in gegevensstromen voorgelegd.De panelleden spreken de voorkeur uit voor een overzicht op organisatieniveau waarbij je kunt doorklikken naar de informatie. De variant wordt vergeleken met een logboek, waarbij als duidelijke voorwaarde wordt gesteld dat de informatie behapbaar en begrijpelijk is. Zo geven een aantal respondenten aan dat zij alleen de officiële

communicatie tussen overheidsorganisaties willen inzien en niet diepgaande loggingsgegevens, omdat dit niet meer behapbaar is.

De panelleden geven aan dat ze de informatie niet regelmatig zullen gebruiken. Als zij geen problemen hebben, zullen zij de informatiestromen zelden inzien. Bij problemen is dit meer relevant en is er behoefte aan detailniveau. Een enkeling gaf ook de suggestie om een bericht in je berichtenbox te plaatsen op het moment dat er informatie tussen organisaties is uitgewisseld.

> *"Het gaat voor mij pas tellen als het belangrijk is en het dicht bij me komt. Ik wil pas tot dat niveau inzoomen als dat nodig is. Een routebeschrijving wijst mij van a naar b, maar ik ga pas inzoomen op b als ik dicht in de buurt ben."*

3.4.3 Verzoeken om correctie

Een aantal panelleden heeft weleens ervaren dat gegevens verkeerd geregistreerd stonden of staan. Zij gaven aan dat het soms zeer lastig is om dit te corrigeren. In één geval is het ook na 40 jaar niet gelukt om de juiste voorletters in de administratie van een overheidsorganisatie te krijgen. Blijkbaar zit hier een ander vraagstuk achter. Of, zoals twee respondenten treffend meldden:

> *"Helaas is het in de praktijk vaak moeilijk je recht te krijgen, dus in de praktijk heb je weinig aan het correctierecht."*

Bijna alle panelleden, op een enkeling na, geven aan dat MijnOverheid de mogelijkheid zou moeten bieden om een correctieverzoek in te dienen. Daarbij wil men bij voorkeur aangeven bij welke organisatie dit wel en niet wordt gecorrigeerd. Zij willen hier zelf toestemming voor geven en controle over hebben. Zij willen de correctie ook graag geheel online afhandelen en alle bijbehorende officiële documentatie kunnen uploaden. Verder ontvangen zij graag een bevestiging van de ontvangst van het verzoek tot correctie en de afhandeling hiervan. Dit zou goed via de berichtenbox van MijnOverheid kunnen verlopen.

De panelleden geven aan dat ze niet zelf de gegevens online kunnen en willen corrigeren. Dit zou misbruik met zich mee kunnen brengen. Er is begrip voor de noodzaak van bewijsvoering, al is de doorlooptijd soms wat lang.

> *"Er zit een grens aan wat wij moeten veranderen. Je kunt natuurlijk niet zelf iets een ander adres geven, maar als je een gesplitst pand hebt en die staat niet in de administratie, dan moet je dat wel kunnen aangeven."*

3.4.4 Vermelden verwijderingstermijn

Het merendeel van de panelleden wil weten wat de (wettelijke) bewaartermijn is van de gegevens is die over hen zijn opgeslagen. De logische redenering daarachter is dat 'als je inzage in gegevens hebt, je ook inzage wilt hebben in de (wettelijke) bewaartermijn'. Het vermelden van de bewaar- of verwijderingstermijn zou logischerwijs als een 'extra kolom' bij inzage in gegevens toegevoegd kunnen worden:

“Ik vind het belangrijk. Niet dat ik er maandelijks naar zou kijken, maar ik wil wel de mogelijkheid hebben om het te bekijken.”

“Hoort dit niet gewoon bij inzage? Zeker als het wettelijk is vastgesteld.”

“Kan dit niet in een kolom achter de gegevens weergegeven worden?”

Een andere, diepere, motivatie is dat het vermelden van de verwijderingstermijn voor de panelleden een bron van kennis is. Meerdere respondenten geven aan bijvoorbeeld graag te willen weten wanneer hun DUO-studieschuld is afgelopen of wanneer een negatieve BKR-registratie verloopt, zodat daarna weer de mogelijkheid is een creditcard te nemen. Ze illustreren met deze voorbeelden dat het gaat om situaties waarin bewaartermijnen effect hebben op hun leven en daarom belangrijk zijn om te weten. Overigens is de BKR geen overheidsregistratie, en kan deze derhalve niet via MijnOverheid ontsloten worden. Maar uit het informatiekundige deel van dit onderzoek zijn ook voorbeelden naar voren gekomen uit bijvoorbeeld de zorg, waarbij ouders willen weten wanneer hun ondertoezichtstelling niet meer geldt, of als ouders ten onrechte zijn gemeld bij het Advies- en Meldpunt Kindermishandeling.

3.4.5 Module met contactgegevens

Over de module met contactgegevens zijn de meningen verdeeld. Eenmanszaken ondersteunen de functionaliteit, zolang ze zelf de gegevens kunnen beheren en wijzigen. Ook de meerderheid van de deelnemers van de oudere doelgroep staan positief tegenover deze functionaliteit:

“Prima om primaire contactgegevens toe te voegen aan overheidscontacten, wel zelf aan te passen.”

“Ja prima, indien te wijzigen en indien bekend hoe de overheid ze gebruikt.”

De jongere doelgroepen ondersteunen de functionaliteit over het algemeen niet. De eerste reactie is dat zij al bereikt kunnen worden, dus wat wil de overheid nog meer weten? Ook wordt het gezien als eenrichtingsverkeer. Als de overheid de panelleden kan bereiken, dan willen de panelleden ook contact kunnen opnemen met de overheid:

“Wij zijn wel vindbaar, maar de overheid niet.”

“De overheid heeft hier vooral wat aan; de burger niet.”

“Ze kunnen mij wel bellen, maar ik hen niet.”

Degenen die wel hun contactgegevens willen delen, vinden het vooral handig hun e-mailadres op te geven. Dit scheelt namelijk post. Ook vinden zij het geen probleem om hun bankrekeningnummer door te geven. Zij het, dat zij wel meerdere bankrekeningnummers willen hebben en beheren. Voor veel administratieve zaken hanteren de panelleden, en met name ook de gesproken eenmanszaken, andere bankrekeningnummers en dat willen ze graag zo houden.

“Wij werken met zakelijke en particuliere rekeningen. Je moet op MijnOverheid de verschillende rekeningnummers op kunnen geven.”

Het doorgeven van een mobiel telefoonnummer hoeft van deze groep niet. Dit beschouwen zij als een privénummer dat de overheid niet hoeft te weten. Zij zitten niet op allemaal telefoontjes van de overheid te wachten, zogezegd. In de burgerpanels is geen reactie gegeven op het alternatief correspondentieadres. Kennelijk wordt dit niet als relevant beschouwd.

Van de groep die de module met contactgegevens wel wil, is iedereen het erover eens dat deze gegevens niet in een registratie van de overheid moeten worden vastgelegd. Zij willen het zelf beheren. Zij kunnen dan bijvoorbeeld ook hun e-mailadres wijzigen als ze dat willen. Als er een module in de site wordt gebouwd, zou iedereen ook voor zichzelf kunnen aangeven of en welke contactgegevens ze achterlaten.

3.4.6 Actief delen van gegevens

Deze functionaliteit wordt door de panelleden met de nodige argwaan bekeken. Is de overheid hier bezig om via een omweg invloed te nemen op het privédomein van de burger? Er is sprake van het nodige wantrouwen. De overheid moet niet groter gemaakt worden dan dat hij is. Bovendien regelen de panelleden zelf wel dat zij hun gegevens met derde partijen delen.

Het blijkt dat de wijze van vormgeving van de functionaliteit van veel belang is. Zolang de burger zelf bepaalt wanneer (eenmalig) welke gegevens gedeeld worden met andere overheidsorganisaties of derde partijen kan men er het voordeel van inzien. Maar wanneer een burger gevraagd wordt een vinkje te zetten om een verstrekking aan derden, waaronder private partijen, te effectueren ontstaat het beeld dat daardoor allerlei gegevensstromen op gang komen waar de burger geen grip meer op heeft. Met wie worden deze gegevens allemaal gedeeld? Komen ze straks op straat te liggen? Twee panelleden geven het volgende aan:

> *“Straks gaat de overheid denken dat dit een aardige inkomstenbron is. Dat mag vast niet, maar daar zie ik een gevaar in.”*

> *“Als ze dit goed aanpakken worden ze groter dan Facebook.”*

De panelleden maken dus een duidelijk onderscheid tussen het publieke en het private domein. De overheid heeft niks met dat private domein te maken en dat moet zo blijven. Burgers willen honderd procent controle hebben over de verstrekking en zelfs dan voelt niet iedereen voor een dergelijke functionaliteit. Een aantal panelleden maakt wel een onderscheid tussen het private en het semi-private domein. Zo vinden zij dat het wel moet kunnen hun gegevens met zorg, scholen en verzekeringsmaatschappijen te delen.

De groep eenmanszaken toont zich minder wantrouwend. Van hen wil het merendeel wel de mogelijkheid hebben om gegevens te delen. Zij geven aan dit prima te vinden, zolang ze zelf beslissen met wie ze gegevens delen.

3.5 Samenvatting burgerperspectief

Overall komt uit de burgerpanels naar voren dat burgers het belangrijk vinden te weten welke gegevens en informatie de overheid over hen registreert. Hoewel het begrip informatiepositie vrij abstract is, blijken de

meeste burgers hier wel degelijk een beeld en gevoel bij te hebben. Over het algemeen hebben ze het beeld dat de overheid veel van hen weet, maar dat zij lang niet altijd weten wat de overheid van hen weet.

Daarom vinden vrijwel alle burgers in de burgerpanels inzage in gegevens en gegevensverkeer en verwijderingstermijnen van belang om hun informatiepositie ten opzichte van de overheid te versterken. Ook de mogelijkheid om een correctieverzoek te kunnen doen via MijnOverheid past daarbij. Burgers geven aan dat inzage in hun persoonlijke kerngegevens handig is, maar dat het eventueel verstrekken van gegevens op het derde detailniveau (zie paragraaf 2.4) waarschijnlijk tot een informatie-overload zou leiden.
Over een eventuele module met contactgegevens en het actief delen van gegevens met derden zijn de burgers minder positief. De meerwaarde voor hun informatiepositie wordt minder gezien.

Idealiter is er enige voorkeur voor het tonen van de gegevens in MijnOverheid. De panelleden ondersteunen echter zowel een ‘dikke’ als een ‘dunne’ variant van MijnOverheid, waarbij MijnOverheid in de ‘dikke’ variant het unieke loket is en in de ‘dunne’ variant MijnOverheid naast de MijnDomeinen functioneert.

Burgers die ervaringen hebben met het (laten) aanpassen van onjuiste gegevens of informatie geven aan dat ze in aanvulling op de inzage- en correctiemogelijkheid eigenlijk liever een soort ‘accountmanager’ hebben die voor hen uitzoekt wat de oorzaak is van het probleem. Hier is met name sprake van wanneer er meerdere overheidsinstanties bij betrokken zijn, en het voor de burger niet altijd duidelijk is waar de oorzaak van het probleem zit, of wie de beheerder is van het ‘onjuiste’ gegeven.

Voor de goede orde wordt hierbij opgemerkt dat in dit hoofdstuk de juridische, organisatorische en financiële consequenties nog niet zijn meegewogen.

4 Bevindingen juridisch perspectief

4.1 Inleiding

Een aantal van de onderzochte functionaliteiten heeft een nauwe relatie met de Wet bescherming persoonsgegevens (Wbp). De rechten die burgers kunnen laten gelden, hangen daarnaast ook samen met andere wetgeving, zoals de Algemene wet bestuursrecht (Awb). In dit hoofdstuk wordt een algemene toelichting gegeven op het werkingsgebied en de filosofie van de Wbp en de Awb, waarbij wordt aangegeven wat hiervan de juridische consequenties voor burgers en bestuursorganen zijn bij het gebruik van MijnOverheid. Vervolgens wordt per functionaliteit aangegeven met welk wettelijk kader rekening gehouden dient te worden. Een korte beschouwing over de domeinen controle en zorg sluit het hoofdstuk af.

4.2 Werkingsgebied en filosofie Wbp

Een aantal van de functionaliteiten (inzage, correctie, verwijdering) heeft direct te maken met de Wbp. In de Wbp staat de relatie centraal tussen de persoon wiens gegevens verwerkt worden (de burger) en de verantwoordelijke voor de verwerking van deze gegevens (degene die het doel en de middelen van de verwerking vaststelt, bijvoorbeeld een bestuursorgaan). De werking van de Wbp en de verwezenlijking van de rechten die burgers in dat kader hebben, zijn op deze relatie tussen persoon en verantwoordelijke gebaseerd. Het is essentieel dat de functionaliteiten van MijnOverheid bij deze relatie aansluiten en die niet in de weg staan of ondergraven.

De achterliggende filosofie van de Wbp is een afweging van belangen tussen verantwoordelijken (zoals bestuursorganen) en burgers. Dit is anders dan het beeld dat bij veel mensen leeft, namelijk de gedachte dat de Wbp een wet is die de privacybescherming van bijvoorbeeld burgers voorop stelt. De belangen van de verantwoordelijken wegen in de Wbp ook zwaar. Dat komt bijvoorbeeld tot uitdrukking in het feit dat het inzage-, correctie- en verwijderingsrecht, *relatieve* rechten zijn. Je kunt er als burger wel een beroep op doen, maar als de verantwoordelijke goede argumenten heeft, mag hij het verzoek naast zich neerleggen. Of het om goede argumenten gaat, weegt desgevraagd het College Bescherming Persoonsgegevens (CBP), dan wel in uiterste instantie de rechter. Anders dan bij de Wbp, wordt bijvoorbeeld bij de Wet geneeskundige behandelingsovereenkomst de bescherming van de patiënt voorop gesteld ten opzichte van de hulpverlener. In die wet geldt een bijna absoluut vernietigingsrecht in tegenstelling tot het relatieve correctierecht in de Wbp.

