Greenpaper

1 mei 2017

SIVI digitale toekomst verzekerd van standaarden

De consument bepaalt!

Regie op persoonsgegevens, samenwerking in de branche herstelt vertrouwen

Inhoud

Management-samenvatting

SIVI en de Werkgroep Strategische Verkenning SIVI 2016 geven met dit greenpaper een aanzet tot de strategische discussie rond samenwerking binnen onze branche. Een discussie die gaat over de meest optimale vormen van samenwerking binnen de nieuwe AVG-regelgeving, en in het verlengde van de kansen die de diverse ROPG-initiatieven bieden. Diverse ROPG-initiatieven en de nieuwe privacy wetgeving stellen de consument centraal. Door samenwerking in de verzekeringsbranche kan de consument gefaciliteerd worden om laagdrempelig regie te voeren over zijn persoonsgegevens; de consument bepaalt! Dit greenpaper levert een bijdrage aan de afwegingen die daar bij horen. Duidelijk is dat door samenwerking bijgedragen wordt aan herstel van vertrouwen van de consument in verzekeraars en intermediairs. In 2017 zal door SIVI actief de dialoog worden gezocht om te komen tot gerichte besluitvorming en acties op dit interessante en bovenal belangrijke dossier.

Vraagstelling en afbakening

De centrale vraag in dit greenpaper is: welke opties hebben ketenpartners binnen de verzekeringsbranche voor samenwerking rond Regie Op Persoonsgegevens (ROPG).

Doel is het creëren van inzicht en overzicht door het op een rij zetten van uitdagingen en opties voor samenwerking. Ketenpartners creëren zo een gemeenschappelijk vertrekpunt en vocabulaire voor de oriëntatie op samenwerking en het maken van keuzes.

Regie Op Persoonsgegevens is de zeggenschap over en de controle op de verwerking van persoonsgegevens. Dit zijn zowel de gegevens die in de wet zijn aangemerkt als persoonsgegevens als gegevens die via de context zijn terug te voeren naar een natuurlijk levend persoon.

De consument staat open voor ROPG onder de juiste voorwaarden

Relatief weinig onderzoek is beschikbaar. Het beschikbare onderzoek laat zien dat er onder de juiste voorwaarden zeker markt is voor ROPG. De belangrijkste voorwaarden zijn:

- Bewustzijn over veiligheid en privacy. Het is opvallend dat men in Nederland niet zomaar veel waarde hecht aan het zelf verkopen van data. Het delen van data doen consumenten met verschillende partijen en met verschillende beweegredenen.
- Een basis van vertrouwen. Dit speelt een veel grotere rol dan het krijgen van geld of een dienst voor de gegevens.
- Gemak: één persoonlijke onlineomgeving voor alle verzekeringspolissen. De consument heeft een duidelijke behoefte aan een totale digitale financiële administratie, mits hij zelf kan bepalen welke informatie wel en niet beschikbaar is.

ROPG-initiatieven in de markt

De laatste jaren kwamen verschillende initiatieven op in Nederland en buitenland. Initiatieven die zorgen dat consumenten de voordelen van ROPG ervaren, en vertrouwen geven over de opslag en juiste toepassing van hun persoonsgegevens. Hoewel deze initiatieven qua opzet en eigenschappen verschillen, richten ze zich allemaal op het kunnen voeren van regie. Dit greenpaper bespreekt de belangrijkste initiatieven.

De indeling van de initiatieven is:
1. Authenticatievoorzieningen
2. Afsprakenstelsels
3. Toepassingen

Veel bestaande ROPG-initiatieven staan nog in de kinderschoenen. De uitrol van authenticatievoorzieningen, afsprakenstelsels en toepassingen verloopt nog niet succesvol. Juist samenwerking kan een initiatief succesvol maken:

- Het vermijdt traditionele kip-ei-vraagstukken.
- Pas als voldoende aanbieders zich aan een bepaald platform/oplossing committeren, ervaart de consument voldoende voordelen.
- Het stimuleert tot het aanbrengen van focus en beperkt zo bijvoorbeeld het aantal te onderhouden koppelvlakken.

Wettelijk kader

Ook de overheid zit op het terrein van ROPG niet stil. ROPG en de toenemende macht van spelers als Facebook en Google, inspireerden de Europese en nationale politiek. Vanaf mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). Kort gezegd zorgt de AVG ervoor dat consumenten geheel in controle komen over hun eigen gegevens. Verwerkers van persoonsgegevens moeten dit faciliteren, met dreigende boetes die kunnen oplopen tot 4% van de omzet. In de praktijk zijn bijna alle ondernemingen verwerkers van persoonsgegevens. De AVG is in eerste instantie een dwingend kader met strakke tijdlijnen, maar kan ook de aanjager zijn van kansen voor financieel dienstverleners.

Kansen

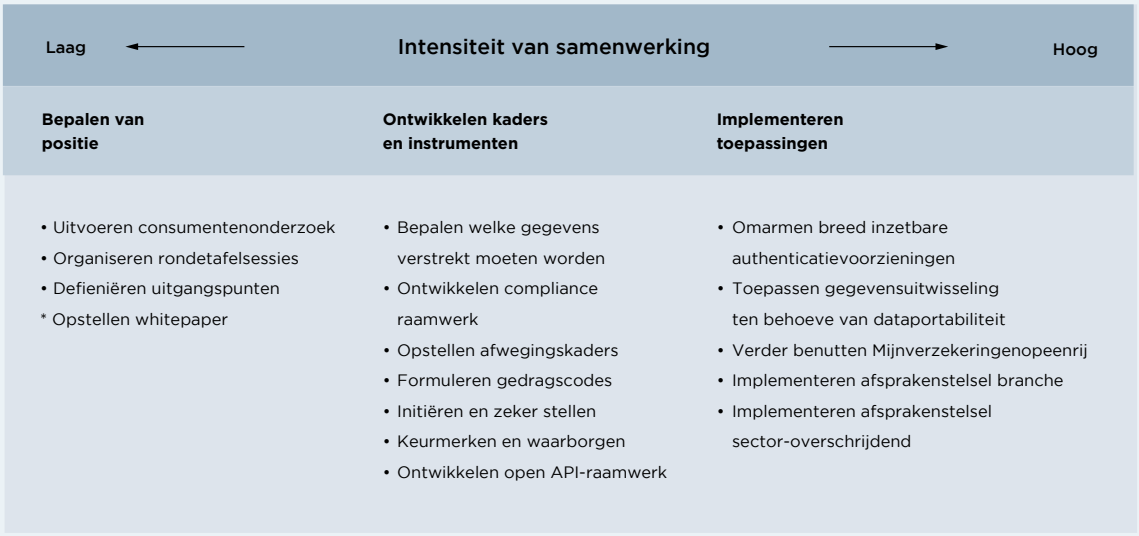
Het AVG betekent onvermijdelijkheden en verplichtingen voor de keten. Maar in het verlengde van de AVG en de diverse marktinitiatieven rond ROPG signaleren we ook kansen voor de verzekeringsbranche:
- voordelen bieden aan de consument;
- vertrouwen herstellen;
- gebruikerservaring verbeteren;
- nieuwe waardeproposities opbouwen;
- drempels verlagen voor advies;
- uitstraling branche verhogen door voorop te lopen in digitale dienstverlening;
- kansen benutten voor samenwerking geformuleerd door de AVG.

Opties voor samenwerking

Samenwerking binnen de keten is één van de strategieën om adequaat te anticiperen op ROPG-ontwikkelingen en van daaruit te vernieuwen. Samenwerking loont:

- ketenactoren vergroten met veel creativiteit de innovatiekracht, capaciteit en vaardigheden van hun ondernemingen;
- ketenactoren zorgen dat de kwaliteit en schaal van hun dienstverlening aan blijven sluiten bij de behoeften en vraag van consumenten;
- het reduceert de kosten in kennis en doorlooptijden;
- niet-competitieve investeringen kunnen partijen gezamenlijk oppakken;
- het levert bewijs dat de verzekeringsbranche als collectief verantwoord zaken doet.

Dit greenpaper onderkent de volgende samenwerkingsopties:



Bij het **bepalen van positie** brengen partijen het inzicht en het overzicht een stap verder, door het maken van keuzes in welke richting de branche zich bij voorkeur wel/niet moet ontwikkelen. Het consumentenonderzoek geeft geen eenduidig en volledig beeld van de vraagkant vanuit de consument ten aanzien van ROPG. Additioneel kwalitatief en kwantitatief onderzoek gericht op ROPG in de verzekeringsbranche biedt een handvat voor het maken van de genoemde keuzes.

Daarnaast is een richtinggevende dialoog nodig tussen de belangrijkste stakeholders. In rondetafelsessies streven we naar een gezamenlijk voordeel, wat leidt tot een gezamenlijk plan voor vervolgacties. In een whitepaper kiezen we nadrukkelijk positie ten aanzien van de vraag hoe de branche omgaat met ROPG.

Kaders ontwikkelen gaat onder andere om het vaststellen van een gemeenschappelijke, afgebakende set gegevens die verzekeraars etc. gaan leveren. Dit creëert duidelijkheid naar de buitenwereld (AP, AFM, consument etc.). Regelgevende en juridische eisen worden steeds strenger, vooral ook vanuit Europa. Hierdoor neemt het belang van een robuust compliance-raamwerk op brancheniveau toe. Een raamwerk maakt interpretatie en toepassingen van wet- en regelgeving vanuit het collectief mogelijk. Verder gaat het om het ontwikkelen van een gemeenschappelijk kader wat toch rekening houdt met de eigen context. Dit kader zorgt dat ketenpartijen op transparante, reproduceerbare wijze een eigen, goed onderbouwde afweging kunnen maken om te voldoen aan de AVG en in te spelen op de kansen. Het kader moet voldoende flexibel zijn om snel in te spelen op nieuwe ontwikkelingen. Iedere organisatie genereert (vroeg of laat) zelf kaders rond ROPG. In dit verband is het de kunst om al deze kaders op elkaar af te stemmen en tot een gezamenlijke opstelling op brancheniveau te komen.

Wat betreft het ontwikkelen van **instrumenten** doelen we vooral op gedragscodes, keurmerken en waarborgen met een richtinggevende, disciplinerende en sturende werking. Ook hier is dialoog en draagvlak op brancheniveau nodig. Een gesloten norm op branche- en ketenniveau ontwikkelen is een optie. Het beschrijft waaraan je minimaal moet voldoen. Hierdoor kan de branche sneller compliant zijn, tegen lagere kosten.

Een open API-raamwerk is toenemend randvoorwaardelijk voor (digitaal) zakendoen.
Het biedt de verzekeringsbranche:

- inzicht in welke functies/services beschikbaar zijn;
- een eenduidige werking over partijen heen, en stelt normen voor beveiliging, authenticatie, performance en beschikbaarheid;
- een goede toegankelijkheid van onlinediensten, ook voor ROPG;
- mogelijkheden voor cocreatie waarbij derden (alleen of in een groep) toepassingen kunnen ontwikkelen op basis van / in het verlengde van aangeboden webservices;
- de kans om een 'vendor en data lock-in' te voorkomen: het ecosysteem wordt niet door één partij bepaald.

