Afsprakenstelsels in de praktijk

Leerervaringen van afsprakenstelsels om te komen tot een uniforme set van eisen voor persoonlijk datamanagement

REGIE OP GEGEVENS
Zelf geregeld, veilig en betrouwbaar!

September 2018

Petra Mettau

PROGRAMMA REGIE OP GEGEVENS

Inleiding

Het hebben van 'regie' (of grip) op je gegevens zorgt ervoor dat je gegevens kunt gebruiken om zaken te regelen, en tegelijkertijd je privacybelangen beter kunt beschermen, bijvoorbeeld doordat je meer zicht krijgt op waar gegevens voor ingezet worden, of doordat je gegevens kunt corrigeren of verwijderen.

Om deze regie op een betrouwbare manier in de praktijk te kunnen faciliteren, zijn organisatorische en technische afspraken nodig. Die afspraken beheer je met elkaar in een afsprakenstelsel.

Om te leren van afsprakenstelsels die in het verleden tot stand zijn gekomen, is een aantal afsprakenstelsels onderzocht die in Nederland werkzaam zijn. Er is gekeken welke rol de overheid heeft gehad bij de totstandkoming en het beheer van deze afsprakenstelsels en naar wat er geleerd kan worden over het opzetten, implementeren en beheren van reeds functionerende afsprakenstelsels zoals voor de telefonie, betaalmarkt, internet-adressen en authenticatie.

Aan de hand van literatuurstudie en een aantal gesprekken met deskundigen die betrokken zijn geweest bij de totstandkoming en/of het beheer van een aantal soortgelijke ontwikkelingen (GSM, iDeal, Idensys, PSD2, eHerkenning, SIDN, iSHARE, Qiy, IRMA, MedMij, Tippiq) wordt in dit stuk bekeken wat leerpunten zijn voor de overheid bij het (mee) ontwikkelen en beheren van de afspraken, infrastructuur en governance om de burger toegang te geven tot de eigen gegevens.

In dit stuk zijn deze leerervaringen vooral beschreven vanuit het perspectief van het ontsluiten van overheidsgegevens om mensen regie te geven over hun gegevens. De vraag hoe private organisaties gegevens gaan ontsluiten en welk aanvullend kader daar voor nodig kan zijn, maakt geen onderdeel uit van deze analyse.

De leerervaringen die naar voren komen uit de interviews zijn:

1. Steun vanuit de top en heldere doelstellingen
2. Rol van de overheid bij totstandkoming van stelsels varieert
3. Open stelsels hebben voorkeur
4. Essentieel is het organiseren van vertrouwen
5. Generieke afspraken ondersteunen sectorale ontwikkelingen
6. Van bilaterale afspraken naar gemeenschappelijke afspraken voor gegevensontsluiting
7. Zorg voor helder beheer en doorontwikkeling van de afspraken

In hoofdstuk 1 wordt een algemene introductie gegeven wat afsprakenstelsels zijn. Aansluitend wordt in hoofdstuk 2 benoemd hoe deze afsprakenstelsels zich verhouden tot de Uniforme Set van Eisen die door het programma Regie op Gegevens wordt opgesteld in samenwerking met het veld. In hoofdstuk 3 worden de 7 leerervaringen beschreven en voorzien van een reactie van het programma.
Tot slot is in bijlage 1 een overzicht opgenomen van de gesprekspartners. In bijlage 2 staat het overzicht van onderzochte afsprakenstelsels.

Regie op Gegevens: de praktijk in beeld

Wat zou het hebben van regie op hun eigen gegevens betekenen voor mensen die bijvoorbeeld dagelijks hun zorg en speciale vervoer moeten regelen? We nemen ***een kijkje*** in het dagelijkse leven van Bettina Bakker en Roos Prommenschenkel.

Hoofdstuk 1
De meerwaarde van afsprakenstelsels

Het uitgangspunt dat burgers en bedrijven regie over hun eigen gegevens moeten kunnen voeren, maakt steeds vaker onderdeel uit van nieuwe richtlijnen en wetgeving. Zo is het bijvoorbeeld een van de pijlers van de AVG en ook in de tweede Payment Service Directive richtlijn (PSD2) speelt het een rol (zie kader).

PSD2 en regie over gegevens

In deze richtlijn kunnen rekeninghouders in de Europese Unie andere dienstverleners dan hun eigen bank toegang geven tot hun betaalrekening(en). Banken moeten dus hun gegevens ontsluiten voor klanten en het mogelijk maken dat derde partijen toegang krijgen tot de betaalrekening van hun klant, mits de klant zelf toestemming geeft. PSD2 heeft als doel een juridisch kader te scheppen met duidelijke en uniforme regels en richtlijnen omtrent de toegang door derden tot betaalrekeningen.

De Nederlandse overheid wil dat mensen zelf meer regie hebben over hun gegevens, ook over gegevens die door de overheid worden beheerd. Daarover is in het regeerakkoord opgenomen: “Ter bevordering van de privacy wordt de eigen regie op persoonsgegevens vergroot. Gebruikers van overheidsdiensten krijgen de mogelijkheid zelf maatschappelijk relevante instanties en organisaties aan te wijzen waaraan een beperkt aantal persoonsgegevens automatisch kan worden verstrekt.”