4.3 Elektronische overheidsdienstverlening

Wat betreft elektronische overheidsdienstverlening is afdeling 2.3. toegevoegd aan de Awb. Dit wordt ook wel de Wet elektronisch bestuurlijk verkeer (Webv) genoemd, maar aangezien het slechts te vinden is als een onderdeel van de Awb benoemen wij verder als een afdeling van de Awb. Deze afdeling omvat algemene regels over het verkeer langs elektronische weg tussen burgers en bestuursorganen. De hoofdlijnen kunnen als volgt worden omschreven:

- De bepalingen over elektronisch verkeer met bestuursorganen zijn van toepassing op alle e-diensten die binnen de scope van dit onderzoek vallen.

- Elektronisch verkeer is nevengeschikt aan conventioneel verkeer. De bepalingen stellen dat elektronisch verkeer kan worden aangeboden *naast* de mogelijkheid op papier of via bezoek aan een loket de diensten af te nemen, voor zover het bestuursorgaan de elektronische weg heeft opengesteld. Verplichtstelling van elektronisch verkeer als enige kanaal vereist een expliciete wettelijke grondslag.
- Elektronisch verkeer en het elektronisch verzenden van berichten zoals bedoeld in deze bepalingen moet ruim opgevat worden en omvat websites, e-mail, elektronische transacties, webservices, etc.
- De Awb stelt voorwaarden die bij de uitvoering van e-diensten in acht moeten worden genomen. Dit zijn voorwaarden ten aanzien van:
    - het feit dat de verzender en de ontvanger (dus zowel bestuursorgaan als burger) eerst kenbaar moeten hebben gemaakt dat zij elektronisch bereikbaar zijn;
    - betrouwbaarheid en vertrouwelijkheid van het verkeer, gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt;
    - vereisten van ondertekening;
    - tijdstippen van verzending en ontvangst bij elektronisch verkeer.

Wat betreft de betekenis van de vereisten van betrouwbaarheid en vertrouwelijkheid zijn het Beveiligingsadvies van de het CBP (van 2001, maar op hoofdlijnen nog steeds bruikbaar) en de Handreiking voor overheidsorganisaties van het Forum Standaardisatie ‘Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten’ (2012) relevante documenten. Daaruit blijkt dat de omvang van de gegevensverwerking en de aard van de persoonsgegevens (zijn het bijzondere persoonsgegevens, zoals gezondheid, godsdienst, ras, strafrechtelijk, etc.) bepalend is voor het vereiste authenticatieniveau van MijnOverheid. Dat betekent dat als er binnen MijnOverheid veel gegevens met elkaar gecombineerd worden, dat consequenties heeft voor het vereiste authenticatieniveau.

4.4 Bevindingen per functionaliteit

4.4.1 Inzage in gegevens en gegevensverkeer

Het inzagerecht is in artikel 35 van de Wbp geregeld. Het artikel geeft de volgende formulering voor het inzagerecht van de burger, als betrokkene, ten opzichte van het bestuursorgaan als verantwoordelijke:

1. De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt.
2. Indien zodanige gegevens worden verwerkt, bevat de mededeling een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.
3. Voordat een verantwoordelijke een mededeling doet als bedoeld in het eerste lid, waartegen een derde naar verwachting bedenkingen zal hebben, stelt hij die derde in de gelegenheid zijn zienswijze naar voren te brengen indien de mededeling gegevens bevat die hem betreffen, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.
4. Desgevraagd doet de verantwoordelijke mededelingen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.

Op grond van de wettekst in artikel 35 lid 2 Wbp dient minimaal een overzicht te worden verstrekt van de doelen van de verwerking, de categorieën en ontvangers van gegevens. Dit betekent dat in ieder geval inzicht gegeven dient te worden op wat wij het detailniveau ‘algemeen’ hebben genoemd, aangevuld met gepersonaliseerde gegevens op kerngegevensniveau. Op grond van jurisprudentie dient de specifieke wens van een burger om op gedetailleerd niveau inzage te krijgen gehonoreerd te worden (zie onder andere de Dexia-zaken).

Overigens is het recht op inzage, in bijvoorbeeld (volledige) dossiers, soms ook in sectorale wetgeving geregeld, zoals in de zorg. En bij de GBA moeten bijvoorbeeld op gegevensniveau mutaties worden bijgehouden en opgeslagen volgens bepaalde afspraken (wie, wanneer, wat, etc). Op grond van lid 4 van artikel 35 kan de burger hier ook inzage in vragen. Dit lid geeft de burger het recht om toelichting te vragen op de informatieprocessen die de verantwoordelijke (het bestuursorgaan) uitvoert om tot een beslissing te komen. Inzage op het niveau van kerngegevens die in de besluitvorming zijn gebruikt kan eveneens worden verzocht. Wanneer het bestuursorgaan de gegevens intern voor besluitvorming gebruikt, is het een redelijk verzoek van de burger om daar inzage in te willen op grond van het vierde lid. Dit geldt ook voor de vraag naar de herkomst van de gegevens en de gegevensstromen. Als de verantwoordelijke die informatie niet wil verstrekken, is het aan het CBP of de rechter om hierover te oordelen.

Uit het inzagerecht van de Wbp vloeit geen verplichting voort om voor alle geregistreerden inzage mogelijk te maken via een digitaal medium (bijvoorbeeld MijnOverheid of MijnDomein). Wel bepaalt artikel 18 Wet algemene bepalingen burgerservicenummer (Wabb), dat iedere instelling die het BSN verwerkt verplicht is om op “algemeen niveau” informatie te verstrekken aan het ministerie van BZK over de uitgevoerde processen en de verstrekte categorieën gegevens.

4.4.2 Verzoeken om correctie

Het correctie- en het verwijderingsrecht van de burger staan in artikel 36 van de Wbp. Dit artikel is als volgt geformuleerd:

1. Degene aan wie overeenkomstig artikel 35 kennis is gegeven van hem betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.
2. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.
3. De verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.
4. Indien de persoonsgegevens zijn vastgelegd op een gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, dan treft hij de voorzieningen die nodig zijn om de gebruiker van de gegevens te informeren over de onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming ondanks het feit dat er grond is voor aanpassing van de gegevens op grond van dit artikel.
5. Het bepaalde in het eerste tot en met vierde lid is niet van toepassing op bij de wet ingestelde openbare registers, indien in die wet een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van gegevens is opgenomen.

De voorgestelde functionaliteit in MijnOverheid houdt in dat de burger langs digitale weg een verzoek tot correctie kan indienen als gegevens volgens hem onjuist zijn. De Wbp verzet zich er niet tegen dat het correctieverzoek langs digitale weg wordt gedaan, maar verplicht het ook niet. Het verzoek wordt gedaan aan de verantwoordelijke (in de praktijk van MijnOverheid doorgaans een bestuursorgaan). MijnOverheid houdt zelf ook nog enkele persoonsgegevens bij. In dat geval zou ook bij de verantwoordelijke voor MijnOverheid, in casu BZK, een verzoek om correctie kunnen worden ingediend. In de praktijk zal het echter meestal gaan om correctieverzoeken bij uitvoerende bestuurorganen. In dat geval dient de functionaliteit om een verzoek tot correctie via MijnOverheid dusdanig ingericht te worden dat dit verzoek in juridische zin dezelfde 'status' heeft als een verzoek dat rechtstreeks bij de betrokken verantwoordelijke is ingediend. Dat geldt temeer voor de mogelijkheid om in één keer te verzoeken een gegeven of informatie bij meerdere overheidsorganisaties te laten corrigeren. Overigens is het van belang te vermelden dat een verzoek om correctie ook om andere redenen gedaan kan worden dan alleen dat een gegeven of informatie foutief zou zijn.

Een bestuursorgaan is niet verplicht het verzoek van de burger te volgen. Voor gegevens die in een transactie gebruikt worden (het kerngegevensniveau) zijn er op grond van sectorwetten vaak interne regels en procedures die voorschrijven hoe een gegeven vastgesteld dient te worden en in welke gevallen er een correctie kan of moet worden doorgevoerd. Wanneer het gegeven is ontleend aan een basisregistratie zal het bestuurorgaan het niet zelf corrigeren, maar de burger naar de basisregistratie verwijzen. Of, wanneer de instelling door het verzoek van de burger zelf gerede twijfel heeft gekregen, een terugmelding aan de basisregistratie doen.

Een beslissing op een verzoek om inzage, correctie of verwijdering door een bestuursorgaan geldt, overeenkomstig artikel 45 Wbp, als een besluit in de zin van de Awb. De Awb-rechtsgang is daarop van toepassing, tenzij bijzondere wetgeving geldt, zoals bij de Kadasterwet. Het is dus overeenkomstig de Awb en andere wetten mogelijk om bezwaar en beroep aan te tekenen tegen een overheidsbesluit ten aanzien van een inzage-, correctie- of verwijderingsverzoek. Alvorens naar de bestuursrechter te gaan, kan de burger ook gebruik maken van de geschillenbeslechtingsregeling van het CBP (overeenkomstig artikel 47 Wbp).

In de kern biedt de Wbp dus een recht op *verzoek* tot correctie, als een relatief, maar geen absoluut correctierecht. Immers de bevoegde instantie mag uiteindelijk een belangenafweging maken op grond van argumenten. De vraag of die argumenten valide zijn kan worden voorgelegd aan het CBP of in uiterste instantie de rechter.

4.4.3 Vermelden verwijderingstermijn

Artikel 10 Wbp behandelt de bewaartermijn van gegevens. Het eerste lid van dit artikel luidt als volgt:

> Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

Artikel 10 en daarmee de voorgestelde functionaliteit 'vermelden verwijderingstermijn' heeft geen relatie met artikel 36 van de Wbp (correctie- en verwijderingsrecht). Daar gaat het immers om gegevens die "feitelijk

onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend dan wel anderszins in strijd met een wettelijk voorschrift" worden verwerkt. De functionaliteit 'vermelden verwijderingstermijn' in MijnOverheid heeft betrekking op gegevens die juist zijn en terecht zijn verwerkt, maar die betrekking hebben op het verleden en na verloop van tijd verwijderd dienen te worden.

In het dienstverleningsdomein zijn weinig wetten die expliciet verplichten om na een bepaalde periode gegevens te verwijderen. De bovenstaande hoofdregel uit de Wbp, artikel 10 lid 1, geldt in deze gevallen. Iedere verantwoordelijke dient op basis van dit artikel zelf de bewaartermijn te bepalen, tenzij een sectorale wet expliciet een termijn aangeeft. Dat laatste is bijvoorbeeld het geval in de zorg, waar een bewaartermijn van 15 jaar geldt, of zoveel langer als noodzakelijk is voor een goede hulpverlening. Soms is de Archiefwet van toepassing. Daarin wordt bepaald gedurende welke periode gegevens juist *niet* verwijderd mogen worden. Daarna mogen de gegevens verwijderd worden, maar dat is op basis van de archiefwet niet verplicht.

In de voorgestelde nieuwe ontwerp-privacyverordening van de Europese Unie staat "het recht om vergeten te worden" overigens centraal. Te verwachten is dat in de komende jaren dit recht een steeds prominentere positie zal krijgen. Keuzevrijheid, de burger kiest of gegevens mogen worden uitgewisseld, is een ander begrip dat in de nieuwe ontwerpverordening centraal staat.

4.4.4 Een module met contactgegevens

Anders dan bij inzage, correctie en de verwijderingstermijn van gegevens sluit deze module niet aan op formele rechten die burgers hebben in het kader van de Wbp. Er is voor deze functionaliteit geen specifiek juridisch kader. Voor de toepassing van de Wbp betekent dit dat voor het verzamelen van contactgegevens - uitgaande van 'gewone' persoonsgegevens - de algemene bepalingen uit de Wbp voor het beschermen van persoonsgegevens gelden. In MijnOverheid worden al enkele contactgegevens opgenomen. Om de berichtenbox te gebruiken is DigiD nodig. In dat kader wordt het e-mail adres en (bij niveau 2 authenticatie, DigiD-midden) ook het mobiele telefoonnummer al genoteerd. Op grond van het doelbindingscriterium van de Wbp mogen deze gegevens niet voor andere doeleinden, bijvoorbeeld als algemeen contactgegeven voor de hele overheid, worden gebruikt.

4.4.5 Actief delen van gegevens

De kabinetsreactie geeft als voorbeeld van het actief delen van gegevens dat een uittreksel uit de GBA of een inkomensverklaring ook in elektronische vorm vanuit MijnOverheid zou moeten kunnen worden ingediend. Het kan zijn dat bestaande wetgeving nu (ook) een verklaring op papier eist en dus zal moeten worden aangepast met de mogelijkheid uitsluitend een elektronische indiening te accepteren. Dat zijn echter geen grote wijzigingen. De Awb stelt immers dat papier en elektronisch verkeer nevengeschikt zijn aan elkaar.

Ingrijpender is een interpretatie - van het actief delen van gegevens - waarin het aan de burger is om te beslissen aan welke private partij hij gegevens verstrekt. De burger kan dit doen door toestemming te verstrekken, tenzij de wetgever de burger op dit punt wil beschermen. Bij erfelijkheidsgegevens is dit bijvoorbeeld het geval (overeenkomstig artikel 21 lid 4 Wbp). Toestemming door de burger dient te voldoen aan de volgende vereisten op grond van de Wbp en de Europese richtlijn bescherming persoonsgegevens (95/46/EC):

- De betrokkene moet in vrijheid zijn wil kunnen uiten.
- De wilsuiting moet betrekking hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen.
- De betrokkene moet voor een goede oordeelsvorming over de noodzakelijke inlichtingen beschikken.