Het **implementeren** van werkende **toepassingen** voor ROPG stelt de consument in staat regie te voeren over zijn persoonsgegevens. Adequate authenticatievoorzieningen zijn randvoorwaardelijk. Afhankelijk van de toepassing stellen we requirements op, werken we ze uit in specificaties en starten we ontwikkel-, test-, pilot- en uitroltrajecten. Krachtenbundeling rond het ontwikkelen van toepassingen draagt bij aan verlaging van risico's en kosten enerzijds en versnelling van implementatie anderzijds. Dit alles met inachtneming van ieders commerciële belang. Dit is dus anders dan bij de invoering van afsprakenstelsels waar de uitdagingen liggen op het terrein van het traditionele kip-ei-vraagstuk en het reduceren van complexiteit.

Samenwerking

Samenwerking is natuurlijk van alle tijden, maar is binnen de verzekeringsbranche meer dan vroeger een noodzakelijke randvoorwaarde geworden voor bijvoorbeeld innovatie, marktpositionering en imagoverbetering.

Samenwerking tussen de ketenpartijen wint aan belang naarmate meer sprake is van:
- Non-competitieve thema's;
- Bijdrage aan herstel van vertrouwen van de consument in verzekeraars en intermediairs;
- Bijdrage aan voordeel voor de consument;
- Partij-overstijgende waardecreatie die meerdere ketenschakels raakt;
- Expliciete kwalitatieve en/of kwantitatieve voordelen.

Het thema van dit paper voldoet aan deze criteria en de setting rond het thema beperkt zich niet tot verzekeraars alleen; het is voor alle ketenpartners even waardevol en relevant.

01

Definitie, Scope & Opbouw

Samenwerking is natuurlijk van alle tijden, maar is binnen de verzekeringsbranche meer dan vroeger een noodzakelijke randvoorwaarde voor bijvoorbeeld innovatie, marktpositionering en imagoverbetering. De centrale vraag in dit greenpaper is: welke opties zijn er voor samenwerking binnen de verzekeringsbranche rond Regie Op Persoonsgegevens (ROPG). Dit hoofdstuk licht de sleuteltermen 'samenwerking', 'persoonsgegevens' en 'regie' toe en verduidelijkt de opbouw van dit greenpaper.

1.1 Definitie Regie Op Persoonsgegevens (ROPG)

ROPG is de zeggenschap over en de controle op de verwerking van persoonsgegevens.
Dit zijn de gegevens die via de context terugvoeren naar een natuurlijk levend persoon en de gegevens die de wet aanmerkt als persoonsgegevens:

1. Persoonlijke gegevens
Dit zijn gegevens die betrekking hebben op een persoon, maar niet zomaar een natuurlijk persoon kunnen identificeren. Via context zijn deze gegevens tot een persoon te herleiden.

2. Persoonsgegevens conform de nog te bespreken Algemene Verordening Gegevensbescherming (AVG)
De AVG zorgt voor één Europese wet en vervangt de Nederlandse Wet bescherming persoonsgegevens (Wbp). Het betreft alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. Onder persoonsgegevens vallen onder andere naam, adres, woonplaats, telefoonnummer en geboortedatum.

3. Bijzondere persoonsgegevens
Dit zijn gevoelige gegevens die extra bescherming vereisen. Bijzondere persoonsgegevens zijn bijvoorbeeld: biometrische gegevens, ras, godsdienst, strafrechtelijk verleden en seksuele oriëntatie.

1.2 Scope

De setting rond ROPG beperkt zich niet tot verzekeraars alleen. Dit is een vraagstuk dat voor alle ketenpartijen even waardevol en relevant is. Samenwerking tussen de ketenpartijen wint aan belang naarmate meer sprake is van:

- Non-competitieve thema's;
- Bijdrage aan herstel van vertrouwen van de consument in verzekeraars en intermediairs;
- Bijdrage aan voordeel voor de consument;
- Partij-overstijgende waardecreatie die meerdere ketenschakels raakt;
- Expliciete kwalitatieve en/of kwantitatieve benefits.

ROPG voldoet aan deze criteria. De centrale vraag in dit greenpaper luidt dan ook:
Welke opties zijn er voor samenwerking binnen de verzekeringsbranche rond ROPG?

1.3 Opbouw

Dit greenpaper beschouwt de ontwikkelingen en opties rond ROPG vanuit het perspectief van de particuliere consument die een verzekeringsproduct afneemt. Hierbij nemen we de volledige keten in ogenschouw. Zzp'ers en werknemers blijven buiten beschouwing.

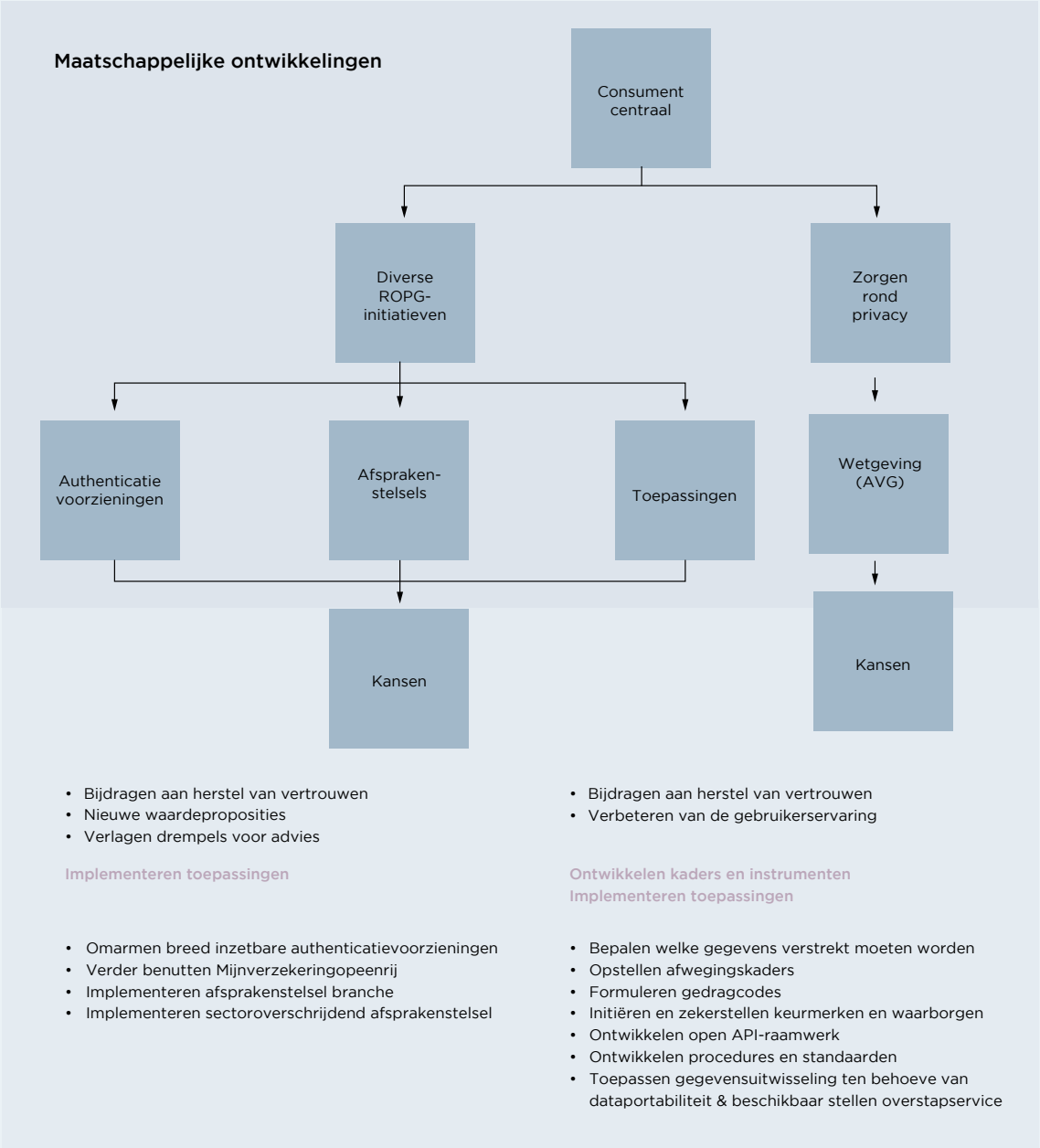
De vraag "Welke opties zijn er voor samenwerken rond ROPG binnen de verzekeringsbranche?" werken we uit in drie delen:

1. Het eerste deel biedt een overzicht van het werkgebied ROPG vanuit meerdere perspectieven:
   - de positie/rol van de consument;
   - bestaande ROPG-initiatieven;
   - het wettelijk kader.

2. Het tweede deel identificeert de kansen rond ROPG. Deze liggen in het verlengde van de bestaande ROPG-initiatieven.

3. Het derde deel staat stil bij de opties voor samenwerking. Hierbij staat de consument uit het eerste deel centraal en anticiperen we op de kansen uit het tweede deel.

Figuur-1 geeft de rode draad van dit greenpaper weer.



02

ROPG en de consument

Hoe kijkt de consument zelf aan tegen ROPG? Juist bij ROPG is de rol van de consument uitermate belangrijk. De consument staat namelijk centraal bij het voeren van regie. De reacties op eerdere uitingen van financieel dienstverleners over het inzetten van persoonlijke gegevens voor het verbeteren van dienstverlening, tonen aan dat het een uiterst gevoelig thema is. Tegelijk bestaat maar weinig onderzoek over hoe de consument aankijkt tegen het delen van persoonlijke gegevens en de rol van diverse partijen daarin.

2.1 De mening van de consument verandert

Wat de consument voor ogen heeft als het gaat om ROPG blijkt bepaald geen statisch gegeven. De mate waarin gerelateerde onderwerpen het nieuws halen, heeft bijvoorbeeld invloed op de meningsvorming. Zo was er in 2016 veel media-aandacht voor (persoons)gegevens. WhatsApp bleek gegevens te delen met Facebook. Ook kwamen slimme poppen op de markt die stemdata van kinderen opnamen en doorverkochten aan adverteerders. Daarnaast maakte de Autoriteit Persoonsgegevens in december 2016 bekend dat er bijna 5500 meldingen binnenkwamen sinds de invoering van de meldplicht datalekken op 1 januari 2016.

De mening van de consument verschilt aanzienlijk per situatie. Afhankelijk van de diensten of eventuele vergoedingen die bedrijven in ruil bieden, heeft de consument een andere instelling. Dit geldt ook voor het type gegevens waar bedrijven om vragen. In de huidige samenleving vinden consumenten het bijvoorbeeld normaal om hun naam en e-mailadres te pas en te onpas achter te laten voor uiteenlopende doeleinden; dit geldt echter niet voor financiële en medische gegevens.

2.2 De consument staat open voor ROPG

Beschikbaar onderzoek laat zien dat er wel degelijk een markt voor ROPG is, mits onder de juiste voorwaarden. Het vergroten van bewustzijn (over veiligheid en privacy) onder consumenten is een belangrijke randvoorwaarde. Het is opvallend dat men in Nederland niet zomaar veel waarde hecht aan het zelf verkopen van data. Het delen van data doen consumenten met verschillende partijen en met verschillende beweegredenen. Een basis van vertrouwen is van belang. Het speelt daarmee een veel grotere rol dan het krijgen van geld of een dienst voor de gegevens.