Maar hoe kun je jouw persoonsgegevens van de ene naar de andere organisatie laten gaan? Of een organisatie toestemming geven om jouw gegevens bij een andere organisatie in te zien? Het is onwerkbaar om elke mogelijke combinatie van organisaties dat onderling te laten regelen, elk op hun eigen manier. Daarom wordt er gesproken om dit gezamenlijk als organisaties te regelen en er afspraken over te maken hoe je dit kun organiseren op een manier die zowel voor de organisaties als de gebruikers gemakkelijk, veilig en efficiënt is. Zo’n geheel aan afspraken wordt een ‘afsprakenstelsel’ genoemd en dat is geen nieuw begrip. Zonder het te beseffen maken we met z’n allen dagelijks gebruik van diensten die gebaseerd zijn op afsprakenstelsels.

Wie kan het zich nog herinneren dat je 30 jaar geleden naar je bankkantoor moest om geld op te nemen? Nu kan je dat ook bij een geldautomaat van een andere bank.

Wie staat er nog van te kijken dat je je mobiele telefoonnummer mee kan nemen van de ene naar de andere telecomprovider? Nu vinden we dat de normaalste zaak van de wereld. Wie maakt er geen gebruik van iDeal, de online-betaaldienst waar alle banken aan meewerken? (zie kader)

Dergelijke ontwikkelingen zijn mede te danken aan afsprakenstelsels. Zoals in het voorbeeld van de mobiele telefonie: wanneer je als telecomprovider de markt op wil, moet je voldoen aan de (inter)nationaal gemaakte afspraken, waaronder het faciliteren van nummerbehoud.

Waarom een afsprakenstelsel?

Er is een toename van digitale transacties en online interactie tussen individuen, bedrijven en overheden. Bij veel organisaties is gegevensuitwisseling traditioneel gebaseerd op bilaterale afspraken (convenanten, SLA’s e.d.). Dat is moeilijk op te schalen en weinig transparant. In plaats van opschalen van bilaterale afspraken zijn de afgelopen decennia in diverse sectoren samenwerkingen tot stand gekomen van deelnemers die streven naar een gemeenschappelijk (eco)-systeem met de andere partijen, in een voorspelbaar en samenhangend geheel. Afsprakenstelsels halen winst uit het standaardiseren van overeenkomsten, waardoor bilaterale contracten, die onderling kunnen verschillen, niet nodig zijn. Veel stelsels halen ook winst uit afspraken over (aansluiten bij) standaarden,

of werken aan het neerzetten van standaarden en het concretiseren van afspraken die niet (volledig) door wet- en regelgeving afgedekt worden. Met name gaat het dan om hoe iets gebeurt dat in de wet- en regelgeving staat, of hoe er voldaan wordt aan wetten en regels. Het doel van het systeem is telkens anders: betalen (iDEAL), telefoneren (GSM), domeinnnamen registreren (ICANN en SIDN), authenticatie door elektronische toegangsdiensten (ETD). Of, in het geval van Regie op Gegevens, ten behoeve van het uitwisselen van persoonsgegevens op zo'n manier dat de persoon in kwestie daar een directe rol in heeft.

Het ontstaan van iDEAL

Aan het begin van online shoppen investeerde elke bank in z'n eigen online betaaloplossing. met als doel de hele markt te veroveren. Was je online aan het winkelen, dan moest je eerst even kijken of je met je bankpas wel kon betalen bij de webshop. Al snel werd duidelijk dat geen van alle banken de hele markt kon veroveren, en populair was het niet om als winkelier elke afzonderlijke oplossing te implementeren. Toen is een aantal toonaangevende banken een traject ingegaan waarin ze afspraken maakten om gezamenlijk online betalen mogelijk te maken. Dat is de basis geweest voor iDEAL.

Wat is een afsprakenstelsel?

In de Angelsaksische literatuur, vooral in het domein van identiteit, wordt vaak gesproken over Trust Frameworks. Identiteitsystemen zijn online omgevingen voor (het managen van) identiteitstransacties. In feite gaat het hier over persoonlijke gegevens in het kader van het vaststellen van iemands identiteit. In het Whitepaper over "***Trust Frameworks for Identity Systems***" wordt beschreven dat er verschillende identiteitssystemen zijn, net zoals er al verschillende systemen of diensten aan het ontstaan zijn om burgers meer regie over hun persoonsgegevens te geven.

'Multi-party' systeem

Al deze systemen en diensten bestaan uit verschillende elementen, maar ze hebben gemeen dat ze, wanneer sprake is van meerdere deelnemende partijen, de deelnemende partijen worden gestuurd door middel van juridisch afdwingbare en onafhankelijke specificaties, regels en afspraken die de werking van dit multi-party systeem regelt. Het is opgericht voor een bepaald doel en geeft deelnemers zekerheid dat iedereen de regels volgt die bij de rol horen.

"A trust framework is a term used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a group of participants bound by a contractual set of requirements."

Bron: OIX, A Global Inventory of Trust Frameworks and Trust Schemes

Open en gedecentraliseerd ecosysteem

Kenmerk van een afsprakenstelsel is vaak dat het niet zelf iets bouwt, maar regels geeft waaraan partijen, die gezamenlijk het systeem opzetten of later toetreden, aan voldoen. Waarbij meerdere partijen onderdelen van het stelsel kunnen bouwen of gebruiken en waarbij er een open en gedecentraliseerd ecosysteem ontstaat waar een monopolie positie kan worden uitgesloten. Dit in tegenstelling tot de grote monopolistische platformen, waar één partij de regels bepaalt van een ecosysteem waar dienstverleners en gebruikers met elkaar interacteren en/of transacties kunnen afsluiten (zie ook leerervaring 3 over open stelsels).