In de praktijk blijkt dat hoe meer persoonsgegevens worden gezien als handelswaar, hoe meer de betrokken personen kwetsbaar worden en geneigd zijn om hun toestemming te geven voor verschillende redenen, die niets te doen hebben met de oorspronkelijke ideeën achter de vereisten voor toestemming. Bovendien kunnen mensen als zij onder stress staan veel minder goed keuzes maken. In dat geval hebben ze begeleiding nodig (Papernote, De informatiepositie van de patiënt, HEC, 2010).

4.4.6 Dienstverlening, controle en zorg

Uit het voorgaande blijkt al dat juridisch het onderscheid tussen dienstverlening, zorg en controle relevant is. Medische gegevens die in de zorg worden gegenereerd vallen op grond van artikel 21 Wbp onder het regime van de bijzondere (gevoelige) gegevens waarvoor extra zorgvuldigheidseisen gelden. Dit betekent dat het verboden is om gezondheidsgegevens te verwerken, tenzij de Wbp of een andere wet dit expliciet als uitzondering mogelijk maakt.

In het kader van opsporing en controle voeren bijvoorbeeld de AIVD en de politie opsporingsactiviteiten uit die niet (gelijk) aan de burger bekend gemaakt hoeven te worden. Gegevensverwerkingen die bijvoorbeeld vallen onder de Wet op de inlichtingen- en veiligheidsdiensten 2002 en de Politiewet vallen ook niet onder de Wbp. Als gegevensverwerkingen ten behoeve van controle wél onder de Wbp vallen, geldt op grond van artikel 43 Wbp dat de rechten van de burger (inclusief het inzagerecht) niet gelden indien dit noodzakelijk is ter voorkoming, opsporing en vervolging van strafbare feiten. Na afloop van het onderzoek dient de burger die ten onrechte is onderzocht wél te worden geïnformeerd. De burger die terecht is onderzocht wordt uiteraard al geïnformeerd.

4.5 Samenvatting juridisch perspectief

De Wet bescherming persoonsgegevens (Wbp) regelt het recht van de burger op inzage, correctie en verwijdering van persoonsgegevens in registraties van overheidsorganisaties. Op grond van de Wbp dient aan burgers in ieder geval inzicht gegeven te worden in het doel van de gegevensverwerking en de overige ontvangers c.q. gebruikers van persoonsgegevens, aangevuld met gepersonaliseerde gegevens op kerngegevensniveau waarop een besluit is gebaseerd. Op grond van jurisprudentie dient de specifieke wens van een burger om op meer gedetailleerd niveau inzage te krijgen gehonoreerd te worden.

Overheidsorganisaties zijn niet verplicht om (bijvoorbeeld via MijnOverheid) actief, uit eigen beweging, gegevens uit hun registratie(s) aan burgers te verstrekken. Ook mogen zij op basis van goede argumenten (bijv. onevenredig hoge kosten) een verzoek om inzage, correctie of verwijdering weigeren. Het CBP, en in uiterste instantie de rechter, bepaalt zo nodig of het echt om goede argumenten gaat. Daarnaast is het verplicht om een bewaartermijn vast te stellen of de bewaartermijn te volgen van een toepasselijke sectorwet. Dit betekent dat ontsluiting van persoonlijke gegevens in de MijnDomeinen en aansluiting bij MijnOverheid op dit moment gebeurt op eigen initiatief en overtuiging van de individuele overheidsorganisaties.

Vanuit juridisch perspectief vergt vrijwillig gebruik van de functionaliteiten van MijnOverheid – zowel van de zijde van de burger als de bestuursorganen – geen aanpassing van wetgeving. In dat geval is de positie van MijnOverheid met de minister van BZK als verantwoordelijke – slechts beperkt tot de enkele persoonsgegevens die MijnOverheid zelf bijhoudt op verzoek van de burger. De inzage-, correctie- en verwijderingsverzoeken hebben in de praktijk echter meestal betrekking op de bestanden van de uitvoerende bestuursorganen. Deze bestuursorganen zijn zelf verantwoordelijke in de zin van de Wbp en mogen binnen de bestaande wettelijke kaders hun eigen afweging maken. Indien, via het toevoegen van functionaliteiten aan MijnOverheid, de bestuursorganen verplicht worden tot medewerking aan verzoeken van burgers, is aanvullende wetgeving vereist. Ook indien MijnOverheid zonder toestemming van de burger persoonsgegevens wil verwerken is aanvullende wetgeving vereist.

5 Bevindingen informatiekundig perspectief

5.1 Inleiding

In dit hoofdstuk staan de uitkomsten van de gesprekken die met uitvoeringsinstellingen, centrale en decentrale overheden zijn gevoerd over het informatiekundig perspectief en de organisatorische, technische en financiële gevolgen die de functionaliteiten kunnen hebben. In bijlage I is een overzicht opgenomen van organisaties en geïnterviewde personen. In paragraaf 5.2. worden de bevindingen per functionaliteit besproken. Zijn de functionaliteiten informatiekundig gezien haalbaar en welke consequenties hebben de functionaliteiten voor de (al aangesloten) overheidsorganisaties? In paragraaf 5.3. staan de resultaten van de internationale quick scan. In paragraaf 5.4. staat een aantal algemene bevindingen beschreven. In dit hoofdstuk wordt ook stilgestaan bij de tweede en derde onderzoeksvraag betreffende de verplichtbaarheid van MijnOverheid en de vraag of MijnOverheid invulling kan geven aan artikel 18 van de Wabb. De laatste paragraaf 5.5 geeft de consequenties van de bevindingen voor het beantwoorden van de onderzoeksvraag weer. Zoals voorgaande hoofdstukken wordt alleen het informatiekundig perspectief geschetst, zonder die te relateren aan de andere perspectieven.

Voor de meeste gesprekspartners waren de nieuwe functionaliteiten voor MijnOverheid min of meer een ‘ver van mijn bed show’. Het faciliteren van burgers met dergelijke functionaliteiten heeft de laatste jaren maar beperkte beleidsmatige aandacht gekregen. Dat geldt voor op het niveau van uitvoeringsorganisaties, maar ook op centraal niveau: in het iNUP staan bijvoorbeeld geen prestatieafspraken die hierop betrekking hebben. Dit betekent dat gesprekspartners vaak ter plekke een mening moesten vormen en ventileren en alleen in heel globale termen over de consequenties konden spreken. Het was om die reden dan ook niet mogelijk om een gedetailleerd inzicht te krijgen in de organisatorische en financiële consequenties van de nieuwe functionaliteiten voor de uitvoeringsorganisaties, centrale en decentrale overheden.

5.2 Bevindingen per functionaliteit

5.2.1 Inzage in gegevens

Om het doel van het kabinetsbeleid te halen en burgers in staat te stellen zichzelf te helpen wanneer ze in de datakluwen van de overheid verstrikt raken is inzage op persoonlijk gedetailleerd niveau nodig. De bestaande situatie is, dat een aantal basisregistraties haar gegevens op gedetailleerd niveau ontsluit via MijnOverheid. Dat geldt bijvoorbeeld voor de GBA. Voor gemeenten betekent inzage bieden op de basisregistraties via MijnOverheid weinig eigen inspanning, omdat dit verloopt via landelijke voorzieningen. Voor de basisregistraties lijken er weinig problemen om inzage op gedetailleerd niveau te bieden.

Anders is dat voor uitvoeringsinstellingen wanneer ze hun *dienstverleningsgegevens* op gedetailleerd gepersonaliseerd niveau inzichtelijk moeten maken. Voor alle organisaties waarmee gesproken werd, is dat enorm complex, zowel technisch, organisatorisch en daardoor ook financieel. Dit wordt veroorzaakt door de wijze waarop de processen en daarbij behorende informatievoorziening zijn georganiseerd. De organisatie is

erop gericht de transacties met burgers correct en efficiënt af te handelen, maar niet om alle gegevensverwerkingen die daarbij voorkomen inzichtelijk te maken. Wanneer dat wordt geëist is het nodig om alle mutaties op BSN-niveau te loggen. Organisaties die hier onderzoek naar hebben gedaan (SVB, Belastingdienst) geven aan dat dit technisch een zeer grote opgave is. Mutaties loggen heeft alleen toegevoegde waarde wanneer de gegevens ook analyseerbaar zijn en het “gegevenspad” in de tijd en in het besluitvormingsproces is te volgen. De bestaande werkwijze is dat mutaties niet worden gelogd. Wanneer er, naar aanleiding van bezwaar of beroep of anderszins, aanleiding is om aan de juistheid van een gegeven te twijfelen wordt daar gericht onderzoek naar gedaan.

Inzage bieden op het niveau van kerngegevens is minder ingrijpend. Het kerngegevensniveau betekent dat de kerngegevens waarop de genomen beslissing in een transactie gebaseerd is, voor de burger ontsloten worden. Dat sluit wel aan bij de transactiegerichte benadering. Organisaties die vergevorderd zijn met het invoeren van zaakgericht werken hebben deze gegevens in één of andere vorm al centraal beschikbaar. Met name de decentrale overheden (gemeenten, provincies en waterschappen) waren daar de afgelopen jaren mee bezig. De stand van zaken bij het invoeren van zaakgericht werken verschilt van zeer vergevorderd tot nog in een beginstadium.

Voor uitvoeringsorganisaties verschilt het ook sterk of de kerngegevens al via een geautomatiseerd routineproces op een centraal punt binnen de organisatie beschikbaar zijn. Wanneer dat het geval is, hoeft alleen de ontsluiting via MijnOverheid te worden georganiseerd, waarbij MijnOverheid een presentatielaag betreft waarin actuele gegevens getoond dienen te worden. Zijn de gegevens nog niet centraal beschikbaar, dan zal het nog aanzienlijke inspanningen vergen om dat te realiseren. Het betreft echter investeringen die voor het inrichten van zaakgericht werken toch nodig zijn.

Het idee om burgers zo gedetailleerd inzage in de gegevens te bieden dat ze bij problemen zelf in staat zijn de datakluwen te ontwarren en hun (gegevens)problemen op te lossen acht men dus nauwelijks realiseerbaar. Soms vindt men het ook ongewenst. De burger moet niet als een soort privédetective de processen binnen de overheid hoeven te onderzoeken. Die zijn daar veel te ingewikkeld voor en de hoeveelheid gegevens is enorm. Zit de burger echt te wachten op telefoonboeken met gegevens en transacties? En zelfs als dat zo is en de inzage perfect zou zijn, is dat nog niet voldoende om een burger zelf haar problemen te laten oplossen, daar is meer voor nodig. Alternatieve voorstellen van de respondenten zijn:

- Geef een burger die een (gegevens)probleem meldt de garantie dat het probleem wordt uitgezocht en dat het resultaat aan hem wordt teruggekoppeld. Vul zo een vorm van casemanagement in. Inhoudelijk komt deze suggestie van de uitvoeringsorganisaties in sterke mate overeen met de wens van burgers om hulp te krijgen van een accountmanager.
- Pak het probleem aan dat organisaties hun verantwoordelijkheid niet altijd waarmaken. Dat is met name belangrijk in het verkeer tussen basisregistraties en hun afnemers en in ketens. Over het algemeen is op papier voldoende duidelijk wat de verantwoordelijkheden zijn van de gebruikende organisaties en van de (soms meerdere) basisregistraties die bij een specifiek probleem van een burger betrokken zijn. In de praktijk neemt niet iedere partij op een controleerbare manier zijn verantwoordelijkheid. Andere partijen gaan omwegen bewandelen om problemen te vermijden of met een work around op te lossen. Begrijpelijk gedrag dat echter leidt tot organisatorische chaos. Om de impasse die op dit punt aan het ontstaan is te doorbreken, wordt gesuggereerd een “gegevensautoriteit” in het leven te roepen die partijen, ook in individuele gevallen, op hun verantwoordelijkheid aanspreekt.

- Maak onderscheid tussen de behoefte bij burgers om de overheid te controleren en zicht te hebben op de informatie waarover de overheid beschikt enerzijds en de informatie die nodig is om problemen op te lossen. Voor het overzicht lijkt het kerngegevensniveau ruim voldoende. Wanneer er een probleem is wil de burger (terecht, zo vindt men) daarover het naadje van de kous weten. Doe dan gericht onderzoek dat zo nodig ook op gedetailleerd gegevensniveau plaatsvindt.

Het beeld dat ontstaat is als volgt. Basisregistraties zijn wellicht (er is maar een enkele basisregistratiehouder gesproken) in staat om hun gegevens op gedetailleerd niveau te ontsluiten. Voor uitvoeringsorganisaties en decentrale overheden is dit zeer complex, een aanzienlijke koerswijziging en daardoor prohibitief duur. Bovendien hebben enkele organisaties de ervaring dat het doel niet bereikt wordt: burgers zijn niet in staat problemen zelf op te lossen. Inzage op kerngegevens is op termijn (voor de ene organisatie sneller dan voor de andere) wel een realistische ambitie.

5.2.2 Inzage in gegevensverkeer

Inzage in het gegevensverkeer tussen organisaties biedt MijnOverheid momenteel niet. Nog meer dan voor inzage in gegevens geldt hier dat het in beleidsmatig opzicht een nieuwe wens is die nog niet in bestaand beleid is verankerd. Vrijwel geen enkele van de onderzochte organisaties is er zelf mee bezig. Consequentie hiervan is, dat er geen processen zijn waarmee de uitwisselingen inzichtelijk gemaakt kunnen worden voor burgers. Een uitzondering vormt het Bureau Keteninformatisering Werk en Inkomen (BKWI). Dat is een organisatie die specifiek gericht is op het faciliteren van gegevensverkeer tussen organisaties. Het BKWI geeft aan dat zij met weinig inspanning inzage op gedetailleerd niveau inzage in het gegevensverkeer kan bieden.