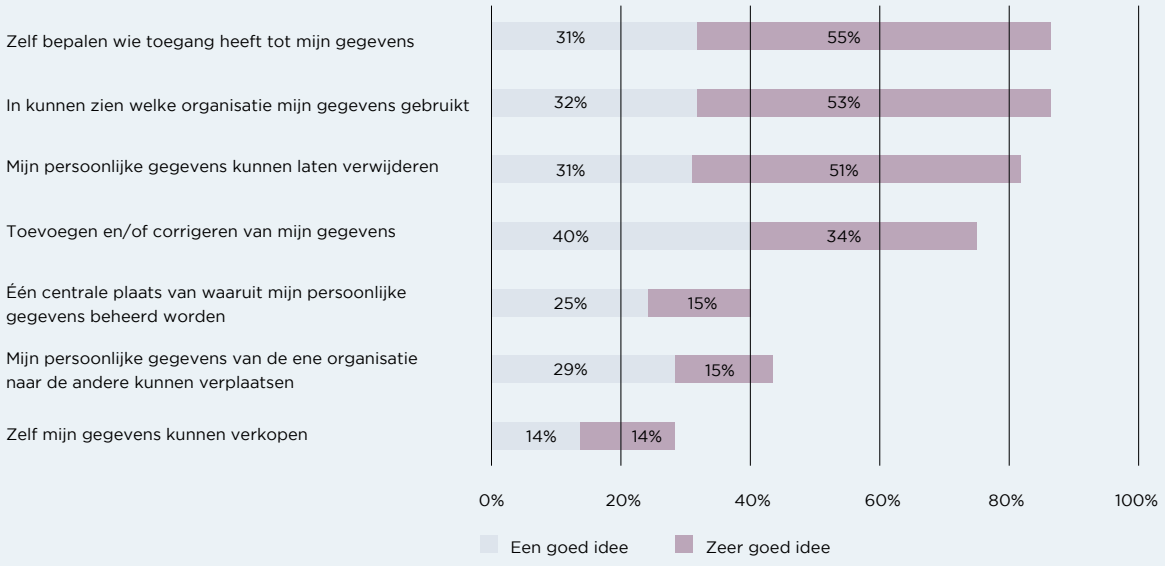
Relatief veel consumenten wensen vanwege gemak één persoonlijke onlineomgeving voor alle verzekeringspolissen. De consument heeft een duidelijke behoefte aan een totale digitale financiële administratie, mits hij zelf kan bepalen welke informatie wel en niet beschikbaar is.

Om te bepalen hoe Nederland tegenover persoonlijke data staat, heeft InnoValor in 2015 door Newcom Research & Consultancy onderzoek laten doen naar de mening van de consument. De basisvraag is of mensen open staan voor ROPG als concept. Een ruime meerderheid (57%) van de ondervraagden

geeft aan waarschijnlijk of zeker gebruik te maken van een dienst waarmee je persoonlijke gegevens kunt beheren. Daarnaast geeft minder dan een kwart (23%) van de respondenten aan vrijwel zeker geen gebruik te willen maken van genoemde dienst. Dit betekent dat er wel degelijk een markt voor ROPG is, mits onder de juiste voorwaarden.

De gevoelens bij gegevensbeheer zijn wat latenter. Bij het beheer van data vanuit een centrale plaats (via een persoonlijke dienst, aangeboden door een organisatie) hebben ondervraagden nog weinig associaties. Ze noemen de woorden veiligheid en privacy, maar verder heeft men hier nog geen idee bij. Dit betekent dat voor het succes van nieuwe diensten rondom (het beheer van) persoonlijke data vooral het vergroten van bewustzijn onder consumenten een belangrijke randvoorwaarde is.

Figuur-2 geeft een beeld van de behoeften van de Nederlandse consument met betrekking tot regie. Opvallend is dat men in Nederland weinig waarde hecht aan het zelf verkopen van data, terwijl volgens onderzoek van Deloitte in de UK 47% van de respondenten besparingen zag als een reden om data te delen.

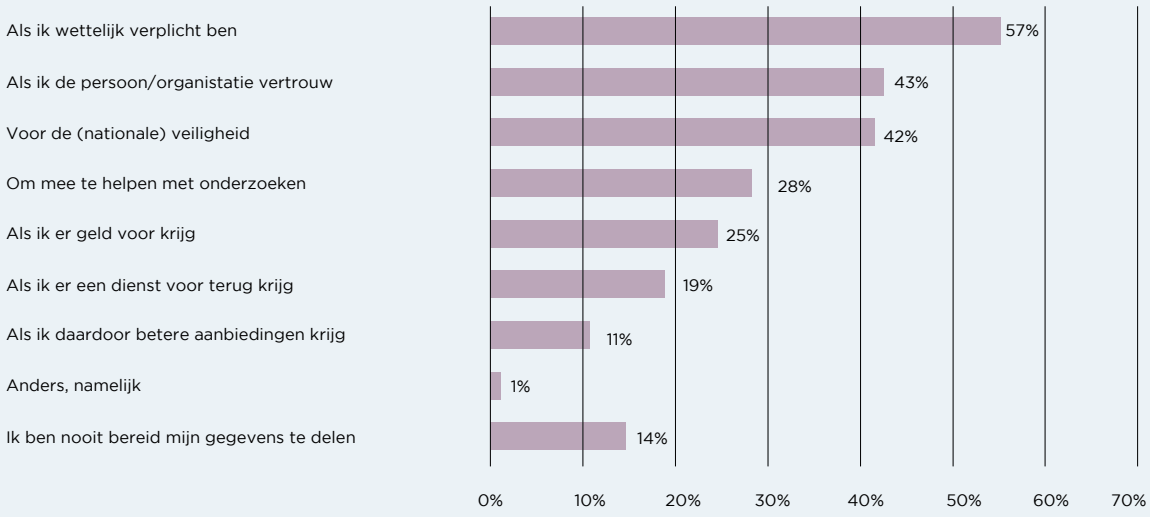


Figuur-2 – Waar liggen de behoeftes?

Cijfers van het CBS bevestigen dit. 69% van de respondenten gaf aan dat zij zich verzekeren dat de gegevens niet voor commerciële doeleinden gebruikt mogen worden wanneer zij gegevens achterlaten op internet.

2.3 Vertrouwen en regie belangrijkste voorwaarden voor consument

Het delen van data doen consumenten met verschillende partijen en met verschillende beweegredenen. Een basis van vertrouwen is van belang: volgens figuur-3 zou 43% van de Nederlanders gegevens delen als ze een organisatie vertrouwen. Het speelt daarmee een veel grotere rol dan het krijgen van geld of een dienst voor de gegevens. Een behoorlijk deel (14%) van de Nederlanders is helemaal niet bereid om persoonlijke gegevens te delen. Het zal altijd lastig blijven om deze groep te verleiden tot gebruik van een dienst wanneer ze daar persoonlijke gegevens voor moeten delen.



Figuur-3 – Bereidheid tot delen van gegevens onder bepaalde voorwaarden

Een onderzoek van TNO naar het beheren en delen van persoonsgegevens bevestigt de ondergeschikte behoefte van het verkrijgen van een dienst of geld in ruil voor gegevens. TNO geeft aan dat 40% van de respondenten zich ongemakkelijk voelt bij het delen van gegevens voor gratis diensten, tegenover 20% die het prima vindt (19% in het onderzoek van Innovalor).

Volgens recent onderzoek van Gfk is 12% van de Nederlanders bereid om persoonlijke gegevens over onder andere hun gezondheid, financiën en energieverbruik te delen in ruil voor een beloning of lagere kosten. 30% van de Nederlanders is hiertoe niet bereid. De exacte positie van de resterende 58% is onduidelijk.

Een onderzoek specifiek in de gezondheidssector schetst een ander beeld. Uit de 'Smart health monitor' blijkt dat consumenten in Nederland ervoor openstaan om gezondheidsdata te delen met commerciële organisaties, mits daar een vorm van beloning tegenover staat. 45% van de respondenten geeft aan bereid te zijn om gezondheidsdata met zorgverzekeraars te delen in ruil voor korting op de zorgpremie. Er is wat voor te zeggen dat dit ook zal gelden voor andersoortige verzekeringen. Ook is het interessant om te zien dat het draagvlak vooral groot is onder jongeren (59% van de respondenten tussen 18-35 jaar). Dit is in lijn met een onderzoek onder jongvolwassenen (18-25 jaar) naar digitaal vertrouwen. Hierbij geeft 37% als voornaamste reden aan gegevens te willen delen indien er voldoende eigen voordelen aan verbonden zijn.

73% geeft aan één persoonlijke onlineomgeving te willen voor alle verzekeringspolissen vanwege het gemak. Een ander onderzoek toont ook aan dat 54% van de respondenten een duidelijke behoefte heeft aan een totale digitale financiële administratie. Dit houdt in dat je financiële gegevens uit verschillende 'mijn omgevingen' in één overzicht kunt raadplegen. Een grote groep geeft echter haar zorg aan over het waarborgen van de privacy.

Daarnaast is het voor de consument van belang om zelf de regie te voeren over een dergelijke administratie. Dit houdt in dat hij zelf kan bepalen welke informatie wel en niet beschikbaar is. Consumenten willen ook zelf iedere keer opnieuw toestemming geven voor de verwerking van de gegevens. In 2015 kwam uit een Europees onderzoek onder 28.000 burgers ook al naar voren dat slechts 15% het gevoel had volledige controle te hebben over zijn persoonlijke gegevens die online waren gedeeld. Bovendien blijkt uit datzelfde onderzoek dat bedrijven gegevens gebruiken voor andere doelen dan waarvoor ze deze gegevens verzamelden. Dit is in ieder geval een zorg die 70% van de ondervraagden deelt. Daar staat tegenover dat eenzelfde percentage begrijpt dat het verschaffen van data onderdeel is van de huidige samenleving. Consumenten accepteren dat er (vaak) geen alternatief is dan alleen het verstrekken van gegevens voor het afnemen van bepaalde producten of diensten.

ROPG-initiatieven in de markt

De grootschalige beschikbaarheid van persoonsgegevens als gevolg van het gebruik van internet en dataopslag creëert zorg onder consumenten over hoe bedrijven met deze gegevens omgaan. Tegelijkertijd biedt de beschikbaarheid van gegevens enorme mogelijkheden, zoals meer efficiëntie en maatwerk in de dienstverlening voor consumenten. De laatste jaren kwamen verschillende initiatieven op in Nederland en buitenland. Initiatieven die zorgen dat consumenten de voordelen van ROPG ervaren, en vertrouwen geven over de opslag en juiste toepassing van hun persoonsgegevens. Deze initiatieven verschillen qua opzet en eigenschappen maar zijn allemaal gericht op het in enige mate kunnen voeren van regie. Dit hoofdstuk geeft een overzicht van verschillende initiatieven in de markt, waarbij het accent ligt op de veranderingen in consumentenbelang. Dit greenpaper bespreekt de belangrijkste initiatieven. De indeling van de initiatieven is:

1. Authenticatievoorzieningen
2. Afsprakenstelsels
3. Toepassingen

3.1 Authenticatievoorzieningen

Authenticatie is het proces dat nagaat of een consument daadwerkelijk is wie hij beweert te zijn, dat wil zeggen: daadwerkelijk de identiteit bezit die hij opgeeft. Dit is relevant, want ROPG is alleen mogelijk als voldoende zeker is of een persoon daadwerkelijk is wie hij beweert te zijn. Vervolgens stelt het vast of die consument ook gerechtigd is om de gewenste service af te nemen. Dit noemen we autorisatie en is nadrukkelijk een op de authenticatie volgende, aparte stap. De geauthenticeerde identiteit is dus nodig voor het verrichten van autorisatie.