Bronbestanden

Regie voeren over de eigen gegevens, staat of valt met het ter beschikking komen van gegevens uit

de bronbestanden, zoals de transactiegegevens van banken, de NAW gegevens uit de GBA, de huurgegevens van verhuurders, salarisgegevens bij werkgevers of de UWV, medische gegevens van de zorgverleners, of het door de Belastingdienst vastgesteld inkomen.

Regie op gegevens

Op dit moment ontstaan er verschillende afsprakenstelsels om burgers en bedrijven te ondersteunen bij de regie over hun gegevens (zoals Qiy en MedMij), ook zien we gegevensdiensten die zich kenmerken door één organisatie die een (technische) oplossing biedt aan burgers om regie te voeren over een aantal persoonsgegevens (zoals IRMA, Schluss en het Financieel Paspoort). Een aantal van deze gegevensdiensten heeft de potentie of de wens om door te groeien naar, of ingebed te raken binnen, een afsprakenstelsel. Het is voor de burger belangrijk dat er diverse aanbieders zijn, maar dat het ook duidelijk is of ze op een betrouwbare en veilige manier omgaan met persoonsgegevens. Veel afsprakenstelsels voor persoonlijk datamanagement zullen voor dezelfde aspecten regels en afspraken opstellen. Die zullen goeddeels ook dezelfde beoogde bedoelingen hebben. Als dat op een hoger/centraler niveau gedaan kan worden, dan scheelt dat werk en regeldruk. Daarom is het wenselijk dat er een Uniforme Set van Eisen komt die aangeeft waar deze stelsels aan zouden moeten voldoen. De onderlinge verschillen van afsprakenstelsels zouden vooral tot uitdrukking kunnen komen in de uitwerking van die specifieke stelsels. Een stelsel in een specifieke branche of gericht op een specifiek soort attributen, zal de wens hebben om daarvoor toegepaste regels op te stellen die de specifieke belangen van de betrokkenen weerspiegelen.

Afsprakenstelsel in de zorg: MedMij

MedMij zorgt dat er persoonlijke gezondheidsomgevingen kunnen komen voor elk individu. Er is echter geen standaardontwerp voor een persoonlijke gezondheidsomgeving van dé patiënt. Immers, de inhoud en het gebruik ervan kunnen uiteenlopen, afhankelijk van levensfase, gezondheidssituatie, vaardigheden en persoonlijke behoefte. MedMij bouwt dan ook niet zelf zo'n omgeving. In plaats daarvan stelt MedMij spelregels op voor het uitwisselen van gegevens. Aan de hand van deze regels kunnen persoonlijke gezondheidsomgeving-aanbieders producten en diensten aanbieden die aansluiten bij de uiteenlopende vragen van het individu.

Een belangrijk uitgangspunt bij MedMij is dat patiënten zelf hun persoonlijke gezondheidsomgeving kunnen kiezen. Het MedMij Afsprakenstelsel zorgt ervoor dat de zorgaanbieder geen afzonderlijke koppelingen hoeft te maken met al deze verschillende persoonlijke gezondheidsomgevingen. De informatie-uitwisseling is gestandaardiseerd en voldoet aan de gestelde veiligheidseisen.

Diverse partijen in de zorg en ondersteuning werken samen aan de ontwikkeling van MedMij: brancheorganisaties, verenigingen van huisartsen, ziekenhuizen, apothekers, thuiszorgorganisaties, verpleeghuizen, zorgverzekeraars, patiënten en (lokale) overheden. Deze organisaties vormen samen het Informatieberaad Zorg. Patiëntenfederatie Nederland coördineert het MedMij-programma en vormt samen met Nictiz en het ministerie van VWS het uitvoerende programmateam.

Hoofdstuk 2
Afsprakenstelsels en de Uniforme Set van Eisen

Elk afsprakenstelsel functioneert binnen bestaande (inter)nationale wet- en regelgeving. Dit kan algemene wet- en regelgeving betreffen (zoals de AVG) of specifieke zoals voor de zorg waar men in het afsprakenstelsel MedMij binnen moet functioneren. Daarnaast hebben afsprakenstelsels te maken met standaarden die van toepassing zijn op het digitale karakter van de uitwisseling van de gegevens. Standaarden zijn belangrijk voor het borgen van interoperabiliteit tussen verschillende dienstverleners en het creëren van een gelijk speelveld tussen de deelnemers aan een stelsel. Waarbij er geen concurrentie is op de waarden van het stelsel, maar wel op de toegevoegde waarde van de verschillende partijen.