Basisregistraties en organisaties als het BKWI lijken het best geëquipeerd om inzage in de verstrekkingen te doen. Op grond van de autorisatietabel zou het bijvoorbeeld voor BPR relatief eenvoudig moeten zijn om op algemeen gepersonaliseerd niveau inzage in gegevensverkeer te verstrekken. Voor een burger is het informatief om te weten welke organisaties structureel gegevens uit de GBA verstrekt krijgen. Vervolgens kan de burger zelf de betreffende organisaties om inzage vragen.

In dit onderzoek blijft buiten beschouwing dat ook private partijen gegevens leveren aan uitvoeringsinstellingen. De inkomstenbelasting is een treffend voorbeeld. Om de Belastingdienst in staat te stellen de opgave van de burgers te controleren, leveren tal van private organisaties zoals werkgevers en financiële instellingen gegevens aan. Voor de burgers is zicht op deze gegevensstromen evenzeer van belang als zicht op wat zich binnen de overheid afspeelt.

Om de nieuwe functionaliteit vorm te geven zijn basisregistraties en organisaties zoals het BKWI, waarvoor faciliteren van gegevensverkeer de core business vormt, het best geëquipeerd. Voor uitvoeringsinstellingen is het zeer complex en prohibitief duur.

5.2.3 Verzoeken om correctie

Voor de respondenten hoort een mogelijkheid om op een eenvoudige manier een verzoek om correctie in te dienen logisch bij inzage: wanneer een burger gegevens ziet die naar zijn mening niet juist zijn, dient het mogelijk te zijn om aanpassing daarvan te vragen. MijnOverheid kan daarbij het doorgeefluik zijn. Relevant is

de ervaring van het BKWI: dat heeft de ontwikkeling van een generieke correctievoorziening gestopt, omdat de correctievoorziening te complex is en er te weinig vraag naar was, waardoor dit een te dure oplossing werd.

Diverse keren waarschuwen respondenten dat het wel zaak is om daarbij geen valse verwachtingen te wekken. Iedere organisatie past regels toe bij het vaststellen van gegevens en die regels blijven van kracht, ook als een burger van mening is dat de gegevens onjuist zijn. Dat is ook het geval wanneer gegevens door een basisregistratie aan de betreffende organisatie zijn verstrekt: dan zal de betreffende basisregistratie dienen te beoordelen of de correctie wordt doorgevoerd. Men vindt dat de burger wel mag verwachten dat haar melding van een onjuist gegeven in ontvangst wordt genomen, wordt uitgezocht en dat de uitkomst van het onderzoek aan hemaar wordt teruggekoppeld. Door een correctieverzoek als een zaak te beschouwen, kunnen organisaties die zaakgericht werken hebben ingevoerd, de afhandeling van het correctieverzoek met bestaande mechanismen bewaken en de burger (via de lopende zaken functie van MijnOverheid) met relatief weinig extra inspanning op de hoogte houden van de status. Wanneer organisaties hun verantwoordelijkheid voor het onderzoeken van het verzoek van de burger onvoldoende waarmaken kan de eerder voorgestelde gegevensautoriteit een burger ondersteunen.

Diverse malen is aangekaart dat de verhouding helder moet blijven tussen een verzoek om correctie en de bezwaar en beroepsprocedure die uitvoeringsorganisaties ook kennen voor het geval een burger een besluit van de uitvoeringsorganisatie niet wil accepteren. Wanneer het onderscheid scherp wordt gehanteerd kan het correctierecht echter een waardevolle aanvulling vormen op bezwaar en beroep. Niet de beslissing wordt aangevochten maar de juistheid van een gegeven. Correctie kan ertoe leiden dat de beslissing moet worden aangepast, maar dat hoeft niet altijd het geval te zijn. Door een apart proces in het leven te roepen dat gericht is op beoordelen van de juistheid van de gebruikte informatie wordt vermeden dat meteen het juridisch zwaarste middel ingezet wordt.

5.2.4 Vermelden van de verwijderingstermijn

Vermelden van de verwijderingstermijn wordt vaak geassocieerd met de uitvoering van de Archiefwet, maar is zoals uit het vorige hoofdstuk bleek in de eerste plaats een functionaliteit die voor de verantwoordelijke voortvloeit uit de Wbp om voor de betreffende gegevensverwerking een bewaartermijn vast te stellen. Documenten en digitale gegevens die in het archief geplaatst worden, mogen op grond van de Archiefwet na een bepaalde periode verwijderd worden. Sommige organisaties voeren daar actief beleid op, anderen gebruiken gegevens op een zeker moment niet meer zonder ze actief te verwijderen. De in dit onderzoek bekeken functionaliteit heeft echter betrekking op een ander geval. Het punt is niet zozeer of gegevens verwijderd mogen worden, maar dat ze verwijderd *moeten* worden op grond van de Wbp of sectorale wetgeving. Wanneer dat het geval is, kunnen sommige gesprekspartners zich voorstellen dat dit een geruststellende gedachte voor burgers is: een Big Brother die vergeet is minder bedreigend: “het recht om vergeten te worden”.

Wanneer gegevens op kerngegeven of gedetailleerd gepersonaliseerd niveau ontsloten zijn voor burgers, is het niet heel veel extra werk om daar ook de verwijderingstermijn bij te vermelden. Dat vergt echter wel dat de verantwoordelijke eerst een bewaartermijn vaststelt. Echt alles verwijderen is vervolgens complex. Zowel als het gaat om verwijderen van bestanden op grond van de verplichting van de verantwoordelijke om te voldoen aan de bewaringstermijnplicht, als waar het gaat om het verwijderen van gegevens op verzoek van de burger. Het tonen van de actuele gegevens vergt namelijk veel gerichte activiteiten om het overzicht af te leiden uit het applicatielandschap waarmee de processen worden uitgevoerd. Om tot effectief verwijderen te kunnen

overgaan dient de relatie tussen het gegeven en het voorkomen ervan in de onderliggende databases langdurig in stand te blijven. Niet alleen het archief maar ook back-up bestanden dienen bijvoorbeeld te worden geschoond om echt op geen enkele wijze meer de gegevens te kunnen achterhalen. In de praktijk kan dit praktisch zo goed als onmogelijk zijn, bijvoorbeeld bij internetbestanden.

Dit leidt tot de aanbeveling van enkele gesprekspartners om het verwijderingsbeleid te richten op bestanden waarvan de burger de meeste last ondervindt wanneer verwijdering achterwege blijft. Dat kan in de dienstverlening bijvoorbeeld om hypotheken gaan die moeten worden doorgehaald. Meestal hebben de gegeven voorbeelden betrekking op controle en zorg. Als een gezin bijvoorbeeld onder toezicht staat, dan wil je als ouder weten wanneer dat niet meer geldt. Of, als ouders ten onrecht bij het Advies- en Meldpunt Kindermishandeling zijn gemeld, dan wil je de melding kunnen verwijderen. Uit het gesprek met een jeugdzorginstelling bleek dat het in het zorgdomein – veel meer dan in het dienstverleningsdomein - als logisch en noodzakelijk beschouwd wordt dat gegevens verwijderd moeten worden en burgers inzage zouden moeten hebben in de verwijderingstermijn. Sterker nog, zij zouden zelf met een knop een verzoek tot het verwijderen van gegevens moeten kunnen doen. In de dienstverlening ondervindt men in de praktijk op dit moment weinig problemen en men veronderstelt dat dit ook voor burgers geldt. Er is dan ook weinig gevoel van urgentie.

5.2.5 Een module met contactgegevens

De voorgestelde functionaliteit van een module met contactgegevens die onderzocht is betreft de volgende gegevens: bankrekeningnummer, mobiel telefoonnummer, e-mailadres en alternatief correspondentieadres.

Een aantal gesprekspartners legt bij het bespreken van de module met contactgegevens direct de link met de voorstellen van werkgroep 12 Compacte rijksdienst om burgers te verplichten één rekeningnummer te kiezen in hun relatie met de overheid. Dat is efficiënter voor de overheid (er is een besparing berekend van tientallen miljoenen euro's) en vermindert fraudemogelijkheden. Een reden om voor MijnOverheid te kiezen is dat het dan juridisch eenvoudig te regelen zou zijn.

Het 06-nummer wordt gezien als een servicegegeven waarmee de dienstverlening verbeterd kan worden.

Wanneer de burger één e-mail adres gebruikt in het verkeer met de overheid (een enkeling wil ook dit verplichten) is dat eenvoudiger voor de burger zelf en voor de overheid. Overigens wordt beoogd steeds meer verkeer via de berichtenbox van MijnOverheid te laten verlopen en op deze wijze wordt e-mailverkeer juist ontmoedigd.

Bij een tijdelijk adres hebben de meeste gesprekspartners weinig beeld van de voor- en nadelen. Zo'n adres zou overbodig kunnen zijn wanneer de burgers voor hun communicatie met de overheid vooral de berichtenbox gebruiken.

Over de status van de gegevens verschillen de beelden. Het zijn geen authentieke gegevens omdat de burger ze naar believen kan aanpassen. Sommigen zien ze als servicegegevens: wanneer de burger het prettig vindt om op één plaats zijn contactgegevens op te geven is dat voor overheid en burger makkelijker. Doet hij dat niet, dan blijft iedere uitvoeringsinstelling zelf steeds contactgegevens uitvragen. Anderen vinden dat er wel eisen gesteld moeten worden aan de gegevens (met name het e-mailadres) en dat het gebruik voor de burger niet vrijblijvend moet zijn: er wordt geopperd dat het toch een soort basisregistratie moet zijn. Wanneer het een

basisregistratie wordt, is MijnOverheid een vreemde plaats om die te beleggen: daar is MijnOverheid niet voor gemaakt.

De conclusie is dat het onderwerp contactgegevens over het algemeen benaderd wordt vanuit het perspectief en het belang van de overheid zelf. Verondersteld wordt dat de burger het ook prettig zal vinden om één keer op één plaats contactgegevens te verstrekken die vervolgens door de hele overheid worden gebruikt.

5.2.6 Actief delen van gegevens

Op de functionaliteit die burgers in staat stelt om hun gegevens zelf ter beschikking te stellen aan private partijen wordt heel verschillend gereageerd. De reacties variëren van “hier staan we positief tegenover” tot “hier is geen rol voor de overheid”. De meeste reacties zijn negatief. Verschillende keren wordt gerefereerd aan het bestaande beleid om de publieke en private sfeer te scheiden, daarmee zou dit voorstel in strijd zijn.

Soms wordt betwijfeld of de burger hiermee wel geholpen is: grote bedrijven zullen geld aan de gegevens gaan verdienen en de burger voor het blok zetten om ze af te geven. Op die manier kan de burger onder oneigenlijke druk worden gezet. De informatiepositie van de burger wordt eerder zwakker dan sterker.

Niet iedereen heeft hetzelfde beeld bij de functionaliteit. De kabinetsreactie geeft als voorbeeld dat burgers soms aan private partijen een uittreksel uit de GBA of een inkomensverklaring van de Belastingdienst moeten verstrekken. De functionaliteit in MijnOverheid houdt in dat dit gegeven niet op papier wordt verstrekt, maar dat de burger het zelf digitaal kan verstrekken vanuit MijnOverheid. Wanneer de onderzoekers dit voorbeeld aanhalen heeft eigenlijk niemand daar bezwaar tegen. Het GBA-uittreksel en de inkomensverklaring worden gevraagd wanneer een private instelling niet voldoende heeft aan een verklaring van de burger zelf, maar een door de overheid vastgesteld gegeven verlangt. De meeste bezwaren lijken er betrekking op te hebben dat deze gegevens zonder wettelijk kader door burgers aan private partijen verstrekt kunnen worden en door private partijen kunnen worden gebruikt.

De vraag is in het onderzoek opgenomen vanwege een initiatief waarbij Manifestpartijen momenteel een aantal pilots uitvoeren rond gegevensverzameling en centrale ontsluiting middels een private partij (Qiy). Dat is weer een andere situatie, in de zin dat de gegevens getransporteerd worden naar een andere omgeving dan MijnOverheid waar de burger ze zelf voor eigen doeleinden kan gebruiken. Met slimme apps kan de burger zelf de gegevens van verschillende overheidsinstanties relateren en analyseren. Om burgers hierin te faciliteren dient MijnOverheid van een faciliteit voor gegevensexport te worden voorzien waarmee een burger zijn eigen gegevens kan beheren. Sommigen vinden dat prima, dan is duidelijk dat de gegevens niet meer onder de verantwoordelijkheid van de overheid vallen en dat geen enkele burger of private partij de overheid ergens op kan aanspreken. Anderen zien ook hier het gevaar dat de informatiepositie van de burger eerder wordt verzwakt dan versterkt.

5.3 Bevindingen internationale quick scan

Denemarken, Estland en Frankrijk kennen een overheidssite vergelijkbaar aan de opzet van www.overheid.nl en MijnOverheid[2]. Een algemene site biedt algemene informatie en een persoonlijke site biedt op de persoon toegesneden informatie en data. Deze sites maken onderdeel uit van de verschillende e-Overheidstrategieën. In de e-Overheidstrategieën is veel aandacht voor de beveiliging (authenticatie) en toegang tot de sites en de kwaliteit van de (basis)gegevens. Slowakije[3] lijkt op dit moment vooral bezig met het implementeren van de voor de e-Overheidsdiensten benodigde infrastructuur. Het versterken van burgerrechten lijkt geen duidelijke plaats in te nemen in de e-Overheidsstrategie van Slowakije. In Duitsland[4], daarentegen, wordt in de e-Overheidsstrategie expliciet melding gemaakt van doelen en acties op het gebied van vertrouwen van burgers in de e-overheid, in de vorm van transparantie, gegevensbescherming en –zekerheid. Hoe dat concreet uitgewerkt wordt, is niet duidelijk geworden uit de grove scan. De Duitse site Bund.de lijkt geen gepersonaliseerd deel te kennen.