3.1.1 De belangrijkste voorzieningen

De gangbare route is op dit moment dat een organisatie zelf voorzieningen voor authenticatie inricht. De voorkeur van consument en aanbieders van online diensten gaat steeds meer uit naar authenticatiemiddelen die een consument breed kan gebruiken. De overheid loopt hier met DigiD in voorop. Steeds meer authenticatievoorzieningen komen in dit verband beschikbaar. Onderstaande tabel benoemt de meest relevante.

Voorziening	Toepassingsdomein	Zwakke/sterke authenticatie
DigiD (NL)	Publiek Privaat (publieke taken)	Sterk (indien sprake is van twee-factor-authenticatie)
Idensys	Publliek	Betrouwbaarheidsniveau wordt bepaald door dienstaanbieder
IDIN (NL)	Publiek/privaat	Sterk
Facebook Google LinkedIn Twitter	Privaat	Zwak

DigiD is een publiek authenticatiemiddel en voor de verzekeringsbranche alleen inzetbaar voor ziektekosten en collectief pensioen.

Branchebrede authenticatievoorzieningen zoals Idensys en iDIN beloven dat de consument met een beperkt aantal inlogmiddelen bij alle dienstverleners kan inloggen op een acceptabel betrouwbaarheidsniveau. Betrouwbaarheid en consumentengemak zijn voor ROPG cruciaal.

Idensys is het publiek-private Nederlandse systeem voor elektronische identificatie. Rondom Idensys heerst vooral nog veel onzekerheid. Als Idensys groen licht krijgt van de Tweede Kamer, dan vindt uitrol naar verwachting pas in 2018 plaats. Verder is voorlopig nog geen zekerheid over de economische levensvatbaarheid van het stelsel (vooral voor het private domein), laat staan over de toekomstige prijsstelling.

iDIN is een online identificatiemiddel waarvoor banken verenigd in Betaalvereniging Nederland in 2016 groen licht gaven. Dit betekent dat consumenten met hun bestaande bancaire inlogmiddelen vanaf 2017 ook kunnen inloggen bij andere dienstverleners. De gegevensset bestaat uit voorletter(s), achternaam, woonadres, leeftijdsindicatie (18 jaar of ouder), geboortedatum, geslacht, e-mailadres en/of telefoonnummer. De aanbieder van een dienst die iDIN inzet, kan aangeven welke gegevens nodig zijn, de consument bepaalt of ze deze ook mag vrijgeven.

Het perspectief voor de verzekeringssector: in 2017 kunnen alle Nederlanders met hun bancaire authenticatiemiddelen inloggen (iDIN) bij dienstverleners onder de voorwaarde dat die dienstverleners dit mogelijk maken door een aansluiting op iDIN.

SIVI verwacht dat de komende jaren in toenemende mate branchebrede authenticatievoorzieningen beschikbaar komen. Verzekeraars, service providers en intermediairs gaan gebruik maken van Digital Identity Service Providers die de consument meerdere inlogopties aanbieden. De analogie met betalen via internet is evident; de consument bepaalt met welk middel ze betaalt. Hier zijn het de Payment Service Providers die bedrijven online betaaloplossingen bieden als iDEAL, PayPal, creditcards, incasso's en overschrijvingen.

Het betrouwbaarheidsniveau van het inloggen via social media kun je verhogen door koppelingen te maken met bestaande accounts. Voorwaarde is wel dat het betrouwbaarheidsniveau van het registratie- en authenticatieproces voor deze bestaande accounts voldoende hoog is. Aegon koppelt gebruikersnaam en wachtwoord van het socialmedia-account aan het (veiliger) Aegon-account en een 5-cijferige pincode. Inloggen bij Aegon kan daarna via Facebook en het opgeven van de genoemde pincode.

3.1.2 Sovrin

Blockchain ('keten van blokken') is een digitaal boek of database met opslag en verificatie van transacties zodat bedrog onmogelijk is. Blockchain is ook een mogelijk authenticatiemiddel, aangezien de technologie veel interessante mogelijkheden voor een transparant beheer van toestemmingsverklaringen biedt. Sinds kort bestaat de onafhankelijke stichting Sovrin om soevereine identiteiten op basis van

een wereldwijd Blockchain-ecosysteem te creëren. De aanname van een soevereine identiteit is dat elk individu in de wereld recht heeft op toegang tot een identiteit die men erkent op mondiaal niveau, en die onafhankelijk is van een overheidsorganisatie of private partij. Deelnemers valideren hierbij elkaars informatie uit een identiteit, zoals naam, geboortedatum of nationaliteit.

Een dienstverlener kan de eigenaar van een Sovrin-identiteit om zulke informatie vragen. Bij toestemming geeft de eigenaar de dienstverlener toegang tot die gegevens. Deze is dan in staat om te controleren of de uitgever van de identiteitsgegevens deze gegevens digitaal heeft ondertekend. Vervolgens legt ze in de Blockchain de toestemming vast en de informatie dat de gegevens zijn gedeeld, door wie, aan wie, om welke reden en met welke beperkingen.

3.2 Afsprakenstelsels

iDEAL en GSM zijn aansprekende voorbeelden van afsprakenstelsels voor betalen en mobiel telefoneren. Voordelen voor de consument:

- Ze kan van aanbieder veranderen;
- Ze kan zelf bepalen via welke bank ze betaalt;
- Ze kan met iedereen bellen.

Op het terrein van ROPG zijn ook afsprakenstelsels in ontwikkeling. De kracht van deze afsprakenstelsels is dat de gegevens bij de bron blijven staan en dat er geen sprake is van insluiting door leveranciers. Meerdere leveranciers geven namelijk invulling aan de rollen die het afsprakenstelsel onderkent. De meeste afsprakenstelsels kennen privacy en dataminimalisatie als basisbeginselen. Dataminimalisatie houdt in dat je alleen gegevens verwerkt die relevant zijn voor het doel van de verwerking.

Een afsprakenstelsel voor ROPG kan sectoronafhankelijk zijn. Dit is een **horizontaal afsprakenstelsel**. Qiy is een voorbeeld waarmee Aegon en Intrasurance binnen de financiële sector experimenteren. Ook de overheid voert in het kader van het programma Regie op Gegevens momenteel verkenningen uit ten aanzien van Qiy. Sectoren kunnen echter ook kiezen voor een eigen uitwerking van een afsprakenstelsel. Dit is een **verticaal afsprakenstelsel**. De zorg kiest bijvoorbeeld voor een eigen afsprakenstelsel voor het Persoonlijk GezondheidsDossier (PGD).

Hieronder bespreken we de meest bekende afsprakenstelsels. De praktische toepassing van deze stelsels staat nog in de kinderschoenen.

3.2.1 Respect Trust Framework

Het Respect Trust Framework is een convenant voor het juist omgaan met persoonlijke informatie. Het convenant richt zich vooral op de samenwerking (data-uitwisseling) tussen partijen, maar een individuele partij kan het ook toepassen.

Het convenant kent vijf basisprincipes:

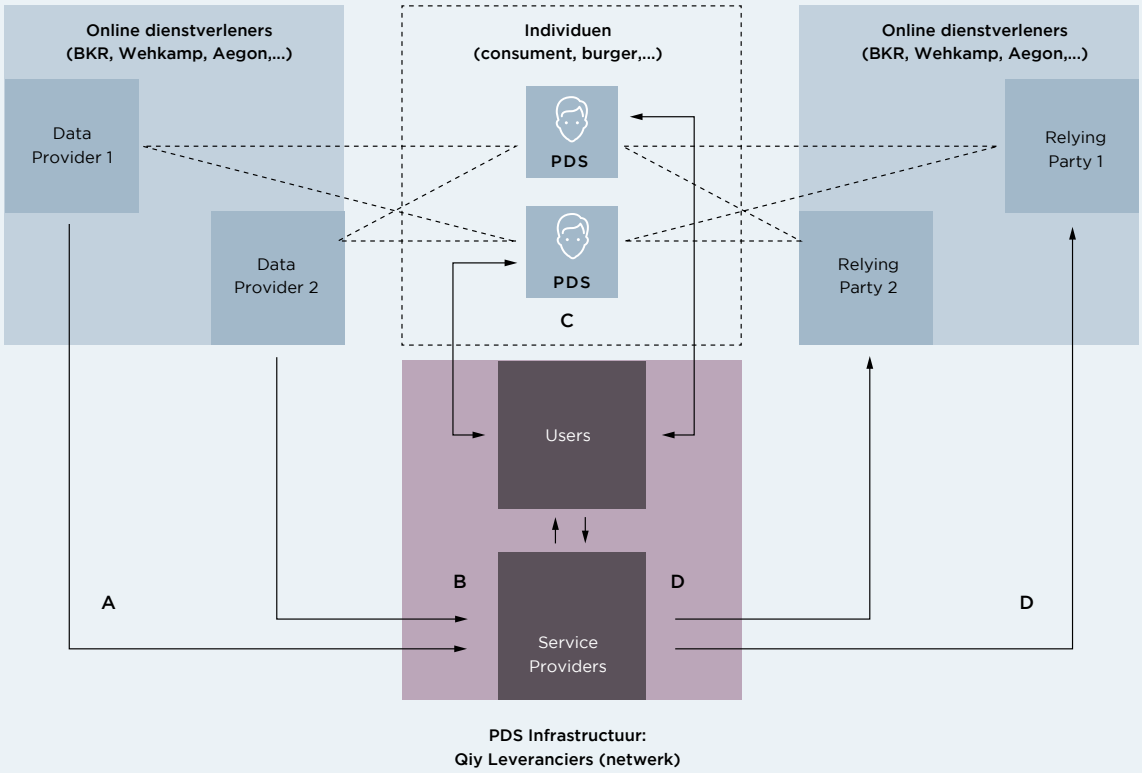
1. Promise: we will respect each other's digital boundaries;
2. Permission: we will negotiate with each other in good faith;
3. Protection: we will protect the identity and data entrusted to us;
4. Portability: we will support other Members' freedom of movement;
5. Proof: we will reasonably cooperate for the good of all Members.

Het "Respect Reputation System" werkt de interpretatie van het convenant uit voor het samenwerken tussen partijen. Het "Respect Business Framework" werkt de interpretatie van het convenant uit voor te hanteren businessmodellen bij het aanbieden van diensten. Het uiteindelijke idee is dat een gebruiker op internet zich kan bedienen met – of zich kan beperken tot – een verzameling van diensten die het convenant volgen.

3.2.2 Qiy

Qiy werkt vanuit het principe dat de consument toestemming geeft voor een specifieke gegevensuitwisseling en belooft de consument digitale zelfbeschikking. Via de persoonlijke Qiy Node beschikt het individu over de eigen gegevens en regelt hij zelf voor wie die gegevens beschikbaar zijn. Dit wordt mogelijk gemaakt via apps gebaseerd op het Qiy Afsprakenstelsel. Qiy voldoet aan de Europese data-wetgeving die vanaf mei 2018 geldt.

Figuur-4 maakt de rol die de verschillende partijen spelen binnen het Qiy Netwerk inzichtelijk.



Figuur-4 - Uitwisseling van persoonsgegevens via het Qiy Netwerk

De infrastructuur van Qiy bestaat uit een flexibel en schaalbaar netwerk van concurrerende leveranciers, met vrije toetreding. Daarbij maken we onderscheid tussen leveranciers die Qiy-domeinen uitgeven aan individuen (Issuers) en leveranciers die online dienstverleners aansluiten op het Qiy Netwerk (Service Providers). Bovendien maken we onderscheid tussen online dienstverleners die data aanleveren (Data Providers) en online dienstverleners die data ontvangen (Relying Parties). In de praktijk zullen veel online dienstverleners beide rollen aannemen.