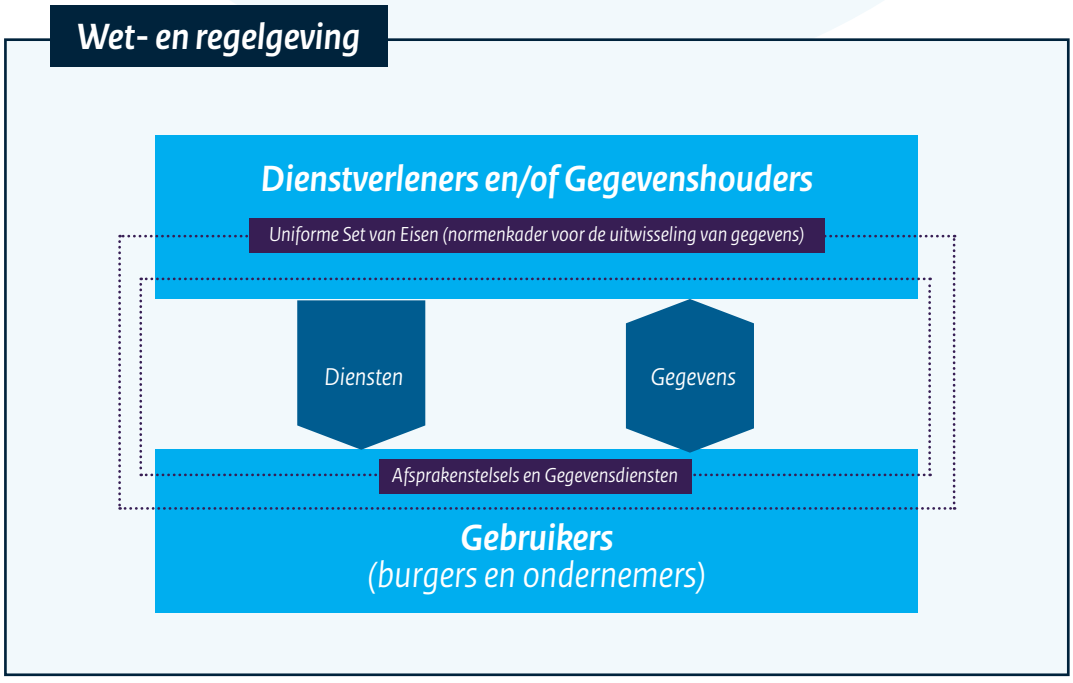
Het programma Regie op Gegevens zal deze bestaande wet- en regelgeving aanvullen of concretiseren, zodat de uitwerking van hoe de regels worden toegepast op een uniforme wijze gebeurt, en voor gebruikers herkenbaar is. Waardoor organisaties, maar ook burgers, er op kunnen vertrouwen dat de iedereen conform de afgesproken privacy- en beveiligingseisen, omgaat met de gegevens.

Gedurende de interviews werd een aantal keer de wens geuit om de Uniforme Set van Eisen op hoofdlijnen te beschrijven, in de vorm van een 'principal based' normenkader. Dit sluit aan bij de aanpak van het programma.

Het programma Regie op Gegevens is niet van plan om zelf een afsprakenstelsel te maken, maar richt zich op de generieke normen die nodig zijn om een zo vrij mogelijk verkeer van gegevens onder regie van de burger mogelijk te maken.

In het volgende hoofdstuk wordt ingegaan wat belangrijke leerpunten zijn om bij het totstandkomen van de Uniforme Set van Eisen rekening mee te houden.

Hieronder wordt schematisch weergegeven hoe de Uniforme Set van Eisen gaat raken aan afsprakenstelsels en gegevensdiensten, waarbij burgers en ondernemers de keuze hebben van welke afsprakenstelsels en gegevensdiensten ze gebruik willen maken.



Hoofdstuk 3
Leerpunten rondom afsprakenstelsels

In de voorgaande hoofdstukken is in vogelvlucht het begrip afsprakenstelsels geduid en hoe dit zich verhoudt tot de Uniforme Set van Eisen waar het programma Regie op Gegevens samen met het veld aan werkt. In dit hoofdstuk worden de leerpunten beschreven die zijn opgehaald door middel van gesprekken en literatuurstudie. Hieruit is een zevental leerpunten gehaald die in dit hoofdstuk worden toegelicht. Aan het eind van elk leerpunt geeft het programma Regie op Gegevens een reflectie op het betreffende leerpunt.

1. Steun vanuit de top en heldere doelstellingen

In bijna elk gesprek kwam 'steun vanuit de top' als kritieke succesfactor naar voren voor het slagen van het tot stand komen van een afsprakenstelsel. Voorbeelden hiervan zijn GSM, MedMij en iDEAL. Het algemene doel waarom je een afsprakenstelsel wilt ontwikkelen, én de belangen van partijen daarbij, moeten helder zijn. Men moet het eens zijn over wat men wil gaan doen en hoe besluitvorming gaat plaatsvinden. Een gemeenschappelijk doel geeft snelheid en focust de discussies.

Principe overeenkomst

Bij voorkeur wordt het gemeeschappelijke doel en de uitgangspunten vastgelegd in een principe overeenkomst. Daarna staan de normen vast, waarbij tijdens de uitwerking wel over de invulling van de normen kan worden gediscussieerd. Van belang is ook dat er duidelijkheid én overeenstemming is over hoe de kosten en de opbrengsten verdeeld zijn.

Business case

Een stelsel moet zo opgezet zijn dat er voor alle partijen die eraan deelnemen een positieve business case te behalen valt. Dat is geen sinecure, omdat je altijd werkt met een tweezijdige markt (individuele eindgebruikers enerzijds en dienstverleners en databronnen anderzijds). Daarnaast moet ook het beheer van het stelsel kostendekkend uitgevoerd kunnen worden.

PSD2 – Steun vanuit de top en heldere doelstellingen

De Europese Unie voert PSD2 in om innovatie in de bankenwereld te versnellen en concurrentie in het betaalverkeer te bevorderen. Een van de strategische doelstellingen die het Europese Parlement met PSD2 heeft, is het creëren van één digitale betaalmarkt voor alle Europese lidstaten. Een andere belangrijke drijfveer voor de invoering van PSD2 is de toegang tot betaaldiensten te verbreden en de betaalmarkt voor nieuwe spelers open te stellen.