De sites van Denemarken, Estland en Frankrijk bieden vergelijkbare functies als de huidige Nederlandse site MijnOverheid. De sites bieden met name inzage in gegevens om op die manier de transparantie en legitimiteit van de overheid te versterken. Via de Deense site hebben burgers bijvoorbeeld toegang tot belasting-, economische, woon- en civiele gegevens.

Estland is, om verschillende redenen, een interessant voorbeeld. Burgers hebben, net als in Frankrijk en Denemarken, toegang tot de site via een e-mailadres van de overheid (code@eestie.ee) dat speciaal bedoeld is voor overheid-burgercontact. Anders dan in Nederland, is deze site er niet alleen voor burgers, maar ook voor ondernemers en ambtenaren. Verder biedt de site verschillende functionaliteiten die de Nederlandse site niet kent. Er kunnen transacties met overheden worden gedaan en documenten kunnen digitaal ondertekend worden.

Frankrijk is een interessant voorbeeld als het gaat om ‘de module met contactgegevens’. Sinds april 2010 kent de Franse site een service waarmee gebruikers met één klik hun contactgegevens voor twaalf overheidsorganisaties en drie nutsbedrijven kunnen wijzigen. Hiernaast kent Denemarken het concept NemKonto (easy account). De overheid maakt hiervan gebruik voor financiële interactie met de burger. De burger kan zelf een van zijn rekeningen kiezen als NemKonto.

Kortom, ook internationaal zijn er vergelijkbare ontwikkelingen als in Nederland. Elektronisch verkeer tussen burger en overheid wordt geregeld en er is steeds meer aandacht voor transparantie. De sites van Estland en Frankrijk kennen functionaliteiten – waaronder een module met contactgegevens – die de huidige Nederlandse site niet kent. Om deze reden is het raadzaam hier in het vervolg nader naar te kijken en eventueel een voorbeeld aan te nemen voor de eventuele doorontwikkeling van de Nederlandse site.

---

[2] Voor Denemarken is dit borger.dk; voor Estland eesti.ee en voor Frankrijk MonServicePublic.fr.
[3] Portal.gov.sk.
[4] Bund.de.

5.4 Algemene bevindingen

Tijdens de gevoerde gesprekken komen niet alleen de losse functionaliteiten aan de orde, maar geven de gesprekspartners ook meer algemene opvattingen en inzichten aan.

5.4.1 Inzage op het geheel nodig: gegevens, gegevensstromen en processen in samenhang

In de kabinetsreactie worden inzage in de gegevens die de overheid over de burger heeft en inzage in het gegevensverkeer nog als twee aparte functionaliteiten genoemd. Een aantal gesprekspartners geeft aan dat apart inzage bieden in gegevens en in gegevensstromen naar hun verwachting aan burgers niet het gewenste inzicht zal geven. Gegevens en gegevensverkeer krijgen betekenis in het kader van de processen die de organisaties uitvoeren en de bewerkingen die de gegevens ondergaan. Zo heeft het UWV bijvoorbeeld het aantal kinderen dat iemand heeft nodig om het aantal uitkeringsdagen in het kader van de werkloosheidswetgeving te kunnen bepalen. Zonder inzicht in het gebruik van de gegevens roept inzage in de gegevens en gegevensstromen onbegrip en vragen op. Een belangrijke functie van MijnOverheid kan zijn om een zo begrijpelijk mogelijk overzicht op het totaal te bieden. Het idee om bij besluiten van de overheid de kerngegevens inzichtelijk te maken sluit hierbij aan.

5.4.2 MijnOverheid als hulpmiddel en in relatie met MijnDomeinen

Naast MijnOverheid hebben een aantal uitvoeringsinstellingen ook een “MijnDomein”: MijnGemeente, MijnSVB, en andere MijnDomeinen. Er tekent zich inmiddels een consensus af dat MijnOverheid de functie zou moeten hebben om het totaaloverzicht te bieden. Wanneer een burger behoefte heeft aan meer detail dient hij zich daarvoor te wenden tot de organisatie die verantwoordelijk is voor de gegevens en die hij via MijnOverheid heeft ontsloten. De wenselijke situatie is dan dat de burger op het MijnDomein meer detail kan vinden en de verantwoordelijke organisatie ook kan benaderen. Op het MijnDomein kunnen ook aanvragen voor diensten gedaan worden of gebruik gemaakt worden van digitale dienstverlening.

De functie van MijnOverheid wordt dan beperkter en duidelijker: het bieden van overzicht. Dat overzicht heeft (zoals eerder aangegeven) de meeste toegevoegde waarde wanneer gegevens, gegevensstromen en de processen waarin ze gebruikt worden in samenhang gepresenteerd worden. Qua detailniveau wordt gedetailleerd gepersonaliseerd niveau alleen haalbaar geacht voor basisregistraties en organisaties als BKWI die gegevensverkeer faciliteren. Gewoonlijk zal het kerngegevensniveau het hoogst haalbare zijn: voor sommige organisaties binnen enkele jaren, voor andere pas op langere termijn. Naar de inschatting van onze gesprekspartners is dat ook voldoende om aan de behoeften van burgers aan overzicht te voldoen.

De consequentie van deze benadering is dat de burgers met vele MijnDomeinen te maken gaat krijgen. Single sign on om te voorkomen dat burgers steeds opnieuw moeten inloggen, staat op de beleidsagenda en is mogelijk via de nieuwste versie van DigiD.

5.4.3 Geen generieke systeemoplossingen voor specifieke (gegevens)problemen

Met name in de verkennende gesprekken bij de start van het onderzoek is enkele malen het uitgangspunt ter tafel gekomen dat er geen generieke systeemoplossingen ingezet moeten worden om specifieke

(gegevens)problemen op te lossen. Bepleit werd om dat als algemeen geldend uitgangspunt te hanteren. Daarbij werden twee concrete voorbeelden genoemd.

Het eerste voorbeeld betreft de gedachte dat gegevens, gegevensstromen en processen binnen de dienstverlening op individueel detailniveau inzichtelijk gemaakt moeten worden om burgers in staat te stellen zelf te constateren waar fouten worden gemaakt en die vervolgens op te lossen. In paragraaf 5.1.1. is uitgebreid beschreven wat daarvan de consequenties zijn en zijn ook een aantal specifieke maatregelen genoemd om de problemen wel op te lossen. Ook werken de organisaties aan het verbeteren van de gegevenskwaliteit om op die manier problemen van burgers te voorkomen en op te lossen.

Het tweede voorbeeld betreft identiteitsfraude. De WRR geeft voorbeelden van een aantal schrijnende gevallen van burgers die in de knel komen door fouten in de gegevenshuishouding van de overheid. Vaak is daarbij sprake van identiteitsfraude. Het is ondoenlijk om alle procedures en processen van de overheid “identiteitsfraudeproof” te maken: een generieke systeemoplossing is niet haalbaar. Tegelijk is het onaanvaardbaar dat burgers die met identiteitsfraude worden geconfronteerd daardoor in zeer ernstige problemen raken. Waar een generieke oplossing niet haalbaar is, dient wel adequate specifieke ondersteuning aan burgers geboden te worden. Het “meldpunt identiteitsfraude” is daarvoor in het leven geroepen.

5.4.4 Profiling

De WRR plaatst een waarschuwingsvlag bij informatieprocessen waarin profielen van burgers worden opgesteld en worden gebruikt om (proactief) actie te ondernemen richting burgers. Dit onderzoek is gericht op vernetwerking, omdat dit in de dienstverlening op grote schaal voorkomt en profielen in mindere mate gebruikt worden. Enkele gesprekspartners wezen erop dat vernetwerking en profilering in informatiekundige zin heel verschillende processen zijn.

In de dienstverlening zoals die is onderzocht is er sprake van uitvoeringsinstelling die op basis van een aantal gegevens een op de wet gebaseerde beslissing neemt over een individu. De instelling moet aan het individu kunnen uitleggen hoe de beslisregels en de gegevens in een oorzaak-gevolgrelatie hebben geleid tot het genomen besluit. Hier ligt voor de burger het aangrijpingspunt om bezwaar en beroep aan te tekenen en voor de rechter om daarover te oordelen.

Profiling werkt anders. Zeer omvangrijke datasets worden bewerkt met wiskundige technieken die correlaties aangeven en voorspellingen doen zonder dat er sprake is van duidelijk aanwijsbare oorzaak-gevolgrelaties. Inzage op de gegevens en de mogelijkheid bieden om correctieverzoeken te doen kunnen bij vernetwerking bijdragen aan het oplossen van problemen, maar lijken bij profilering door het ontbreken van de oorzaak-gevolgrelatie niet of nauwelijks effectief. De conclusie is dat hier een beleidsvraagstuk aan de orde is dat afwijkt van vernetwerking en dat nog niet prominent op de beleidsagenda staat. Dit vraagstuk is ook aan de orde in de dienstverlening. In de controleprocessen binnen de dienstverlening wordt nu al op relatief bescheiden schaal gebruik gemaakt van categorisering en risicoprofielen. De technische mogelijkheden om dat op grotere schaal te doen en daarbij gebruik te maken van gegevens van buiten de eigen organisatie nemen momenteel snel toe. Dient de burger hier ook proactief via MijnOverheid of MijnDomeinen over te worden geïnformeerd? Deze discussie wordt nog maar op heel beperkte schaal gevoerd.

5.4.5 Controle en zorg

Dienstverleningsprocessen hebben deels andere karakteristieken dan processen in de domeinen van controle en opsporing en van zorg. De manier waarop bij opsporing gegevens verzameld worden is heel anders dan in de dienstverlening en dat geldt ook voor de mogelijkheden die bestaan om gegevens tijdens het proces met de betrokken burger te delen. Gegevens in de zorg hebben een heel persoonlijk, gevoelig karakter, waardoor vaker dan in de dienstverlening het wenselijk zal zijn om een patiënt of cliënt vooraf toestemming te laten geven voor een verstrekking van gegevens. Door deze verschillen in de informatieprocessen zijn de bevindingen die gelden voor de dienstverlening niet zonder meer toepasbaar binnen de opsporing, de zorg en de controleprocessen die onderdeel zijn van de dienstverlening. Een gesprekspartner uit het zorgdomein gaf aan dat de overheid er slim aan zou doen om vooraf na te denken over wat de verschillende functionaliteiten voor andere domeinen zoals zorg betekenen.

5.5 Verplichtbaarheid MijnOverheid

Naast de zes functionaliteiten om de informatiepositie van de burger via MijnOverheid te versterken is ook gevraagd onderzoek te doen naar de ‘verplichtbaarheid’ van MijnOverheid. De vraag of het mogelijk is overheidsorganisaties te verplichten om op MijnOverheid aan te sluiten is een governancevraagstuk. Binnen de e-overheid worden wettelijke verplichtingen gehanteerd (bijvoorbeeld bij het gebruik van de basisregistraties) of bestuurlijke afspraken zoals in het iNUP zijn vastgelegd. In deze paragraaf worden de bestaande verplichtingen beschreven, wordt verkend welke mogelijkheden er zijn om deze aan te scherpen en welk effect daarvan verwacht mag worden op het gebruik van MijnOverheid.

5.5.1 Huidige verplichtingen

MijnOverheid is onderdeel van de elektronische overheid. De dagelijkse sturing is in handen van het dagelijks bestuur van de bestuurlijke regiegroep e-Overheid en dienstverlening en de uitvoering vindt plaats onder verantwoordelijkheid van de programmaraad e-Overheid voor burgers. Het “werkprogramma” tot 2015 is het iNUP, daarin zijn bestuurlijke afspraken gemaakt en prestatie-eisen geformuleerd waar de partijen zich aan gecommitteerd hebben. Voor MijnOverheid geldt geen wettelijke verplichting om die in stand te houden. In het iNUP zijn betreffende MijnOverheid prestatieafspraken gemaakt over de onderdelen lopende zaken en de berichtenbox, maar niet over persoonlijke gegevens, de functionaliteit die in dit onderzoek centraal staat. Er is dus geen bestuurlijke afspraak om gebruik te maken van MijnOverheid voor het bieden van inzage, verzoeken om correctie en verwijderen. Er is evenmin een ambtelijke afspraak gemaakt in de Interdepartementale Commissie Bedrijfsvoering Rijksdienst over verplicht gebruik van de functie persoonlijke gegevens. Ook de Wbp leidt niet tot een verplichting om MijnOverheid te gebruiken. De uitvoering van de wet wordt wel ondersteund wanneer inzage, vragen om correctie en verwijderen voor burgers eenvoudiger worden door MijnOverheid. Kortom, zowel bestuurlijk als juridisch bestaat er op dit moment op geen enkele manier een verplichting om de functie “persoonlijke gegevens” van MijnOverheid te gebruiken.

5.5.2 Toekomstige verplichtingen

Bij de geïnterviewden is brede overeenstemming over dat de ambities van het kabinet om de informatiepositie van burgers substantieel te verbeteren alleen tot stand komen wanneer dat verplicht wordt gesteld. De ervaring met vrijblijvende aanbevelingen is dat ze maar heel beperkt effect hebben. In wezen bestaat die situatie nu

voor de functie persoonlijke gegevens in MijnOverheid. Er zijn partijen die vrijwillig aansluiten, maar dat is mondjesmaat. Een verplichting is ook nodig om burgers een compleet, maar ook een qua vormgeving uniform en samenhangend overzicht te kunnen bieden.