Qiy timmert al meer dan tien jaar aan de weg. Ondanks de vele aandacht blijft het aantal toepassingen op basis van het Afsprakenstelsel zeer beperkt. Voor Qiy is er één door een marktpartij geleverde applicatie beschikbaar, maar deze applicatie behelst niet het gehele Qiy-gedachtegoed. Voor een aantal aspecten moet uit pilots nog blijken hoe implementaties gebaseerd op Qiy presteren; dit geldt onder andere voor de criteria prestaties, technische schaalbaarheid en stabiliteit.

3.2.3 MedMij

Diverse partijen in de zorg, waaronder de beroepsverenigingen van huisartsen, ziekenhuizen en De zorg werkt aan het programma 'Meer regie over gezondheid' ('MedMij'). De volgende partijen werken hierin samen: de beroepsverenigingen van huisartsen, ziekenhuizen en apothekers, de Patiëntenfederatie en de overheid. MedMij wil in de toekomst zorgen dat de consument de regie voert over zijn persoonlijke gezondheidsomgeving. Een persoonlijke gezondheidsomgeving is een digitale omgeving die een consument in staat stelt om zijn relevante gezondheidsgegevens overzichtelijk en veilig in te zien, aan

te vullen met zelf gegenereerde gegevens en te delen met wie hij wil. Ook als deze verspreid staan opgeslagen bij zorgaanbieders en overheden. In 2016 werkte het programma uit welke afspraken, standaarden en basiseisen nodig zijn voor het gebruiksvriendelijk, veilig en betrouwbaar uitwisselen van gezondheidsinformatie. Het afsprakenstelsel MedMij wil voorkomen dat een leverancier van een persoonlijke gezondheidsomgeving met alle zorgaanbieders en overheden afzonderlijk afspraken moet maken.

Op dit moment zijn de eerste apps en websites in ontwikkeling die consumenten in staat stellen om gegevens over medicatie, allergieën en laboratoriumresultaten in te zien bij aangesloten organisaties, en deze te delen met anderen.

3.3 Toepassingen

Hierna volgt een overzicht van verschillende toepassingen in de markt, waarbij het accent ligt op ROPG en de veranderingen in consumentenbelang. Het gaat hierbij iedere keer om een toepassing van één leverancier/partij. Dit is het grote verschil met afsprakenstelsels. Hierbij is altijd sprake van meerdere leveranciers die de dataproviders, dienstverleners en consumenten bedienen, waardoor geen sprake is van insluiting. We bespreken alleen de bekendste en belangrijkste toepassingen. Daar waar meer over bekend is, bespreken we ook de kracht en de nadelen.

3.3.1 DataPlaza

DataPlaza is een complete omgeving die ROPG faciliteert. De consument kan via DataPlaza kosteloos een digitale kluis aanmaken in een soort digitale notaris-omgeving. Hij krijgt toegang na het verkrijgen van een NotarisID. Voor een NotarisID gaat de consument met een identiteitsbewijs fysiek naar de notaris, die zijn persoonsgegevens vastlegt. Daarna krijgt de consument een gebruikersnaam en wachtwoord waarmee hij zich kan authenticeren bij dienstaanbieders als DataPlaza. Dienstaanbieders stellen vervolgens enkel controlevragen (ouder dan 18? etc.) en maken expliciet waarvoor de gegevens gebruikt worden. Hierdoor realiseert het dataminimalisatie en doelbinding. Consumenten kunnen via DataPlaza onder de noemer Digitale Erfenis digitale wachtwoorden en inlogcodes bewaren. Met toestemming van de consument kunnen derden, bijvoorbeeld na het eigen overlijden, van deze data gebruikmaken. Notarissen promoten DataPlaza. Over het aantal gebruikers en het exacte gebruik is weinig bekend.

3.3.2 Financieel Paspoort

Het Financieel Paspoort is een decentraal ROPG-platform dat zich richt op het verkrijgen en verstrekken van gegevens uit een grote verzameling van bronsystemen. Het slaat gegevens niet centraal op; de consument kan deze gegevens op eigen apparatuur opslaan en/of deze gegevens verstrekken aan derden. Ten aanzien van opslag en verstrekking ligt de regie bij de consument.

Doelstelling van de achterliggende Stichting Financieel Paspoort is:

- consumenten overzicht bieden over financiële zaken van nu en in de toekomst, betreffende sparen, lenen, verzekeren, huis en hypotheek, sociale zekerheid, beleggingen en pensioen.
- consumenten de regie geven over de verstrekking van deze informatie aan derden, ten behoeve van bijvoorbeeld advies of het verkrijgen van een hypotheek.

Het Financieel Paspoort zit nog in de ontwikkelingsfase.

3.3.3 Only Once

Only Once is een Nederlandse startup met internationale ambities en biedt de consument een ROPG-omgeving. Binnen deze omgeving onderhoudt de consument zijn profiel en bepaalt hij wie welke gegevens en documenten mogen raadplegen (vergelijkbaar met bijvoorbeeld Dropbox). Het initiatief richt zich onder andere op zzp'ers, die veel informatie moeten delen om een opdracht op te starten. Zodra deze gegevens wijzigen, ontvangt de 'abonnee' de gewijzigde data. Only Once is nog niet breed uitgerold.

3.3.4 Mydex

Een Engels voorbeeld van een ROPG-initiatief is Mydex. Mydex is actief vanaf 2007. Consumenten kunnen met Mydex persoonsgegevens beheren en hergebruiken op een effectieve en veilige manier. Organisaties als woningbouwverenigingen, energiemaatschappijen en mobiele-telefonie-aanbieders gebruiken Mydex om hun klanten een klantmap aan te bieden. De consument heeft via de klantmap toegang tot zijn (persoons)gegevens, terwijl de organisatie meer garanties over actuele klantinformatie zoals adres en telefoonnummer heeft. Over het precieze gebruik van Mydex is echter weinig bekend.

3.3.5 DataCoup

DataCoup is een Amerikaans bedrijf en voorziet in een ROPG-omgeving. Het is een marktplaats waar individuen hun persoonsgegevens, zoals socialmedia-activiteit of creditcardtransacties, kunnen verhandelen tegen een maandelijkse beloning. Nadat een consument selecteert welke data hij wil verhandelen en met wie, laat DataCoup zien wat de waarde van die data is. Het combineert de data met de data van andere DataCoup-gebruikers, geanonimiseerd en geaggregeerd tot algemene datasets. DataCoup verkoopt deze datasets aan afnemers als datamakelaars, adverteerders en marketeers. De gebruikers ontvangen hiervoor in ruil een maandelijkse beloning die zij kunnen verzilveren in DataCoup. Over het gebruik van DataCoup is weinig bekend.

3.3.6 IRMA

IRMA (I Reveal My Attributes) is een samenwerking tussen Radboud Universiteit Nijmegen, Stichting Internet Domeinregistratie Nederland, Tilburg Institute of Law, Technology and Society en TNO. IRMA is een techniek die privacygegevens afschermt en zich volledig inzet op dataminimalisatie. Het belangrijkste kenmerk is dat de gebruiker nooit meer informatie toont dan op een bepaald moment op een bepaalde plek nodig is. IRMA draait om een NFC-smartcard die je kunt gebruiken in winkels en via een reader online. De gebruiker legitimeert zich in winkels en bij organisaties met de kaart (authenticatie) en deelt attributen als leeftijd en banknummer. IRMA zit nog in de pilotfase.

3.3.7 OpenPDS

OpenPDS is een door MIT ontwikkelde open-source-architectuur voor Personal Data Store-toepassingen. Het biedt een ROPG-omgeving aan consumenten en stelt ze in staat om hun data te verzamelen, op te slaan en fijnmazige toegang aan anderen te geven.

Interessant aan de OpenPDS:

- Dataminimalisatie: het levert niet noodzakelijk de feitelijke data, maar bij voorkeur de afgeleide data als “ik ben ouder dan 18” in plaats van geboortedatum.
- Het richt op de zogenaamde ‘observed’ en ‘inferred’ data. Dit zijn data die een consument niet actief zélf deelt, maar worden afgeleid uit diens gedrag (bijvoorbeeld gps-data, surfgedrag, enzovoort). De consument zet een OpenPDS-app op zijn telefoon, die als een soort schil om alle data inclusief sensoren als GPS heen zit. Andere apps kunnen dan via SafeAnswers-modules gerichte vragen stellen. Zonder OpenPDS heeft bijvoorbeeld een camera-app toegang tot de locatiegegevens, maar een OpenPDS-gebruiker zou bijvoorbeeld kunnen instellen dat die app via OpenPDS alleen te weten krijgt of hij op dit moment in de omgeving van zijn huis is of niet.
- Eén van de weinige systemen die zich ook richt op niet rechtstreeks door de consument zelf verstrekte data.

OpenPDS zit nog in de ontwikkelfase.

3.3.8 MijnOverheid

MijnOverheid is de persoonlijke omgeving voor overheidszaken en draagt de belofte in zich van een ROPG-omgeving. De burger ziet hier welke gegevens bij de overheid bekend zijn over werk, AOW-pensioen, huis, auto en studie. De burger vindt na inloggen op MijnOverheid zijn persoonlijke Berichtenbox. Hiermee kan de burger post van de overheid digitaal ontvangen. Als de burger een bericht in zijn Berichtenbox ontvangt, kan hij daarvan automatisch een melding krijgen via e-mail. Zes miljoen Nederlanders maken gebruik van dit portaal, 35 pensioenfondsen leveren via MijnOverheid uniforme pensioenoverzichten aan deelnemers. De Belastingdienst, de Sociale Verzekeringsbank, het

UWV, de RDW en ruim honderd gemeenten sturen berichten via deze onlinedienst.

De nadelen van Mijn Overheid:
- Het is nu nog geen echte personal data manager, omdat het enkel eenrichtingsverkeer vanuit overheidsinstanties faciliteert. Het is vergelijkbaar met een digitale postbus.
- Mijn Overheid corrigeert geen fouten in de ontvangen gegevens. Dit wordt pas vanaf 2018 mogelijk. Dan krijgt de burger meer regie over gegevens die hij bij de overheid opslaat.

3.3.9 Dappre

Dappre is een mobiele app voor het beheer van contacten en het delen van persoonlijke contactgegevens. De app is ontwikkeld door Digital Me en gebaseerd op het afsprakenstelsel van Qiy. Het biedt de consument vanuit een veilige online gebruikersomgeving overzicht en controle over zijn persoonlijke contactgegevens. Aegon en Intrasurance maken gebruik van Dappre.

3.3.10 TNO TrustTester

TNO TrustTester is een heel andere invulling rond ROPG. Het volgt het zelfde spoor als OpenPDS en IRMA. Het gaat uit van het principe dat het organisaties niet om de informatie zelf gaat: ze willen alleen weten of een bepaalde claim correct is. De bank wil bijvoorbeeld niet exact weten hoeveel de consument verdient, maar of hij inderdaad genoeg verdient voor de gewenste hypotheek. De bank is meer geholpen met een simpel en definitief 'ja' dan met een salarisstrook die je ook nog eens op waarheidsgehalte moet controleren.