PDS2 verplicht banken hun data-infrastructuur open te stellen voor derden. Het idee erachter is dat als derde partijen toegang hebben tot de betaalrekeningen, zij producten en betaaldiensten kunnen ontwikkelen en aanbieden die beter aansluiten bij de behoeften van klanten of rekeninghouders. Met de opkomst van de FinTech-industrie zijn nieuwe businessmodellen en diensten ontwikkeld die de verhoudingen binnen de markt behoorlijk hebben veranderd. De herziening van de richtlijn is daarom niet zo zeer een oorzaak, maar meer een gevolg van de ontwikkelingen in de markt die sinds enkele jaren in gang zijn gezet.

Verwacht wordt dat burgers met de nieuwe regelgeving meer keuze krijgen in financiële toepassingen. Daarnaast kunnen bedrijven het gebruiksgemak van financiële diensten verhogen. Zo kan je dan bijvoorbeeld ook via niet-financiële bedrijven betalingen doen, rekeninginformatie ophalen en je saldo checken.

Duur totstandkoming
De duur van het tot stand komen van afsprakenstelsels varieert tussen ongeveer 2 jaar tot wel 10 jaar van de eerste start tot implementatie. De implementatie (voldoende massa van aanbieders en gebruikers) vergt, naast het maken van afspraken, ook de benodigde inspanning.

Eigenaarschap
Uiteindelijk moet er een partij zijn die eigenaarschap (en ondernemerschap) toont ten aanzien van het stelsel. Vaak is dit een onafhankelijke partij, maar wel met een gedrevenheid om het stelsel door te ontwikkelen en te laten groeien. Qua onafhankelijkheid is de overheid daar vaak een logische keuze voor. Bij commerciëlere stelsels zie je vaak een consortium dat een 3de partij hiervoor heeft opgericht. Beide constructies hebben de neiging tot inertie: de overheid is geen ondernemer, partijen in een consortium zijn elkaars concurrenten.

Reflectie RoG – Bestuurlijk draagvlak
Het programma Regie op gegevens organiseert een bestuurlijk overleg om de uitgangspunten voor betrouwbare gegevensuitwisseling onder regie van de betrokken personen een goede bestuurlijke basis te geven. Deze uitgangspunten vormen op hun beurt weer de basis voor de Uniforme Set van Eisen.

2. Rol van de overheid bij de totstandkoming van stelsels varieert

De rol van de overheid bij de totstandkoming van stelsels loopt uiteen van initiator tot deelnemer. Bij een aantal afsprakenstelsels heeft de overheid het initiatief genomen, zoals bij het GSM traject in de jaren 80 van de vorige eeuw. Op Europees niveau zijn de PSD2 en eIDAS tot stand gekomen. En in Nederland is de overheid eigenaar van de afsprakenstelsels ETD en eHerkenning. De overheid kan ook, samen met andere partijen, initiator, financier of deelnemer zijn. Voorbeelden daarvan zijn iSHARE en MedMij.

GSM – initiatief van diverse nationale overheden

De afspraken voor een internationaal mobiel (GSM) netwerk zijn begin jaren 80 van de vorige eeuw gestart in Europa. In die tijd bestonden er enkel nationale telecomaanbieders, in handen van nationale overheden. Een aantal Europese landen, waaronder Groot-Brittannië, Noorwegen, Frankrijk en Zweden, besloten om van de diverse analoge mobiele systemen een doorontwikkeling te maken naar een, in eerste instantie Europese, digitale standaard voor mobiele telefonie. Naast de voordelen van een grensoverschrijdend mobiel netwerk zagen de overheden ook grote mogelijkheden voor de stimulering van hun nationale telecomindustrie die de taak werd gegeven de benodigde technologie te ontwikkelen. Er werd een speciaal Europees standaardisatie organisatie (ETSI) opgericht om de technische afspraken in goede banen te leiden. De idee was dat een Europese standaard *economies of scale* zou creëren en aldus de kosten van implementatie op een aanvaardbaar niveau zou houden. Het vrijmaken van de frequenties gebeurde via een ander Europees instituut, het CEPT. De rest is geschiedenis.

De huidige ontwikkelingen van 4G naar 5G dragen nog steeds de grondkenmerken van bovenstaand model in zich. En nationale overheden, vanuit hun taak als overheid, zijn uiteraard nog steeds betrokken bij de afspraken rond beveiliging, interferentie, interoperabiliteit en volksgezondheid.

Overheid op afstand
Afsprakenstelsels kunnen ook volledig tot stand komt in de private sector waar de overheid geen rol bij speelt. De meest aansprekende voorbeelden daarin zijn iDEAL en het Creditcard-stelsel.

Overheid als eigenaar
In de praktijk zijn er ook initiatieven om een afsprakenstelsel vorm te geven, gebaseerd op interoperabiliteit en open toegang, zoals bij Idensys, waarbij tijdens de ontwikkeling toch wordt gekozen voor een gesloten model met enkele aanbieders, bijvoorbeeld: DigiD voor burgers en een aanbesteding voor een privaat middel.

Neutrale partij
Tot slot ontstaan er initiatieven in de private sector die werken aan een afsprakenstelsel voor burgers en bedrijven, maar die aangeven daar een neutrale organisatie voor nodig hebben voor een onafhankelijke vertrouwensinfrastructuur, zoals Tippiq.