Een wettelijke verplichting is daarbij geen garantie voor succes, zelfs niet wanneer er een sanctie staat op het niet nakomen van de wettelijke plicht. Er zijn partijen binnen de overheid die een kosten-batenafweging maken en die de mogelijkheid openhouden dat ze liever een boete betalen dan de verplichting na te komen. Belangrijk voor succes is, dat de verplichting praktisch uitvoerbaar en geprioriteerd is. Beter dan het eenzijdig opleggen van een verplichting is het wederzijds aangaan ervan. Dat ziet er bijvoorbeeld als volgt uit. De leverancier van de centrale faciliteit (MijnOverheid) neemt op zich om tijdig een voorziening voor productie gereed te maken en beschikbaar te stellen. De bruikbaarheid van de voorziening is vooraf getoetst met een uitvoeringstoets of een impactanalyse. Er is voor de gebruikers een businesscase die de meerwaarde voor bestuurders aantoont. De planning die gebruikers van de faciliteit moeten halen is realistisch en afgestemd met de planning van andere voorzieningen. Op deze basis kan een bestuurlijke afspraak gemaakt worden in de Bestuurlijke Regiegroep. Men geeft aan dat een bestuurlijke afspraak, volgend op het geschetste voorbereidingstraject, de beste kans van slagen heeft. Een wettelijke verplichting kan in dat kader de verplichting aanscherpen en bijdragen aan succesvolle implementatie.

Verschillende partijen geven aan dat het naar hun mening niet mogelijk is om op korte termijn een verplichting om de functie “persoonlijke gegevens” en de additionele functionaliteiten te gaan gebruiken en toe te voegen aan de iNUP-prestatieafspraken. Daar is de impact in veel gevallen te groot voor. De bestaande iNUP-prestatieafspraken vragen al een grote inspanning. Implementatie van deze voorzieningen is in een aantal gevallen bovendien randvoorwaardelijk voor het gebruiken van “persoonlijke gegevens”.

De bestuurlijke aansturing van MijnOverheid is complex. Het onderdeel persoonlijke gegevens is nog in ontwikkeling, de berichtenbox is in beheer bij Logius. Naast het verantwoordelijke beleidsdepartement BZK zijn ook de Programmaraad e-Overheid voor burgers, het Bestuurlijk Overleg MijnOverheid en de Programmaraad van Logius bij de aansturing betrokken. Bovendien is de bestuurlijke context aan het veranderen. Nu steeds meer onderdelen van de e-Overheid in de beheerfase komen is bij BZK de vraag aan de orde hoe lang de bestaande programmasturing op het iNUP nog adequaat blijft. Om tot voldoende bestuurlijk draagvlak voor de implementatie van de nieuwe functionaliteiten te komen is het zaak de Programmaraad en het Bestuurlijk Overleg vanaf het begin bij de voorbereiding van de besluitvorming te betrekken.

5.6 Invulling artikel 18 Wabb

In deze paragraaf staat de vraag centraal of de minister via MijnOverheid invulling kan geven aan zijn verplichting op grond van artikel 18 Wabb tot “de instandhouding van een voorziening met behulp waarvan voor een ieder algemene informatie beschikbaar wordt gesteld met betrekking tot a. het gebruik van burgerservicenummers en b. de gegevensverwerkingen van gebruikers, waarbij burgerservicenummers worden gebruikt”.

Om aan deze verplichting te voldoen heeft de minister de website www.burgerservicenummer.nl ingericht. Het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) voert het beheer over deze website. De website geeft informatie op het algemene niveau. Op dit moment heeft de site niet de functie die het zou moeten hebben. Het kost moeite om uitvoerders te bewegen om de site bij te houden en uit analyse

van de gegevensstatistieken blijkt dat de site door burgers nauwelijks geraadpleegd wordt. Uitvoerders hebben daardoor het beeld dat ze uitvoering geven aan een verplichting die nauwelijks enig voordeel oplevert.

We interpreteren de onderzoeksvraag zo, dat voorgesteld wordt om de bestaande verplichting in stand te houden en de bestaande site www.burgerservicenummer.nl te migreren naar MijnOverheid. Het bestaande MijnOverheid vult dan meteen www.burgerservicenummer.nl aan. Weliswaar ontsluiten nog lang niet alle organisaties hun gegevens via MijnOverheid, maar de organisaties die dat wel doen bieden een gepersonaliseerde inzage en gedetailleerder inzicht in de geregistreerde gegevens. De bevindingen in het burgerperspectief maken duidelijk dat de burgers hier sterk behoefte aan hebben. MijnOverheid sluit daardoor beter aan bij de behoeften van burgers zoals die in het burgerperspectief naar voren zijn gekomen. De tekst van de wet impliceert niet dat de minister beslist een aparte voorziening in stand moet houden. Dat betekent dat het mogelijk is om via MijnOverheid inzage te geven in gegevens en in gegevensstromen en zo invulling te geven aan de wettelijke verplichting die de minister heeft. Een mogelijk voordeel om het via MijnOverheid te laten verlopen is dat de kans op een goed functionerende en up-to-date site groter is dan momenteel het geval is.

5.7 Samenvatting informatiekundig perspectief

In het (landelijke) informatiebeleid is de afgelopen jaren weinig expliciet aandacht gegeven aan het versterken van de informatiepositie van burgers. Dit perspectief, geconcretiseerd in mogelijke nieuwe functionaliteiten van MijnOverheid, werd door een aantal respondenten ervaren als een geheel nieuwe invalshoek waar men ter plekke een oordeel over moest vormen. Mede daardoor konden zij alleen heel globaal uitspraken doen over de informatiekundige, technische, organisatorische en financiële consequenties van de voorgestelde functionaliteiten.

De consequenties die het bieden van inzage in gegevens heeft, verschilt sterk met het detailniveau waarop inzage geboden dient te worden. Om de burger in staat te stellen zelf vast te stellen waar foute gegevens zijn gebruikt, is inzage op een gedetailleerd gepersonaliseerd niveau nodig. Dit vergt bij de uitvoeringsorganisaties ingrijpende organisatorische en technische aanpassingen met daarmee samenhangende prohibitief hoge kosten. Inzage bieden in de kerngegevens waarop een besluit is gebaseerd sluit aan bij de transactiegerichte of zaakgerichte benadering die in het beleid (iNUP) en door partijen zelf wordt gehanteerd. De wenselijkheid en haalbaarheid verschilt per organisatie. De ene organisatie is veel verder met de invoering daarvan dan de andere. Ook zal nader moeten worden onderzocht wat wordt verstaan onder kerngegevens. Inzage bieden in de gebruikte gegevens is verder in de ogen van de uitvoeringsorganisaties onvoldoende om burgers in staat te stellen mogelijke problemen die ze ondervinden zelf op te lossen. De overheid zal in hun ogen daartoe met een vorm van accountmanagement en aangescherpte verantwoordelijkheden de burgers dienen te ondersteunen.

Inzage bieden in gegevensstromen lijkt voor basisregistraties en voor organisaties die gegevensverkeer faciliteren (zoals bijvoorbeeld BKWI) haalbaar te zijn. De gegevens zijn beschikbaar en de benodigde inspanningen hebben betrekking op het ontsluiten via MijnOverheid. Uitvoeringsinstellingen en mede-overheden zijn echter in het geheel niet bezig met het bieden van inzage in het gegevensverkeer en zullen daarvoor verstrekkende, complexe en daardoor prohibitief dure aanpassingen moeten doorvoeren.

Naar de mening van de respondenten dient een burger op een eenvoudige wijze een correctieverzoek te kunnen indienen op de gegevens die getoond worden in MijnOverheid, dan wel in de MijnDomeinen door de uitvoeringsorganisaties zelf. Dit correctieverzoek zou (wellicht met MijnOverheid als doorgeefluik) bij de

betreffende dienstverlener ingediend moeten worden. Daarbij is het ook zaak geen valse verwachtingen te wekken: bijna altijd dient de uitvoeringsorganisatie bestaande regels te volgen bij het vaststellen van gegevens en kan niet zondermeer tegemoet gekomen worden aan het verzoek van de burger.

In de bestaande dienstverleningspraktijk is er nauwelijks sprake van enige sense of urgency als het om verwijderen van gegevens gaat. Men ondervindt zelf nauwelijks problemen en wijst erop dat voorbeelden om het belang van tijdige verwijdering van gegevens te adstrueren meestal op de domeinen zorg en controle betrekking hebben. Gericht aanpakken van de wel bestaande problemen in de dienstverlening heeft de voorkeur boven een generieke aanpak.

De mogelijke functionaliteit van een module met contactgegevens wordt over het algemeen benaderd vanuit het perspectief en het belang van de overheid zelf. Er zijn bijvoorbeeld besparingen mogelijk wanneer de burger verplicht is één rekeningnummer in haar relatie met de overheid te gebruiken. Verondersteld wordt dat de burger het ook prettig zal vinden om één keer op één plaats contactgegevens te verstrekken die vervolgens door de hele overheid worden gebruikt.

Op de mogelijke functionaliteit actief delen van gegevens wordt soms positief, soms negatief gereageerd. In ieder geval is het zaak het onderscheid tussen publiek en privaat gebruik van gegevens scherp te houden. Sommige uitvoeringsinstellingen en mede-overheidsorganisaties veronderstellen dat burgers voordelen van de functionaliteit zullen hebben, anderen vrezen dat hun informatiepositie er eerder door zal verzwakken.

Om te bereiken dat de nieuwe functionaliteiten gerealiseerd worden door *alle* uitvoeringsinstellingen – via MijnOverheid en/of de MijnDomeinen -en de decentrale overheden is een (wettelijke) verplichting noodzakelijk. Vooraf dient in het bestuurlijke besluitvormingsproces geborgd te worden dat de verplichting ook praktisch uitvoerbaar is.

Het is mogelijk en het heeft voordelen om via MijnOverheid te voldoen aan de verplichting van de staat om het gebruik van het burgerservicenummer inzichtelijk te maken (artikel 18 Wabb).

6 Factsheets per functionaliteit

In onderstaande factsheets staan de voorgaande hoofdstukken kort en overzichtelijk samengevat. Bij de functionaliteiten inzage in gegevens, inzage in gegevensstromen, verzoeken tot correctie en het vermelden van de verwijderingstermijn is onderscheid gemaakt in de verschillende detailniveaus.

6.1 Inzage in gegevens

Inzage in gegevens			
Omschrijving	De kabinetsreactie op het WRR-rapport gaat uit van het voor de burgers elektronisch inzichtelijk maken welke gegevens overheidsorganisaties van burgers gebruiken, zodat de burger in staat wordt gesteld daar toezicht op te houden en zelf regie te voeren. Inzage zou ook moeten gelden voor dossiers waarin gegevens van meerdere instellingen worden samengebracht, inclusief de herkomst van de gegevens en gegevens die gebruikt zijn voor pro-actief handelen.		
Perspectief	Burger	Juridisch	Informatiekundig
Algemeen niveau	+ Burgers vinden het handig om te zien bij wie ze staan geregistreerd.	+ In artikel 18 van de Wabb staat een verplichting om op algemeen niveau inzicht te verschaffen.	+ BSN.nl biedt dit overzicht (niet gepersonaliseerd).
Kerngegevens	+++ Burger wil zien wat de overheid van hem weet vanwege a) inzicht, b) controle en c) geheugensteun. Dit geldt in het bijzonder voor burgers met een (gegevens)probleem. Zij willen weten wat er fout staat.	+/- Artikel 35 Wbp geeft de burger recht op een volledig overzicht op algemeen niveau, aangevuld met gepersonaliseerde gegevens op kerngegevensniveau. De verantwoordelijke mag gemotiveerd afwijken. Er geldt *geen* verplichting om actief inzage te verstrekken aan burgers.	+/- Een aantal organisaties heeft de kerngegevens al via MijnOverheid inzichtelijk gemaakt. Voor andere organisaties geldt dat zij de kerngegevens hebben opgeslagen; publicatie daarvan is een informatiekundige drempel.
Gedetailleerd gepersonaliseerd niveau	- De gemiddelde burger zou dit niet begrijpen; het is een niveau te diep.	+/- Indien de burger op gedetailleerd niveau inzage wenst dient dit op grond van jurisprudentie gehonoreerd te worden.	--- Dit niveau zit niet in de architectuur en organisatiefilosofie. Het gaat waarschijnlijk slechts om enkele gevallen die individueel afgehandeld kunnen worden.

Conclusie	Inzage in persoonlijke kerngegevens is van belang voor de informatiepositie van burgers. Burgers vinden een dergelijke functionaliteit via MijnOverheid wenselijk, c.q. noodzakelijk in geval van problemen. De Wbp biedt het recht op inzage, maar geen verplichting aan overheidsorganisaties om dit actief te doen. Het ontsluiten van kerngegevens heeft voor diverse organisaties forse informatiekundige consequenties. Inzage in een gedetailleerd persoonlijk niveau is slechts in enkele individuele situaties nodig, daar kunnen en hoeven op korte termijn geen grote informatiekundige aanpassingen voor te worden gedaan.