De kracht van TNO TrustTester:

- Het valideert een bewering en voorziet die bewering van een digitaal stempel waarop de ontvanger kan vertrouwen.
- De validerende partij krijgt niet te zien van welke partij de aanvraag komt. Het UWV krijgt bijvoorbeeld niet te zien dat de vraag "verdient >1000?" van een werkgever, bank of dergelijke komt. Sterker nog, het UWV ziet zelf niet eens de uitkomst van de validatie, door de 'homomorfe encryptie' die TrustTester gebruikt.
- TNO TrustTester gaat opvallend ver op het gebied van dataminimalisatie en anonimisatie.

In 2017 volgen pilots voor TNO TrustTester.

04

Wettelijk kader

In het vorige hoofdstuk zagen we hoe diverse initiatieven in de markt het belang van consumenten en burgers rond ROPG dienen. Ook de overheid zit op het terrein van ROPG niet stil. Het belang van de consument staat hierbij voorop: het borgen van privacy, het uitoefenen van controle, het voorkomen van handel in persoonsgegevens en concentratie van macht bij spelers als Google en Facebook.
Dit hoofdstuk licht toe hoe de wetgever inspeelt op ROPG. Hiervoor bespreken we eerst de relevante wet- en regelgeving en adviezen/richtlijnen. Daarna zoomen we kort in op de spelers die kaders zetten, toezicht houden en invloed uitoefenen.

Voor een goed begrip van de context is het vooral belangrijk te weten dat vanaf 25 mei 2018 de Algemene Verordening Gegevensbescherming (AVG) van toepassing is. Dit is een nieuwe (ingrijpende) Europese wetgeving voor de bescherming van persoonsgegevens. Deze nieuwe wetgeving stelt de consument centraal en in staat om regie te voeren over zijn persoonsgegevens; de consument bepaalt.
De AVG vervangt de Wet bescherming persoonsgegevens en de Richtlijn bescherming persoonsgegevens. Deze wetgeving staat centraal in dit hoofdstuk, omdat het grote impact heeft. AVG bakent ROPG nader af. De belangrijkste bepalingen die relevant zijn voor de verzekeringsbranche komen daarna aan de orde, en tot slot de verantwoordelijkheden in de keten.

4.1 Wet- en regelgeving en adviezen/richtlijnen op het terrein van privacy

4.1.1 Directe wet- en regelgeving

Verschillende regelingen zijn van toepassing op het gebied van privacy met betrekking tot persoonsgegevens. Hieronder volgen de belangrijkste omtrent de bescherming van persoonsgegevens.

Wet Bescherming Persoonsgegevens (Wbp)
Deze wet implementeert de Europese Richtlijn Bescherming Persoonsgegevens (Directive 95/46/EG). Deze wet zal gelden tot 25 mei 2018 in Nederland.

Algemene Verordening Gegevensbescherming (AVG)
Eén van de grootste veranderingen in het privacy-landschap is de invoering van de zogeheten General Data Protection Regulation (GDPR). Dit is een nieuwe Europese wetgeving voor de bescherming van persoonsgegevens.

De nieuwe AVG is een verordening, in tegenstelling tot de oude Richtlijn Bescherming Persoonsgegevens. Dit betekent dat de AVG rechtstreeks van toepassing is binnen de gehele EU.

Bedrijven en overheden krijgen tot 25 mei 2018 de tijd om hun bedrijfsvoering met de AVG in overeenstemming te brengen. Op dat moment trekken ze de Wet bescherming persoonsgegevens (Wbp) en de Richtlijn Bescherming Persoonsgegevens (Richtlijn 95/46/EG) in.

Wet cliëntenrechten bij elektronisch verwerking van gegevens
De Eerste Kamer stemde eind oktober 2016 in met een wetsvoorstel waarin het de elektronische uitwisseling van medische gegevens tussen zorgverleners regelt. Zorgaanbieders hebben na inwerkingtreding van de wet nog drie jaar de tijd om te zorgen dat hun systemen voldoen aan deze nieuwe wet. De wet stelt eisen aan de beveiliging van medische gegevens en bevordert de privacy van patiënten. Een belangrijk onderdeel van de wet is dat een zorgaanbieder de gegevens van de patiënt pas beschikbaar mag stellen als de zorgaanbieder vaststelt dat de patiënt uitdrukkelijk zijn toestemming heeft gegeven. De wet biedt verschillende mogelijkheden voor patiënten om toestemming te geven aan zorgaanbieders:

- Hij mag besluiten dat de ene arts wel toegang heeft tot zijn gegevens en de andere niet en kan dat zelfs vooraf al aangeven. Bepaalde gegevens zijn zo voor die zorgaanbieders niet beschikbaar.
- Hij kan besluiten om slechts een deel van zijn gegevens beschikbaar te stellen en dus niet al zijn gegevens.
- Hij mag zijn medisch dossier op elektronische wijze bekijken of om een elektronisch afschrift vragen van zijn dossier.

Zorgverzekeraars, bedrijfsartsen en verzekeringsartsen mogen geen toegang tot de systemen met medische gegevens. Indien ze misbruik maken, dan staat hier een boete tegenover.

4.1.2 Adviezen en beleidsregels

Naast deze algemene regelingen zijn er ook adviezen en beleidsregels die handvaten bieden voor het verwerken en beschermen van persoonsgegevens.

Belangrijk om te kennen:

1. **Adviezen en rapporten van de Artikel 29-werkgroep.** De Artikel 29-werkgroep bestaat uit de nationale privacy-toezichthouders van de lidstaten van de Europese Unie en de European Data Protection Supervisor (EDPS). De EDPS houdt toezicht op de verwerking van persoonsgegevens bij de instellingen en organen van de EU. De Artikel 29-werkgroep heeft een onafhankelijk en raadgevend karakter. De belangrijkste taak van de werkgroep is het bevorderen van een uniforme toepassing van de principes uit de privacyrichtlijn in alle lidstaten door samenwerking tussen de Europese toezichthouders. Ook coördineert de werkgroep gezamenlijk onderzoek en de hieruit voortvloeiende nationale handhaving van de toezichthouders. De Artikel 29-werkgroep vormt in 2018 samen met de EDPS de European Data Protection Board (EDPB).

2. **Beleidsregels van de Autoriteit Persoonsgegevens** (AP), voorheen College Bescherming Persoonsgegevens (CBP). Deze komen in lijn met de AVG.

3. **ePrivacy-richtlijn (2009/136/EC)**, die onder andere toeziet op de regels omtrent het gebruik van cookies. Nederland implementeerde deze richtlijn in de Telecomwet. Naar verwachting volgt in 2017 een nieuw voorstel voor deze richtlijn.

4.1.3 Richtlijnen met raakvlak AVG

Naast bovengenoemde direct relevante wet- en regelgeving bestaat nog andere wet- en regelgeving die invloed heeft op het invullen van ROPG voor de consument. Hieronder volgen twee richtlijnen die een duidelijk raakvlak hebben met de AVG:

Payment Service Directive 2 (PSD2) richt zich op het versterken van de concurrentie in het betalingsverkeer. De PSD2 onderscheidt traditionele financiële instellingen (account servicing payment serviceproviders, ASPSP), 'payment initiation service providers' (PISP) en 'account information service providers' (AISP)). Die laatste twee hebben geen bankvergunning (nodig).
De belangrijkste verandering die PSD2 bewerkstelligt, is dat de AISP toegang kan krijgen tot de rekeninginformatie als de eigenaar van de rekening daar toestemming voor geeft ('access to account', XS2A). Ook mogen PISP's betalingen doen in opdracht van een rekeninghouder. Zo ontstaat een interessant speelveld voor intermediairs op financieel gebied en kan de consument via nieuwe dienstverleners regie voeren over zijn betaalgegevens.

Anti Money Laundering Directive 4; deze richtlijn richt zich op het voorkomen van witwaspraktijken en terrorismefinanciering. Een belangrijk onderdeel hiervan is het kennen van je klant (KYC = Know Your Customer). Deze vierde versie scherpt verschillende bepalingen hierover aan en vergroot de reikwijdte. Daarnaast hebben landen een plicht om een UBO-register (UBO = Ultimate Beneficial Owner) vast te leggen. Financiële instellingen moeten persoonsgegevens van hun klanten opvragen en vastleggen in verband met identificatie en verificatie van de klant.

4.2 Spelers die kaders zetten, toezicht houden en invloed uitoefenen

Verschillende spelers vervullen een rol in de totstandkoming van eisen aan de gegevensverwerking en oefenen controle uit op de naleving ervan. Wanneer het gaat over ROPG op de Nederlandse markt, moeten we rekening houden met zowel Nederlandse als Europese spelers op het gebied van persoonsgegevens. In dit paper maken we onderscheid tussen autoriteiten, belangenorganisaties en wetenschappelijke instituten. Het gekozen overzicht is niet allesomvattend, maar is een overweging van de belangrijkste relevante organen.

4.2.1 Autoriteiten

Autoriteiten zijn gezaghebbende organisaties met een formele rol in de definitie en/of naleving van gegevensverwerking. Verschillende Nederlandse en Europese autoriteiten houden zich bezig met de bescherming van persoonsgegevens:

1. **Autoriteit Persoonsgegevens (AP).** De AP is de nationale toezichthouder. De AVG verplicht ieder land om er één te hebben. Ze houdt toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens. Onder het toezicht valt ook het doen van onderzoek naar en adviseren over nieuwe regelgeving.

2. **EDPS (European Data Protection Supervisor)**. De EDPS houdt toezicht op de verwerking van persoonsgegevens bij de instellingen en organen van de EU. Deze toezichthouder vormt samen met de Artikel 29-werkgroep de European Data Protection Board (EDPB).

3. **Autoriteit Consument & Markt (ACM)**. De ACM richt zich op consumentenbescherming en heeft dus ROPG binnen haar domein. Afhankelijk van zaken die actueel zijn, kan ACM zich richten op verschillende ontwikkelingen die betrekking hebben op (de verwerking van) persoonsgegevens. Zo boog de ACM zich in het verleden over de cookiebepalingen en de privacyverklaringen op websites.

4. **Autoriteit Financiële Markten (AFM)**. De AFM houdt zich niet direct bezig met de verwerking en bescherming van persoonsgegevens door financiële instellingen. Dit kan veranderen als bijvoorbeeld blijkt dat in de financiële sector meer datalekken plaatsvinden of dat een groot percentage instellingen niet aan de regelgeving voldoet.

5. **Nederlandsche Bank (DNB)**. De DNB is verantwoordelijk voor het bewaken van de financiële stabiliteit in Nederland. De integriteit van en het vertrouwen in financiële instellingen en de

financiële sector als geheel zijn aandachtsgebieden van het toezicht in de sector. Indien privacygerelateerde zaken impact (kunnen) hebben op de financiële sector, dan besteedt de DNB aandacht aan hoe instellingen binnen de financiële sector moeten omgaan met privacy.

4.2.2 Belangenorganisaties

Een belangenorganisatie is een organisatie gericht op belangenbehartiging voor een specifieke doelgroep en/of een ideëel motief. Het gaat bijna altijd om een duidelijk omschreven doel met een specifiek maatschappelijk nut. Leden of donateurs zijn betrokken bij de belangenorganisaties. Ze hebben geen formele rol in de praktijk, maar beïnvloeden de maatschappij wel.