Reflectie RoG – rol van de overheid
Met het instellen van het programma Regie op Gegevens, en de ambities die zijn neergelegd in de ***Tallinn Ministerial Declaration on eGovernment***, het ***Regeerakkoord Rutte III***, de ***Nederlandse Digitaliseringsstrategie: Nederland Digitaal*** en ***NL DIGIbeter: Agenda Digitale Overheid***, neemt de overheid duidelijk het initiatief om te komen tot een aantal basisafspraken.

Omdat het kunnen uitwisselen van je gegevens al heel snel over de grenzen van publiek en privaat heen gaat, richt het programma zich op een Uniforme Set van Eisen dat breed gedragen wordt door het veld.

3. Open stelsels hebben voorkeur

Bij de inrichting van stelsels kan je kiezen voor een systeem met een meer open of gesloten karakter.

Meer of minder open
De mate van openheid kan op verschillende manieren worden gerealiseerd. In de eerste plaats door aan te geven in welke mate de rollen in het stelsel open staan voor toetreding door partijen. Kan bijvoorbeeld iedereen meedoen die aan de gestelde vereisten voldoet? Een tweede element gaat over de mate van openheid van de besluitvorming. Tot slot zal altijd een afweging moeten worden gemaakt over de (on)wenselijkheid van een centrale partij die alle transacties afhandelt.

Van gesloten naar open
Daarbij is het niet onlogisch dat een stelsel wat meer gesloten begint, maar de intentie heeft om open te zijn. Omdat de zogenoemde open Multi-party governance erg ingewikkeld, tijdrovend en duur kan zijn in de opstartfase. De wat meer gesloten start geeft ook de eerste investeerders in het stelsel de mogelijkheid om (kennis)voordeel op te doen ten aanzien van latere instappers.

Reflectie RoG – naar een open stelsel
Het programma Regie op Gegevens stelt voor om als uitgangspunt op te nemen dat afsprakenstelsels voor persoonlijk datamanagement open stelsels zijn.

4. Essentieel is het organiseren van vertrouwen

Essentieel onderdeel van een afsprakenstelsel, waarin verschillende organisaties samenwerken om gegevens uit te wisselen is, dat er vertrouwen is bij alle deelnemers. Zowel de gegevenshouders, de aanbieders van gegevensdiensten en de eindgebruiker. Maar hoe veranker je vertrouwen in een infrastructuur? Naast een structuur voor authenticatie, is de verwachting dat er ook een consent-infrastructuur gaat ontstaan waarin is vastgelegd wie welke gegevens mag zien en onder welke condities. Vanzelfsprekend gebaseerd op bestaande wet- en regelgeving. Toekomstbeeld is om uiteindelijk de data bij de bron te houden en mensen (of organisaties met verifieerbare toestemming van de betrokken persoon) toegang te geven tot zo'n bron.

PSD2

PSD2 verbiedt de nieuwe dienstverleners van de klant om andere gegevens van de klant in te zien dan waarvoor expliciet toestemming is gegeven. Klanten moeten instemmen met de toegang tot, het gebruik en de verwerking van deze gegevens. Met de nieuwe regels is het niet (meer) mogelijk om toegang te krijgen tot de gegevens van de klant door middel van "screenscraping". Screenscraping betekent toegang tot de gegevens via de klantinterface met de beveiligingsreferenties van de klant. De Nederlandse banken gaan dedicated interfaces ontwikkelingen, via de consumer interface, waar de derde partij een aparte identificatie voor nodig heeft zodat altijd traceerbaar is of de klant of de derde partij heeft ingelogd.

Betrouwbare gegevensuitwisseling
Het ontsluiten van gegevens die je als organisatie beheert, voor andere doeleinden dan waar jouw organisatie voor is opgericht, is voor veel organisaties geen logische of comfortabele stap. Om dat wel te willen (of moeten) doen, is het belangrijk dat ze zeker weten dat gegevensuitwisseling veilig, betrouwbaar en juist gebeurt. In een afsprakenstelsel wordt dat met elkaar bedacht, uitgezocht en geregeld, zodat niemand het wiel zelf hoeft uit te vinden, er een efficiënte en betrouwbare infrastructuur ontstaat voor het uitwisselen van gegevens en duidelijk is welke aanbieders van afsprakenstelsels en gegevensdiensten voldoen aan de gestelde gemeenschappelijke eisen.

Reflectie RoG – organiseren van vertrouwen
Een gemeenschappelijk Uniforme Set van Eisen geeft de deelnemende partijen én de burger zekerheid dat er op een betrouwbare en veilige manier gegevens ter beschikking kunnen worden gesteld aan de burger die daarmee op een vertrouwde manier zelf regiehandelingen kan uitvoeren met deze gegevens.

5. Generieke afspraken ondersteunen sectorale ontwikkelingen

Momenteel wordt voornamelijk sectoraal gewerkt aan het ontsluiten van persoonsgegevens voor burgers en bedrijven. Voorbeelden zijn het MedMij afsprakenstelsel in de zorg, PSD2 voor de banken, Tippiq vanuit de energiemarkt en iSHARE voor de logistieke sector. Een aantal organisaties ontwikkelt generieke oplossingen voor het delen van data (Qiy, IRMA), die al dan niet ingezet kunnen worden voor sectorale toepassingen.

Deze sectorale ontwikkeling is verklaarbaar omdat data delen nog in ontwikkeling is en veel diverse vraagstukken kent. Het is logisch om hier vooral vanuit de eigen sector mee bezig te zijn. Er is nog geen gemeenschappelijk antwoord op generieke vraagstukken. Een aantal daarvan wordt door diverse deskundigen benoemd. De belangrijkste drie zijn:

1. Zorg voor interoperabiliteit tussen stelsels
2. Organiseer trust
3. Kom tot noodzakelijke standaarden om gegevensuitwisseling efficiënt en betrouwbaar te maken.