6.2 Inzage in gegevensverkeer

Inzage in gegevensverkeer			
Omschrijving	Inzage in gegevensverkeer biedt bijvoorbeeld inzicht in gegevensuitwisselingen: • Vanuit een basisregistratie naar uitvoeringsinstellingen en andere (basis)registraties. • Tussen uitvoeringsinstellingen die gegevens bij hun collega's opvragen. • Binnen ketens waarin uitvoeringsinstellingen samenwerken via elektronische dossiers of portalen.		
Perspectief	Burger	Juridisch	Informatiekundig
Algemeen niveau	+ Burger wil weten welke organisaties wat over hem (mogen) uitwisselen. Dit kan ook door een mouse-over aan te brengen op persoonlijke gegevens.	+ In artikel 18 van de Wabb staat een verplichting om op algemeen niveau inzicht te verschaffen.	+ BSN.nl is er al. Via autorisatietabellen van basisregistraties zou dit deels ook op persoonlijk niveau inzichtelijk kunnen worden gemaakt.
Kerngegevens	+++ Burger wil zien wat de overheid uitwisselt vanwege a) inzicht, b) controle, c) geheugensteun en d) kwaliteitsimpuls voor de organisatie. Dit geldt in het bijzonder voor burgers met een (gegevens)probleem. Zij willen weten wat er fout is en zullen dit zeker raadplegen.	+/- Artikel 35 Wbp geeft de burger recht op een volledig overzicht op algemeen niveau, aangevuld met gepersonaliseerde gegevens op kerngegevensniveau. De verantwoordelijke mag gemotiveerd afwijken. Er geldt *geen* verplichting om actief inzage te verstrekken aan burgers.	-- Dit niveau zit niet in het beleid van uitvoeringsinstellingen en mede-overheden. Consequenties zijn niet te kwantificeren, zullen fors zijn.
Gedetailleerd gepersonaliseerd niveau	-- Burger heeft hier geen behoefte aan, mits de kerngegevens kloppen.	+/- Indien de burger op gedetailleerd niveau inzage wenst dient dit op grond van jurisprudentie gehonoreerd te worden.	-- Dit niveau zit niet in de architectuur en organisatiefilosofie. Kosten zijn prohibitief hoog.
Conclusie	Voor burgers is inzage in gegevensverkeer van kerngegevens wenselijk. In het bijzonder in geval van (gegevens)problemen. Wbp biedt het recht op inzage in gegevensverkeer (per organisatie), maar geen verplichting aan overheidsorganisaties om dit actief te doen. Het ontsluiten van gegevensverkeer heeft voor organisaties forse informatiekundige consequenties. Inzage in een gedetailleerd persoonlijk zit niet in de organisatiefilosofie en is prohibitief duur.		

6.3 Verzoeken om correctie

Verzoeken om correctie			
Omschrijving	De mogelijkheid om náást het indienen van correctieverzoeken bij de afzonderlijke gegevenshouders, via een uitbreiding van MijnOverheid een gemeenschappelijke correctiefaciliteit te realiseren waarmee de burger bij alle partijen tegelijk een verzoek indienen om de fout en de gevolgen daarvan recht te zetten.		
Perspectief	Burger	Juridisch	Informatiekundig
Algemeen niveau	Nvt	Nvt	Nvt
Kerngegevens	+++ Burgers willen dit graag; met name van belang voor burgers die (gegevens)problemen hebben en gegevens daadwerkelijk willen corrigeren.	+ Juridische basis in artikel 36 Wbp; verzoeken tot correctie mogen ook digitaal. De Wbp heeft betrekking op enkelvoudig correctieverzoek per gegevensbeheerder. Voor dit niveau geldt daarnaast sectorwetgeving.	+ Indien gegevens op dit niveau ontsloten zijn, zijn *enkelvoudige* verzoeken tot correctie haalbaar. Een *gemeenschappelijke* correctiefaciliteit vereist forse investeringen. Vanuit zaaksystemen kan statusinformatie beschikbaar worden.
Gedetailleerd gepersonaliseerd niveau	-- Niet noodzakelijk en gaat te ver.	- In de Wbp wordt niet gesproken over het detailniveau van gegevens.	-- Dit niveau zit niet in de architectuur en organisatiefilosofie.
Conclusie	Burgers vinden dit zeer wenselijk. De Wbp heeft alleen betrekking op enkelvoudig correctieverzoek per gegevensbeheerder. Een gemeenschappelijke correctiefaciliteit vereist forse investeringen. Zowel burgers als organisaties geven aan dat het indienen van een verzoek tot correctie niet het middel is waarmee (gegevens) problemen opgelost kunnen worden. De afhandeling van een verzoek tot correctie kan moeizaam verlopen. Als eerste moet duidelijk zijn wie de verantwoordelijke organisatie is en daarna moeten de gegevens, indien terecht, ook daadwerkelijk aangepast worden, ook in andere registraties. Gesuggereerd wordt dat een accountmanager en/of een gegevensautoriteit hierbij behulpzaam kan zijn.		

6.4 Vermelden verwijderingstermijn

Vermelden verwijderingstermijn			
Omschrijving	Deze functionaliteit houdt in dat, bij gegevens waarvoor een bewaartermijn geldt en die via MijnOverheid inzichtelijk gemaakt worden, vermeld wordt wanneer het gegeven moeten worden gewist.		
Perspectief	Burger	Juridisch	Informatiekundig
Algemeen niveau	+ Geeft overzicht.	+ De Wbp stelt in algemene zin dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel van de verwerking. Specifieke bewaartermijnen staan in specifieke (sectorale) wetgeving.	+ Associatie met Archiefwet, waarbij gegevens na een bepaalde termijn niet meer bewaard hoeven te worden. Vooral in zorg- en controledomein van belang, gezien burger daar het meeste last kan ondervinden.
Kerngegevens	++ Geeft inzicht en biedt daarmee mogelijk een handelingsoptie.	+ De Wbp stelt in algemene zin dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel van de verwerking. Specifieke bewaartermijnen staan in specifieke (sectorale) wetgeving.	+ Als kerngegevens ontsloten worden, dan is het relatief eenvoudig de verwijderingstermijn erbij te benoemen. Daadwerkelijk verwijderen uit alle databases is complex.
Gedetailleerd gepersonaliseerd niveau	-- Niet noodzakelijk.	+ De Wbp stelt in algemene zin dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel van de verwerking. Specifieke bewaartermijnen staan in specifieke (sectorale) wetgeving.	- Omdat inzage bieden prohibitief duur is niet van toepassing.
Conclusie	Deze functionaliteit zou burgers meerwaarde bieden en versterkt hun informatiepositie. Wbp schrijft geen actieve publicatie van verwijderingstermijn voor. Informatiekundige consequenties zijn beperkt indien de kerngegevens reeds ontsloten zijn. Het inzage geven in de verwijderingstermijn van gegevens is iets anders dan het recht van de burger om te verzoeken gegevens te verwijderen. Voor burgers is met name het daadwerkelijk verwijderen - of de mogelijkheid hebben daarvoor een verzoek in te dienen – van belang. Voor organisaties geldt dat het echt helemaal verwijderen van alle betreffende persoonsgegevens vaak complex is.		

6.5 Module met contactgegevens

Module met contactgegevens			
Omschrijving	De mogelijkheid om in MijnOverheid een module met contactgegevens op te nemen met bijvoorbeeld bankrekeningnummer, email, mobiele telefoon en tijdelijk correspondentieadres. Over doel en inrichting en invulling van een dergelijke module bestaan verschillende beelden.		
Perspectief	Burger	Juridisch	Informatiekundig
Bankrekening Nummer	- Burger wil meerdere rekeningnummers kunnen gebruiken vanwege eigen administratieve proces	- Geen juridisch basis.	+++ Het gebruik van één bankrekeningnummer levert besparingen op voor de overheid.
E-mail adres	+/- Sommige burgers geven aan dat e-mailadres handig kan zijn; het bespaart papier- en verzendkosten. Andere burgers ontvangen liever een brief van de overheid.	- Geen juridische basis. DigiD en de berichtenbox eisen e-mailadres.	+ Als servicegegeven is e-mailadres gewenst; het levert ook een besparing op (mails sturen i.p.v. brieven). De berichtenbox vormt een alternatief op e-mailcontact tussen overheidsorganisaties en burgers. Via de berichtenbox wordt e-mailverkeer ontmoedigd.
Mobiel telefoon-nummer	-- Mobiele telefoon is voor vrienden en zaken, maar niet voor de overheid.	- Geen juridische basis DigiD-niveau midden eist een mobiel telefoonnummer.	+ Vanuit serviceconcept gewenst.
Alternatief correspondentie-adres	+/- Roept bij burgers geen reactie op.	- Geen juridische basis.	+/- Zou overbodig worden als berichtenbox in grotere mate gebruikt gaat worden.
Conclusie	Er zijn verschillende beelden en verwachtingen. Als er een module met contactgegevens komt, zouden burgers zelf hun eigen gegevens willen beheren. Bij organisaties bestaan hierbij verschillende beelden. Men redeneert overwegend vanuit de eigen behoeften en veronderstelt dat de burger het prettig zal vinden om één keer op één plaats contactgegevens te verstrekken.		

6.6 Actief delen van gegevens

Actief delen van gegevens			
Omschrijving	Mogelijkheid om eigen gegevens op eigen verzoek actief te delen met derde partijen, zowel publiek als privaat.		
Perspectief	Burger	Juridisch	Informatiekundig
	+/- De overheid moet niet groter gemaakt worden dan hij is; onderscheid publieke en private domein moet niet doorbroken worden. Als er voor wordt gekozen, dan willen burgers zelf kunnen bepalen met wie wel en geen gegevens worden gedeeld. Eenmanszaken staan hier neutraler tegenover.	+/- De Awb stelt dat papier en elektronisch verkeer nevengeschikt zijn aan elkaar. Doelbindingsbepalingen in de Wbp	+/- Op conceptueel niveau wordt erover nagedacht, maar de betekenis voor ICT en architectuur is onduidelijk.
Conclusie	Er bestaan verschillende beelden over deze functionaliteit. Deze verschillen van eenmalig actief delen van eigen gegevens, tot het geven van toestemming voor het delen van gegevens in algemene zin. Vanuit alle drie de perspectieven lijkt deze functionaliteit als zodanig niet direct bij te dragen aan de informatiepositie van burgers.		

7 Conclusies en beantwoording onderzoeksvragen

7.1 Beantwoording van de onderzoeksvragen

De hoofdvraag van dit onderzoek is of de informatiepositie van de burger versterkt kan worden door extra functionaliteiten aan de site MijnOverheid toe te voegen. Deze vraag is vanuit het perspectief van de burger, een juridisch en een informatiekundig perspectief onderzocht.

7.1.1 Beantwoording onderzoeksvragen

1. Welke additionele functionaliteiten van MijnOverheid kunnen bijdragen aan het versterken van de informatiepositie van de burger?

Vanuit elk van de gehanteerde perspectieven (burger, juridisch en informatiekundig) dragen vier onderzochte mogelijke functionaliteiten van MijnOverheid bij aan de versterking van de informatiepositie van de burger. Het gaat dan om *'inzage in gegevens'*, *'inzage in gegevensverkeer'*, *'verzoeken om correctie'* en *'het vermelden van de verwijderingstermijn'*. De genoemde functionaliteiten moeten in onderlinge samenhang gezien en geprioriteerd worden. Zonder inzage in gegevens en gegevensverkeer, is het indienen van een correctieverzoek of het vermelden van de verwijderingstermijn niet mogelijk.

Als het sec om inzage en transparantie gaat, dan volstaat hierbij het presenteren van de door overheidsorganisaties gehanteerde kerngegevens op persoonsniveau. De huidige Wbp biedt hiervoor de wettelijk basis, zij het dat hierin geen verplichting voor overheidsorganisaties zit om gegevens actief en voor alle burgers inzichtelijk te maken.

Gaat het echter om het oplossen van (gegevens)problemen, dan is een gedetailleerder inzicht nodig in de onderliggende gegevens en gegevensstromen waarop de kerngegevens gebaseerd zijn. Dit laatste is echter vanuit het informatiekundig perspectief buitengewoon complex, kostbaar en op korte termijn niet haalbaar. Bovendien overheerst bij de respondenten de mening dat de overheid zijn eigen problemen moet oplossen en het probleem niet bij de burger moet neerleggen. Een eventuele accountmanager kan de burger hierbij helpen en een gegevensautoriteit kan organisaties die hun verantwoordelijkheid niet waarmaken aanspreken.

Burgers geven aan dat zij nog een functionaliteit aan MijnOverheid zouden willen toevoegen, namelijk de mogelijkheid om gegevensuitwisselingen een halt toe te kunnen roepen of vooraf toestemming te geven voor een gegevensuitwisseling, zoals dat ook in de zorg meer gebruikelijk is. In het geval van de GBA heeft de burger bijvoorbeeld al het recht om gegevensverstrekking aan derden stop te zetten. Via MijnOverheid zou duidelijk kunnen worden gemaakt welke gegevens dit betreft en MijnOverheid zou een mogelijkheid tot het stopzetten van gegevensleveringen kunnen bieden. In het algemeen impliceert deze extra functionaliteit dat bij de inzage in gegevensverkeer ook de wettelijke grondslag van de uitwisseling gecommuniceerd moet worden en bij welke partij de burger moet zijn om een verzoek tot het stopzetten van de uitwisseling in te dienen.

Informatiekundig zijn de consequenties van een dergelijke functionaliteit zeer groot en momenteel moeilijk in omvang in te schatten.

De functionaliteiten *'module met contactgegevens'* en het *'actief delen van gegevens met derden'* dragen niet zondermeer bij aan het versterken van de informatiepositie van de burger. De eerste is vooral in het belang van de overheid en betreft met name dienstverlening. De tweede roept gemengde reacties op. Een scherpe scheiding tussen publieke en private verantwoordelijkheden is absoluut noodzakelijk. Burgers dienen 100 procent controle te hebben op wat er gebeurt. Maar ook dan voelt lang niet iedereen ervoor en wordt gevreesd dat deze functionaliteit weleens een tegenovergesteld effect zou kunnen hebben en de informatiepositie van de burger zou kunnen verzwakken.

2. Kunnen, en zo ja op welke wijze, overheidsorganisaties verplicht worden aan te sluiten op de functionaliteiten van MijnOverheid?

Voor het versterken van de informatiepositie van burgers is het van belang dat alle overheidsorganisaties inzage geven in gegevens, gegevensverkeer en de verwijderingstermijn en tevens de mogelijkheid bieden tot het digitaal indienen van een correctieverzoek. Het huidige juridische en wettelijke kader kent geen verplichting, en uit het onderzoek komt naar voren een verplichting in enigerlei vorm, met bestuurlijke afspraken over de wijze van realisatie ervan, nodig is om de gewenste resultaten te boeken.
Verschillende partijen geven daarbij wel aan dat het naar hun mening niet mogelijk is om reeds op korte termijn een eventuele verplichting om de functionaliteit "inzage in persoonlijke gegevens" en de additionele functionaliteiten te realiseren. Daarvoor is de informatiekundige impact in veel gevallen te groot.