Verschillende belangenorganisaties zijn actief op het terrein van privacy en bescherming van persoonsgegevens. De meest bekende organisaties zijn:

1. **Consumentenbond.** De Consumentenbond treedt op als belangenbehartiger, informeert consumenten over en geeft advies omtrent ROPG bij gebruik van software, apps, internet etc. Ook doet de Consumentenbond onderzoek naar privacyverklaringen en -voorwaarden van bedrijven en de wijze waarop organisaties omgaan met persoonsgegevens. Daarover rapporteert de Consumentenbond vervolgens de resultaten aan zijn leden. Tot slot biedt de Consumentenbond een privacyforum waarop consumenten informatie en ervaringen kunnen uitwisselen over de verwerking van persoonsgegevens.

2. **Bureau Européen des Unions de Consommateurs (BEUC)**. De BEUC is de Europese koepelorganisatie voor consumentenorganisaties zoals de Consumentenbond. De BEUC heeft een actieve ROPG-agenda en maakt zich sterk voor een veilige digitale omgeving waarop klanten kunnen vertrouwen, ook met betrekking tot een effectieve controle op hun persoonsgegevens. De BEUC doet dat onder andere door overleg te voeren met beleidsbepalers (bijvoorbeeld de Artikel 29-werkgroep, de Europese Commissie en het Europees Parlement). Ze maakt brieven aan hen openbaar, vaardigt persverklaringen uit, publiceert position papers en informeert het publiek.

3. **Bits of Freedom (BoF)**. BoF is een burgerrechtenbeweging die zich inzet voor vrijheid en privacy op internet. Ze geeft advies over hoe mensen zorgvuldig om kunnen gaan met hun persoonsgegevens. Ze treedt op als belangenbehartiger ten aanzien van het recht op privacy en helpt mensen met het verkrijgen van inzage in de gegevens die over hen zijn vastgelegd.

4. **Patiëntenfederatie Nederland** vertegenwoordigt ruim 160 patiënten- en consumentenorganisaties en heeft privacybescherming als speerpunt. Met hun initiatief MedMij pakken ze een actieve rol op het terrein van ROPG. MedMij gaat zorgen dat de consument de regie voert over zijn persoonlijke gezondheidsomgeving.

5. **Verbond van Verzekeraars en Adfiz** vertegenwoordigen respectievelijk verzekeraars en adviseurs/ bemiddelaars. Hier zijn privacycommissies actief die ontwikkelingen voor hun leden duiden.

4.2.3 Wetenschappelijke instituten

De wetenschap stimuleert de publieke en politieke meningsvorming over privacy en bescherming van persoonsgegevens. Voorbeelden zijn het Rathenau Instituut en de Universiteit van Tilburg.

4.3 Afbakening ROPG conform AVG

Afbakening van ROPG op basis van de AVG vindt plaats aan de hand van de volgende onderwerpen:

1. Categorieën gegevens
2. Verwerkingsgronden en verwerking
3. Regie

Om één en ander te verduidelijken wordt, maken we een vertaalslag naar de impact voor de verzekeringsbranche en ketenintegratie.

4.3.1 Categorieën gegevens

Figuur-5 toont een verdeling van de verschillende categorieën gegevens.

Figuur-5 – Onderverdeling gegevens

Hieronder volgt een korte beschrijving van de verschillende categorieën.

1. **Algemene gegevens.** Dit is een heel breed begrip; alle gegevens die geen betrekking hebben op een persoon vallen hieronder, bijvoorbeeld bedrijfsinformatie.

2. **Persoonlijke gegevens** zijn gegevens die betrekking hebben op een persoon, maar niet zonder meer een natuurlijk persoon kunnen identificeren. Hierbij kun je bijvoorbeeld denken aan gegevens met betrekking tot een overleden persoon. Een overleden persoon valt niet onder de definitie van natuurlijk persoon, daarom kan het in dit geval nooit gaan om persoonsgegevens conform de AVG.
Daarnaast verstaan we onder persoonlijke gegevens ook gegevens die zonder context niet herleidbaar zijn tot een natuurlijk persoon. Een kenteken kun je bijvoorbeeld herleiden tot een natuurlijk persoon als er toegang is tot het RDW.

> ***Voorbeeld***
> *Iemand doet aangifte van diefstal van een voertuig. De gegevens van het voertuig worden dan aangemerkt als op die persoon betrekking hebbend.*

3. **Persoonsgegevens conform AVG** zijn alle gegevens die betrekking hebben op een geïdentificeerd of identificeerbaar natuurlijk persoon. Onder persoonsgegevens vallen onder andere naam, adres, woonplaats, telefoonnummer en geboortedatum. Daarnaast kunnen gegevens over eenmanszaken ook persoonsgegevens zijn. Het grijze gebied van persoonlijke gegevens is van belang: gegevens die onder omstandigheden voldoen aan de definitie van de AVG en daardoor persoonsgegevens worden. Een voorbeeld is het dynamische IP-adres. In oktober 2016 besloot het Hof van Justitie dat een dynamisch IP-adres ook een persoonsgegeven kan zijn. Het is immers voor internetproviders mogelijk om een

persoon te identificeren door hun eigen gegevens te combineren met een IP-adres. Voor partijen die niet eenvoudig toegang hebben of kunnen krijgen tot de gegevens van een internetprovider, is een dynamisch IP-adres geen persoonsgegeven.
In een veranderende maatschappij ontstaan steeds nieuwe soorten gegevens waarvan vastgesteld moet worden of deze persoonsgegevens zijn. Dit kan in de specifieke context plaatsvinden. Op den duur is het mogelijk dat bepaalde gegevens standaard persoonsgegevens worden.
Naast schriftelijke gegevens kan beeldmateriaal, zoals foto's of bewakingsbeelden, ook een persoonsgegeven zijn. De vorm van het gegeven moet je dus zeer ruim zien: op grond van de wet moet je enkel kijken of een gegeven (in welke vorm dan ook) tot een persoon is te herleiden.

4. **Bijzondere persoonsgegevens** zijn gevoelige gegevens zoals biometrische gegevens, ras, godsdienst, strafrechtelijk verleden en seksuele oriëntatie. Deze gegevens vereisen extra bescherming.

Voorbeeld
De consument sluit een inboedelverzekering af via een intermediair; de consument verstrekt de volgende gegevens aan de intermediair:

- *Persoonsgegevens: NAW, geboortedatum, e-mail, telefoonnummer, rekeningnummer;*
- *Bijzondere persoonsgegevens: gezinssamenstelling (hier is een mogelijkheid om gegevens te minimaliseren door verificatievragen te stellen of een range te vragen);*
- *Algemene gegevens: specificaties woning, zoals oppervlakte en materialen dak en vloer.*

4.3.2 Verwerkingsgronden en verwerking
Regie betreft de mate waarin een persoon controle kan uitoefenen over het inzien, beheren en/of delen van de eigen persoonsgegevens met/door derden.

De volgende twee aspecten bepalen de wijze van het uitoefenen van regie:
1. Verwerkingsgrond. Welke juridische grond(en) geldt/gelden voor de verwerking van de persoonsgegevens?
2. Verwerking. Wat gebeurt er met de persoonsgegevens?

4.3.2.1 Verwerkingsgrond
Het verwerken van persoonsgegevens is alleen toegestaan op basis van verwerkingsgronden die in de AVG staan. Verwerkingsgronden zijn eisen waarom je iets met een gegeven mag doen.

Minimaal één van de gronden moet van toepassing zijn; een combinatie van gronden is ook mogelijk. De AVG werkt de volgende zes gronden uit:

1. **Toestemming**. De betrokkene (consument) moet op een ondubbelzinnige wijze toestemming geven aan de verwerkingsverantwoordelijke voor het verwerken van zijn of haar persoonsgegevens. Het moet duidelijk zijn voor welk doel de toestemming dient. De consument moet deze uit vrije wil hebben afgegeven en het moet altijd mogelijk zijn om de toestemming weer in te trekken.
   Het geven van toestemming voor het doorgeven van persoonsgegevens geldt ook voor processen binnen de keten, bijvoorbeeld:
   a. De consument sluit verzekeringen af via intermediairs bij een bepaalde verzekeraar;
   b. De verzekeraar start een marketingactie via mail richting genoemde consumenten.

   De uitdaging is de toestemming (vooraf) adequaat te regelen / vast te leggen voor de keten. Transparantie naar de consument is hierbij een belangrijke randvoorwaarde.

   Sinds het provisieverbod op complexe producten is het niet meer vanzelfsprekend dat de intermediair het beheer voert over een afgesloten verzekering. Toestemming van de consument is dan vereist voordat de verzekeraar gegevens deelt. De uitdaging is dit op een eenduidige wijze te borgen binnen de keten.

2. **Uitvoering van een overeenkomst.** Het verwerken van persoonsgegevens is toegestaan als dat nodig is voor de uitvoering van een overeenkomst. Het tekenen van een contract vormt daarmee een indirecte toestemming, en is te onderscheiden van de hierboven genoemde verwerkingsgrond 'toestemming'. Als bijvoorbeeld de bewoner van een woning een opstalverzekering afsluit, dan is het vanzelfsprekend noodzakelijk om het adres van de woning te verwerken. Het beëindigen van de overeenkomst is impliciet ook het intrekken van de toesteming.

   Een goede overeenkomst geeft aan welke gegevens wie met welke derde partijen mag delen, met welke reden en wanneer. Indien dit niet in de overeenkomst staat, dan is het mogelijk om op een later moment om toestemming te vragen voor dit specifieke punt, zonder hierbij de overeenkomst te hoeven wijzigen.

3. **Wettelijke plicht**. Op de verwerkingsverantwoordelijke kan een wettelijke plicht rusten die verwerking van persoonsgegevens noodzakelijk maakt. Banken/verzekeraars zijn bijvoorbeeld verplicht om een aantal financiële gegevens aan de Belastingdienst te verstrekken en daarvoor het BSN van hun klanten vast te leggen.

4. **Algemeen belang/openbaar gezag.** Verwerking kan nodig zijn voor de uitoefening van openbaar gezag of voor de vervulling van een taak van algemeen belang. Publiekrechtelijke organisaties moeten bijvoorbeeld gegevens van daders delen met verzekeraars, zodat zij weten op wie zij de schade moeten verhalen.

5. **Vitaal belang.** Als iemand zelf niet in staat is om toestemming te geven en snel handelen noodzakelijk is, dan is het toegestaan om persoonsgegevens te verwerken. Wanneer bijvoorbeeld iemand vanwege een ongeluk snel een bloedtransfusie nodig heeft, dan is het noodzakelijk en toegestaan om diens bloedgroep te achterhalen in zijn medisch dossier.

6. **Gerechtvaardigd belang.** De verwerkingsverantwoordelijke moet een afweging maken tussen zijn eigen belangen om gegevens te verwerken en de belangen van de betrokkene. Een heel brede interpretatie is hier mogelijk met veel kans op discussie. Jurisprudentie toont de hantering in de praktijk. Een voorbeeld uit de verzekeringsbranche is dat een verzekeraar voor de afwikkeling van de schadeclaim naast de gegevens van zijn eigen klant (uitoefening overeenkomst) ook de gegevens van de tegenpartij en van eventuele getuigen moet verwerken. Gerechtvaardigd belang is een veelgebruikte grond voor gegevensverwerking door verzekeraars, maar het is echter geen grond waar consumenten invloed op kunnen uitoefenen.

Voorbeeld
Het afsluiten van een verzekering is een verwerkingsgrond, namelijk het uitvoeren van een overeenkomst. Voor alle doelen die de overeenkomst specificeert mag de verzekeraar, de noodzakelijke persoonsgegevens verwerken.