Reflectie RoG – generieke afspraken
Het proces om te komen tot een Uniforme Set van Eisen heeft tot doel generieke vraagstukken inzichtelijk te krijgen en er een antwoord op te geven door middel van een normenkader op generiek niveau. Vervolgens kunnen sectoren hier zelf een specifieke invulling aan geven.

6. Van bilaterale afspraken naar gemeenschappelijke afspraken voor gegevens ontsluiting

Het is gemakkelijk voor te stellen dat met meer dan 4000 banken in Europa, het duurzamer is om aan gemeenschappelijke standaarden voor gegevensontsluiting te werken. De inspanningen om enorme hoeveelheden interfaces te implementeren

iSHARE – gemeenschappelijke afspraken voor gegevens ontsluiting

iSHARE is ontwikkeld door partijen uit de logistieke sector. Dit afsprakenstelsel werkt sinds 2018 waardoor in de logistieke sector iedereen met iedereen op een eenvoudige en gecontroleerde manier data kan delen. Ook met tot dusver onbekende partijen. Dit gebeurt in opdracht van de Topsector Logistiek die met iSHARE samenwerking in de keten verder wil aanjagen. iSHARE is volledig internationaal inzetbaar, wel is de adoptie in Nederland gestart. Uitgangspunt is dat data wordt gedeeld bij de bron en de data eigenaar te allen tijde controle heeft over zijn data.

en continue te onderhouden, zijn niet haalbaar en zouden de gewenste innovatie van de bancaire sector en daarbij behorende dienstverlening (wat een doel is van PSD2) in de weg staan.

Nederlandse banken kiezen voor het gezamenlijk ontwikkelen van een interface. Ook is een initiatief gestart met het doel om een open, gemeenschappelijke en geharmoniseerde Europese API-norm (Application Programming Interface) te creëren waarmee derde partijen toegang krijgen tot bankrekeningen onder PSD2.

Interface
Uitvoeringsorganisaties, als belangrijkste beheerder van persoonsgegevens binnen de overheid, gegevensdiensten en dienstaanbieders, zijn gebaat bij een gemeenschappelijke en geharmoniseerde interface waarmee zij gegevens kunnen ontsluiten, al dan niet naar diverse sectorale of generieke infrastructuren die de eigen regie van de burger ondersteunen.

Standaardisatie
Hoe deze API-standaardisatie tot stand komt, verschilt per stelsel. Bij de PSD2 heeft de EU ervoor gekozen dit niet zelf te ontwikkelen, maar door de markt tot stand te laten komen. Bij MedMij is deze standaardisatie wel beschreven.

Reflectie RoG – Eenduidige gegevensontsluiting
Het programma Regie op Gegevens heeft oog voor de ontwikkeling dat het voor overheden wenselijk kan zijn dat gegevens naar stelsels en gegevensdiensten eenduidig worden ontsloten. Dit onderwerp is nog in ontwikkeling en wordt onder meer meegenomen in de programmalijn van maatschappelijke initiatieven.

MedMij – standaardisatie van gegevensuitwisseling

Als elke app of website zelf afspraken moet maken over gegevensuitwisseling met meerdere registratiesystemen, dan ontstaat een wirwar aan gesprekken in verschillende talen. MedMij lost dit op met afspraken tussen de persoonlijke gezondheidsomgevingen en de (registratie) systemen van de zorgverlener. Om deelnemer te worden aan het MedMij afsprakenstelsel, moet de leverancier voldoen aan de MedMij-spelregels. Deze ICT-leveranciers (dat hoeft geen tussenpersoon te zijn, maar kan ook door de zorgaanbieder zelf gedaan worden) wisselen versleuteld gegevens met elkaar uit. Zelf kunnen zij de informatie niet inzien. Andere voorwaarden gaan onder andere over het beveiligd opslaan en gebruik van gezondheidsgegevens. Persoonlijke gezondheidsomgevingen en registratiesystemen die de gegevens niet goed beveiligen en zich niet aan de afspraken conformeren kunnen niet deelnemen aan ***MedMij***.

7. Zorg voor helder beheer en doorontwikkeling van de afspraken

Gegevensuitwisseling onder regie van de burger vraagt om een gemeenschappelijke set van juridisch afdwingbare en onafhankelijke specificaties, regels en afspraken voor de werking van een gemeenschappelijk (eco)systeem.

Verschillende actoren hebben hier verschillende rollen en verantwoordelijkheden. Het inrichten van de governance betreft afspraken over de besluitvorming en het verdelen van de verantwoordelijkheden tussen actoren ten behoeve van het gezamenlijke doel dat is afgesproken. Denk daarbij aan verantwoordelijkheden ten aanzien van de visie, financiën, beheer van de afsprakenset, beheer van de standaarden ten aanzien van de gegevensontsluiting, handhaving van de naleving van de afspraken, certificering (indien daarvoor gekozen wordt), klachten/geschillen, calamiteiten.

Beheer

Voor het beheer van deze gemeenschappelijke afspraken zijn diverse constructies denkbaar die van veel factoren afhangen. Is het stelsel nationaal of internationaal? Wil de overheid er een rol in blijven houden? Bestaan er reeds logische beheerorganisaties of moet er een nieuwe organisatie voor worden ingericht? Hoe wordt toetreding tot het afsprakenstelsel geregeld?