3. In hoeverre kunnen de additionele functionaliteiten van MijnOverheid en verplichtstelling daarvan invulling geven aan artikel 18 van de Wet algemene bepalingen burgerservicenummer?

Het is mogelijk en het heeft voordelen om via MijnOverheid te voldoen aan de verplichting van de staat om het gebruik van het burgerservicenummer inzichtelijk te maken. Artikel 18 Wabb verplicht de minister tot "de instandhouding van een voorziening met behulp waarvan voor een ieder algemene informatie beschikbaar wordt gesteld met betrekking tot a. het gebruik van burgerservicenummers en b. de gegevensverwerkingen van gebruikers, waarbij burgerservicenummers worden gebruikt". Daartoe is nu de website www.burgerservicenummer.nl ingericht. Door deze site te migreren naar MijnOverheid voorziet dat tevens aan de behoefte van een overzicht bij burgers. Omdat de tekst van de wet niet eist dat de minister een aparte voorziening in stand moet houden, is het mogelijk om via MijnOverheid inzage te geven in gegevens en in gegevensstromen en zo invulling te geven aan de wettelijke verplichting die de minister heeft.

7.2 Algemene conclusies

Informatie alleen is niet voldoende voor versterking informatiepositie burger

Een eerste constatering is dat het versterken van de informatiepositie van de burger tweeledig is. Aan de ene kant gaat het om de 'gewone' burger en aan de andere kant om een burger die verstrikt is geraakt in wet- en regelgeving. De 'gewone' burger hecht weliswaar aan inzage en invloed, want dat maakt de overheid transparant, maar de mate en frequentie waarin eventueel gebruik gemaakt zal worden van mogelijke nieuwe functionaliteiten van MijnOverheid is beperkt.

De burger die een (gegevens)probleem heeft met de overheid, vindt het daarentegen des te belangrijker te weten wat over hem geregistreerd is, en hoe een eventuele onjuistheid in de registraties gecorrigeerd kan worden. Inzage biedt hem de mogelijkheid de oorzaak van zijn probleem te achterhalen en daar zelf invloed op

uit te oefenen. Zowel de burgers als de door ons geraadpleegde organisaties geven echter aan dat inzage in gegevens en verzoek tot correctie niet afdoende zijn om (gegevens)problemen op te lossen. Uit het onderzoek komt naar voren dat een of andere vorm van accountmanagement en/of een gegevensautoriteit (een partij die ervoor zorg draagt dat alle partijen in de keten hun verantwoordelijkheid daadwerkelijk waarmaken) hierbij behulpzaam kan zijn. Geconstateerd wordt dat naast het digitale kanaal het persoonlijke en/of telefonische contact noodzakelijk blijft. Dit geldt zeker ook voor een groep burgers die minder digitaal vaardig is.

Nieuw serviceconcept kent aandachtspunten
Indien MijnOverheid en/of de MijnDomeinen een belangrijke rol en plaats krijgen in het versterken van de informatiepositie van burgers ontstaat een nieuwe serviceconcept. De burger heeft *inzage* in hoe hij bij de overheid geregistreerd staat, wat er over hem wordt uitgewisseld en wanneer gegevens verwijderd worden. De burger heeft *invloed* / *regie* door correctieverzoeken in te dienen, toestemming voor het uitwisselen van gegevens te geven en berichten met de overheid uit te wisselen. De burger kan in probleemgevallen geholpen worden door duidelijk te maken bij welke organisatie hij daarvoor terecht kan. MijnOverheid functioneert als portaal voor de zogenaamde MijnDomeinen waarlangs burgers transacties met overheidsorganisaties verrichten. Essentieel is dat de verschillende verantwoordelijkheden duidelijk via MijnOverheid gecommuniceerd worden. Onomstreden moet zijn welke organisatie voor welk gegeven verantwoordelijk is. Via single sign on komt de burger op de MijnDomeinen terecht en kan hij transacties met overheidsorganisaties verrichten. Volgens dit service-concept zou MijnOverheid ook invulling kunnen geven aan artikel 18 van de Wabb.

In het hoofdstuk met de informatiekundige bevinden is aangegeven dat dit service-concept niet van de ene op de andere dag te realiseren is. Er zijn mogelijkheden wanneer ervoor wordt gekozen om de functionaliteiten betrekking te laten hebben op de kerngegevens die bij het nemen van besluiten in transacties worden gebruikt. Wel is daarvoor verdere definiëring van kerngegevens (en detailgegevens) nodig en moet er ruimte voor diversiteit en snelheid in aansluiting tussen de verschillende uitvoeringsorganisaties zijn. Hierbij moet ook de vraag welke van deze gegevens in MijnOverheid dan wel in de MijnDomeinen dan wel in beide worden gepresenteerd worden beantwoord. Verder is een verplichting met bestuurlijke afspraken over de wijze van realisatie ervan is nodig om de gewenste resultaten te boeken.

Gedurende het onderzoek kwamen ook een aantal andere aandachtspunten naar voren. Een eerste is dat als MijnOverheid uitgebreid wordt, de beveiliging omhoog moet. Dit werd zowel door de burgers als de experts naar voren gebracht. Er is dan een hoger authenticatie-niveau noodzakelijk. Ook moet onomstreden duidelijk zijn dat alleen de burger inzage heeft in zijn gegevens en dat gegevens niet voor andere doeleinden gebruikt worden (doelbinding).

Een tweede aandachtspunt betreft de domeinen zorg en controle. De focus van dit onderzoek heeft op het dienstverleningsdomein gelegen. Er is één gesprek met een zorginstelling geweest. Uit dit gesprek, en uit het gesprek met de WRR, kwam naar voren dat de informatieprocessen in deze domeinen anders van aard zijn. Niet alleen juridisch, maar ook qua betekenis voor burgers. De bevindingen uit het rapport zijn niet zondermeer toepasbaar op deze domeinen. Het is aan te bevelen om deze domeinen nader te verkennen om te kunnen bepalen wat de verschillende functionaliteiten voor deze domeinen betekenen.

Een ander aandachtspunt betreft de informatieprocessen rondom profiling. Het onderzoek heeft zich gericht op ‘vernetwerking’ waarbij sprake is van een aanwijsbare oorzaak-gevolgrelatie. Dat gaat voor ‘profiling’ niet op. Als het gaat om profiling, dan heeft een burger niets aan inzage in gegevens en verzoeken om correctie.

Diverse respondenten hebben de vraag aan de orde gesteld hoe de informatiepositie van de burger in deze gevallen beschermd en versterkt kan worden.

Tot slot geldt dat er in de markt veel ontwikkelingen op het gebied van identiteit en informatiepositie van de burger zijn. Denk bijvoorbeeld aan FinBox (een gezamenlijk berichtenbox initiatief van de banksector) en het zogenaamde Qiy-concept (waarbij burgers zelf een soort kluis met persoonsgegevens beheren). Met name speelt de vraag hierbij wat de overheid zelf wil doen, wat al in de markt ontwikkeld wordt en of en hoe zij hierbij wil aansluiten.

7.3 Succesfactoren voor het vervolg

Deze verkenning biedt een perspectief op de mogelijkheden om de informatiepositie van burgers te versterken door een aantal nieuwe of verbeterde functionaliteiten in MijnOverheid en/of de MijnDomeinen ter beschikking te stellen aan burgers. Daarmee is niet gezegd dat een en ander eenvoudig te realiseren is. Alvorens gekomen kan worden tot een uitvoerbaar implementatieplan dient enerzijds een afweging gemaakt te worden tussen de drie verschillende perspectieven (burger, juridisch, informatiekundig) en anderzijds nog veel uitgezocht en verkend te worden, waarbij deze verkenning als uitgangspunt kan dienen. Op basis van het onderzoek en de gevoerde gesprekken met stakeholders kunnen de volgende factoren benoemd worden die bepalend zullen zijn voor een succesvol vervolg:

1. **Uitwerking en implementatie van functionaliteiten**
   - Deze verkenning geeft een globaal beeld van de nieuwe functionaliteiten. Tijdens het onderzoek viel op dat respondenten vaak heel verschillende beelden hebben van de nieuwe functionaliteiten. Het is noodzakelijk dat deze eerst conceptueel, functioneel en technisch verder worden uitgewerkt. Die uitwerking is zowel nodig per functionaliteit, als in samenhang. Er zijn aanzienlijke verschillen tussen de functionaliteiten waar het de partijen betreft die betrokken zijn, de technische en juridische vraagstukken die opgelost moeten worden, en de startpositie van betrokken partijen.
   - De praktische uitvoerbaarheid van de functionaliteiten en een eventuele verplichting daarvan, dient vooraf door middel van pilots en uitvoeringstoetsen te zijn vastgesteld.
   - Er dient helderheid geschapen te worden over de financiële haalbaarheid en de financiering van de eenmalige ontwikkelkosten en de structurele beheerkosten van de eventuele nieuwe functionaliteiten.

2. **Positionering MijnOverheid en MijnDomeinen**
   - MijnOverheid en de MijnDomeinen zullen meer in samenhang beschouwd moeten worden, waarbij een zorgvuldige positionering van MijnOverheid ten opzichte van de MijnDomeinen noodzakelijk is. Op dit moment is MijnOverheid een voorziening (‘doorverwijzer’) die een (beperkt) overzicht biedt en toegang geeft tot (een aantal) MijnDomeinen. Er is flexibiliteit nodig in het tempo, en wellicht ook qua functionaliteiten, waarmee organisaties hun gegevens ontsluiten via de MijnOverheid en/of de MijnDomeinen. Sommige organisaties zullen aanzienlijke investeringen in hun gegevenshuishouding en de realisatie van hun MijnDomein moeten doen om goed aan te kunnen sluiten op MijnOverheid.
   - Essentieel is het uitgangspunt dat MijnOverheid geen verantwoordelijkheden overneemt van de uitvoeringsinstellingen en basisregistraties. Dat is nodig om de relatie tussen verantwoordelijke en betrokkene die centraal staat in de Wbp intact te laten. Wanneer partijen hun verantwoordelijkheid niet waarmaken dienen ze daarop te worden aangesproken door een bevoegde instantie.

3. **Bestuurlijk draagvlak**

- Het is van belang dat het ministerie van BZK en de betrokken uitvoeringsorganisaties en decentrale overheden binnen de bestaande governance-structuur van MijnOverheid (ondermeer de Programmaraad e-Overheid voor burgers en het Bestuurlijk Overleg MijnOverheid) een gezamenlijke afweging maken tussen de drie onderscheiden perspectieven (burger, juridisch, informatiekundig).
- Omdat er, zowel bestuurlijk als juridisch, op dit moment op geen verplichting bestaat om de functie “persoonlijke gegevens” van MijnOverheid te gebruiken is het van belang dat er bestuurlijk draagvlak ontstaat voor de realisatie van eventuele nieuwe functionaliteiten in, MijnOverheid en/of de MijnDomeinen. Daartoe dient het versterken van de informatiepositie van de burger de nodige politiek-bestuurlijk prioriteit te krijgen.
- Daarbij dient wel rekening gehouden te worden met de reeds bestaande bestuurlijke afspraken die lopen tot 2015. De onderzochte organisaties richten zich momenteel op het nakomen van de prestatie-afspraken die in de Bestuurlijke Regiegroep Dienstverlening en e-Overheid zijn gemaakt en in het iNUP zijn gespecificeerd. Daarin zijn ook prestatie-afspraken opgenomen over MijnOverheid (met name het onderdeel Berichtenbox).

Bijlage I Geïnterviewde personen

Datum	Organisatie	Naam
Eerste gespreksronde		
20-04-2012	Logius	Louis Tinselboer
23-04-2012	Wetenschappelijke Raad voor het Regeringsbeleid	Dennis Broeders & Henk Griffioen
23-04-2012	Belastingdienst	Jan Duijghuisen
24-04-2012	SVB	Luc Boss & Fransje Verheij
25-04-2012	College Bescherming Persoonsgegevens	Jan Vlug & Rina Steenkamp
Tweede gespreksronde		
14-05-2012	VNG	Hans Versteeg & Paul Picauly
21-05-2012	Belastingdienst	Janfolkert Muizelaar & Frans La Housse
25-04-2012	BPR	Anette Vorwerk
29-05-2012	BKWI	Bert Uffen
06-06-2012	KING	Theo van den Brink & Ton Laarhoven
08-06-2012	Qiy	Marcel van Galen
12-06-2012	Kadaster	Arco Groothedde
12-06-2012	Gemeente Dordrecht	Karel van de Hengel
21-06-2012	Interprovinciaal Overleg	Arianne de Man & Koos Ju
29-06-2012	Unie van Waterschappen	Marianne Krug
04-07-2012	SVB	Martin te Beek, Kempe Kruisbrink & Jenny Cals
10-07-2012	Bureau Jeugdzorg Amsterdam (BJAA)	Nanette Heutinck
Derde gespreksronde		
31-08-2012	Ministerie van Binnenlandse Zaken	Janine Jongepier, John Newton & Pim van Loon
03-09-2012	Logius & Belastingdienst	Louis Tinselboer & Joop Kroon
04-09-2012	Belastingdienst	Jan Duijghuisen

Bijlage II Bestudeerde documentatie

Organisatie / auteur	Documentnaam	Datum / jaar
KING	Impactanalyse MijnOverheid	05-03-2012
WRR	iOverheid	02-03-2011
HEC	De informatiepositie van de patiënt	2010
Forum Standaardisatie	Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten	2012
College Bescherming Persoonsgegevens (destijds registratiekamer)	Beveiliging van persoonsgegevens	2001
Kabinet	Kabinetsreactie op WRR-rapport iOverheid	25-08-2011
Diverse overheidsorganisaties	Interne documentatie omtrent gegevensregistraties	