Ook het toezicht wordt specifiek voor elk afsprakenstelsel ingericht, vaak afhankelijk van de sector waarvoor het stelsel werkt. Zo zal voor de uitvoering van de PSD2 in Nederland een viertal toezichthoudende organisaties betrokken zijn: Autoriteit Persoonsgegevens, De Nederlandse Bank, Autoriteit Consument en Markt en de Autoriteit Financiële Markten.

Reflectie RoG – Rollen van de overheid

Het programma Regie op Gegevens onderscheidt vier rollen van de overheid: kaderstellend, ontsluiten van (bron)gegevens, aanbieden van diensten en tot slot ten aanzien van toezicht.

ICANN: hoe het beheer van het stelsel in de tijd kan veranderen

ICANN (*Internet Corporation for Assigned Names and Numbers*) is een non-profitorganisatie die een aantal internet-gerelateerde taken uitvoert, zoals het toekennen en specificeren van topleveldomeinen, toewijzen van domeinnamen en de distributie van IP-nummers. ICANN is opgericht op 18 september 1998 en nam toen de taken over van Jon Postel, een Amerikaanse computerwetenschapper die een zeer belangrijke bijdrage leverde aan de oprichting van het internet.

Aanvankelijk functioneerde de ICANN onder toezicht van het Amerikaanse ministerie van handel. Op 1 oktober 2016 is de ICANN verzelfstandigd en geprivatiseerd, voor het uitvoeren van een aantal functies. Een multistakeholdermodel moet er voor zorgen dat de organisatie verantwoording aflegt aan de globale internetgemeenschap.

ICANN beheert zelf geen domeinnamen. Dit laat het over aan andere organisaties, *registry's* genoemd. In Nederland is dat de Stichting Internet Domeinregistratie Nederland (SIDN).

Reageren? Graag!

Graag zien we reacties van lezers op dit stuk. In de voorgaande hoofdstukken is een aantal leerervaringen besproken. Een drietal beschouwingen hebben we hieronder nogmaals opgenomen. We gaan graag met jou als lezer in gesprek. Dit stuk wordt gepubliceerd op onze ***Community RoG op Pleio***. Waar je in de groep 'Uniforme Set van Eisen' deel kan nemen aan de discussie.

1. Omdat personen hun gegevens willen delen tussen zowel private als publieke organisaties, richt het programma Regie op Gegevens zich op een Uniforme Set van Eisen dat zowel door private partijen als de overheid wordt gedragen.

2. Het proces om te komen tot een Uniforme Set van Eisen heeft tot doel generieke vraagstukken inzichtelijk te krijgen en er een antwoord op te geven door middel van een normenkader op generiek niveau. Vervolgens kunnen sectoren hier zelf een specifieke invulling aan geven.

3. Het programma Regie op Gegevens stelt voor om als uitgangspunt op te nemen dat afsprakenstelsels voor persoonlijk datamanagement open stelsels zijn.

Leren door doen

Het programma '***Burgers en bedrijven in regie op hun gegevens***' is aan het experimenteren met en leren van bestaande oplossingen en innovaties om het hebben van regie op gegevens mogelijk te maken.

De ambitie van het programma:
'Het is waardevol als inwoners en ondernemers -op een veilige en betrouwbare manier- hun gegevens kunnen gebruiken om zaken in hun leven te regelen en hun privacy te beheren.

Dit vraagt om heldere afspraken over hoe en waarvoor gegevens ontsloten worden, zodat gebruikers, gegevenshouders en dienstenaanbieders met vertrouwen mee kunnen doen aan het uitwisselen van gegevens, over de grenzen van publiek en privaat heen.'

Het programma Regie op Gegevens werkt in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Bijlage 1
Gesprekspartners

Richard Blad	Ministerie van Binnenlandse zaken en Koninkrijksrelaties
Wouter Diephuis	Ministerie van Binnenlandse zaken en Koninkrijksrelaties
Marcel Heldoorn	Patiëntenfederatie
Indra Henneman	MedMij
Bob Hulsebosch	Innovalor
Bob Kronenburg	Alliander
Bart Jacobs	IRMA
Wil Janssen	Innovalor
Carlo Luijten	Ministerie van Binnenlandse zaken en Koninkrijksrelaties
Douwe Lycklama	Innopay
Esther Makaay	SIDN
Adriana Nugter	Nugter bvba
Claire Rijkelijkhuizen	Ministerie van Financiën
Jurrian Wesselink	Innopay

Bijlage 2
Onderzochte afsprakenstelsels

- Elektronische toegangsdiensten (ETD) – het stelsels dat eHerkenning reguleert
- MedMij – afsprakenstelsel voor uitwisseling van gezondheidsgegevens
- SIDN – beheert de domeinnamen voor het topleveldomein .nl en Registrar van ICANN, de internationale organisatie voor onder meer de distributie van IP-nummers
- GSMA en ETSI – De afspraken voor het internationale GSM netwerk
- iDEAL – stelsel om online betalen te faciliteren
- iSHARE – afsprakenstelsel voor de logistieke sector
- Tippiq – afsprakenstelsel waarin het huis en alles wat daar in en rond (digitaal) gebeurt, centraal staat
- Qiy – afsprakenstelsel geeft mensen controle over hun eigen gegevens
- IRMA – gegevensdienst die, via de eigen mobiele telefoon, mensen in staat stelt om eigen gegevens over zichzelf wel/niet te laten zien aan dienstverleners of andere partijen