4.3.2.2 Verwerking
Persoonsgegevens dienen voor dienstverleners als een soort grondstof in administratieve processen. Ze moeten bepaalde inzichten geven. Onder het verwerken van persoonsgegevens verstaan we: elke handeling die betrekking heeft op persoonsgegevens. Dit kan variëren van het vastleggen en het bewaren van gegevens tot het wijzigen of verwijderen van de gegevens of het verspreiden of delen ervan.

4.3.3 Regie en rechten van de consument

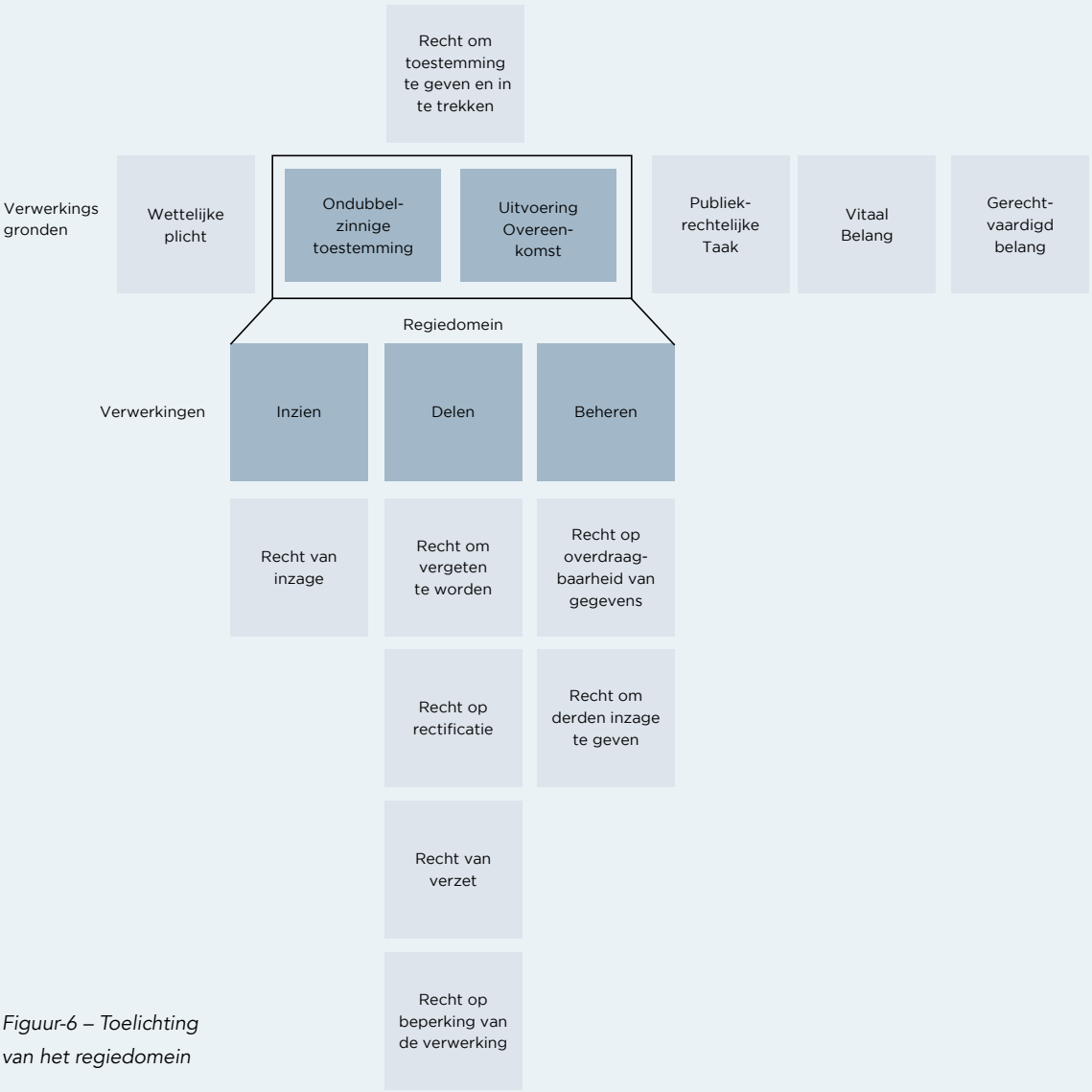
ROPG kan drie vormen hebben:
1. Inzien. In de eerste plaats gaat het om het inzien van gegevens. Iedere consument heeft het recht om bij iedere organisatie die gegevens over hem of haar registreert, gratis op te vragen welke persoonsgegevens zij hebben.

2. Beheren. Een stap verder gaat het als een consument via dat kanaal zelf in staat is om gegevens te wijzigen, rectificeren of verwijderen of als de betrokkene de gegevens kan laten corrigeren of verwijderen. Het beheren van gegevens gaat over de mogelijkheid om zelf te bepalen wat er wel en niet staat vastgelegd.

3. Delen. Daarnaast kan een consument zelf bepalen wie gebruik mag maken van zijn of haar persoonsgegevens, voor welk doel en hoe vaak. Hierbij krijgt de consument de mogelijkheid om aan te geven wie gegevens mag inzien en aan wie de gegevens verzonden mogen worden. In beide gevallen gaat het om het delen van gegevens. Het delen van gegevens kan de consument zelf doen, of bijvoorbeeld als verwerkingsverantwoordelijke overlaten aan een verwerker.

Voorbeeld
Privéomstandigheden kunnen wijzigen. Een klant wil dan misschien zijn gegevens inzien om te bepalen of wijzigingen nodig zijn. Een verzekeraar biedt een klant in dit geval toegang tot een 'mijn omgeving' waar de klant al zijn persoonsgegevens kan inzien. Conform de wet moet de verzekeraar toegang bieden tot alle persoonsgegevens betreffende de klant waarover de verzekeraar beschikt.

In figuur-6 is in een overzicht aangegeven wat er onder regiedomein verstaan wordt. Het overzicht geeft de verschillende verwerkingsgronden en verwerkingen weer. In blauw staat aangegeven op welke aspecten regie betrekking heeft.



Figuur-6 – Toelichting van het regiedomein

Rechten voor consumenten scheppen de ruimte voor regie. Hierna leggen we kort uit wat de diverse rechten voor consumenten volgens de AVG zijn.

Recht om toestemming te geven en in te trekken
Het is verplicht de consument te wijzen op het recht om de gegeven toestemming in te trekken. Het intrekken van toestemming moet net zo gemakkelijk zijn voor de consument als het geven ervan. Bijvoorbeeld wanneer toestemming digitaal is verleend, moet het ook mogelijk zijn deze toestemming digitaal in te trekken en niet via andere ingewikkeldere wegen zoals per post.

Recht van inzage
Een consument heeft het recht om van de verwerkingsverantwoordelijke te horen als hij zijn persoonsgegevens verwerkt. De consument heeft recht op inzage in deze gegevens bij verwerking van zijn persoonsgegevens. Daarnaast heeft hij onder andere recht op informatie over:

- de doelen van de verwerking;
- de betrokken categorieën van persoonsgegevens;
- de ontvangers die de persoonsgegevens krijgen;
- de opslagperiode;
- het feit dat de consument het recht heeft op het indienen van een verzoek tot rectificatie en een verzoek tot het wissen of beperken van de gegevens;
- het feit dat de consument een klacht kan indienen.

De impact van dit recht op de systemen bij verzekeraars, volmachten en intermediairs is groot. De keten moet een adequate administratie voeren voor de verwerking van persoonsgegevens.

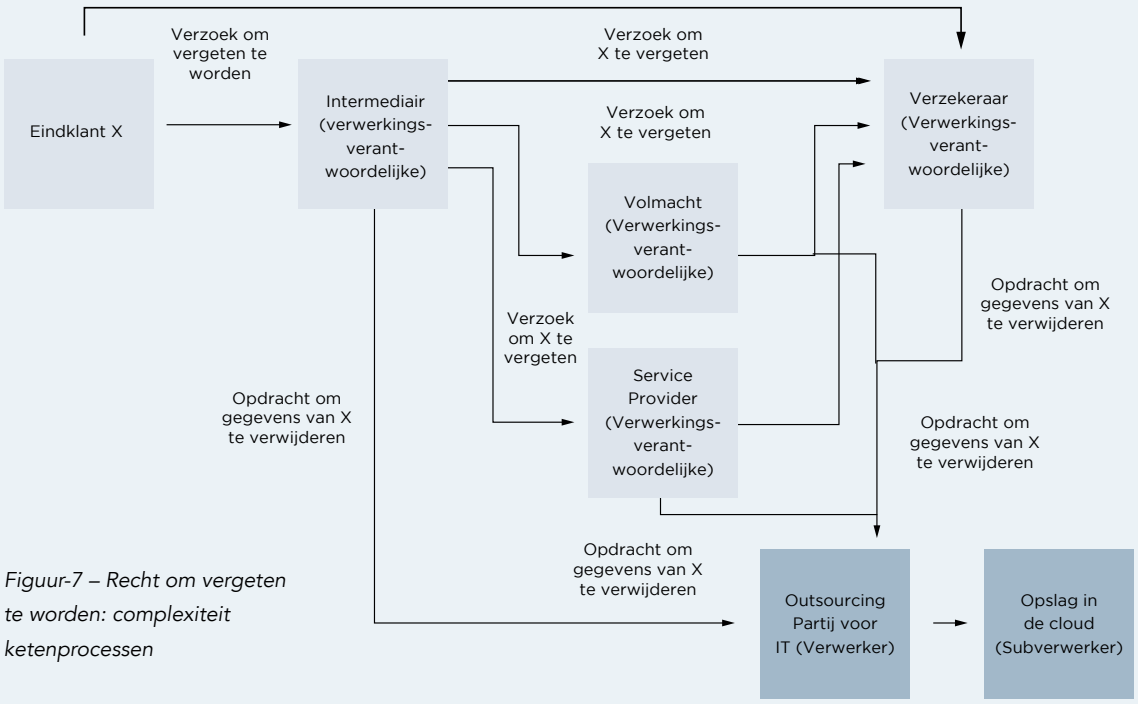
Recht om vergeten te worden
Een consument heeft soms het recht om zijn opgeslagen persoonsgegevens te laten verwijderen. Een verantwoordelijke moet een verzoek daarvoor inwilligen als één van de volgende gevallen van toepassing is:

- de opslag van de gegevens is niet langer nodig voor de doelen waarvoor zij zijn verzameld;
- de consument trekt de gegeven toestemming in en er is geen andere rechtsgrond voor de verwerking;
- de consument maakt bezwaar tegen de verwerking;
- de gegevens zijn onrechtmatig verwerkt;
- wissen van gegevens is nodig om te voldoen aan een wettelijke verplichting.

De verwerkingsverantwoordelijke moet redelijke maatregelen nemen om de gegevens te verwijderen, maar ook om iedere koppeling naar kopie of reproductie te wissen. Verder geldt hier natuurlijk wel dat wettelijke bewaartermijnen gelden voor gegevens die ze wettelijk moet bewaren.
Indien de verwerkingsverantwoordelijke besluit de gegevens te anonimiseren, mag ze deze bewaren, op voorwaarde dat ze niet tot een individu te herleiden zijn.

De consument mag het verzoek doen aan iedereen die zijn gegevens verwerkt. De ketenpartij die het verzoek ontvangt, moet het proces starten om vergeten te worden. De verwerkingsverantwoordelijke is dus niet standaard de initiator. Een organisatie moet aan dit soort verzoeken kunnen voldoen en kunnen nagaan of het verzoek valide is of niet. Het impliceert ook dat de keten afspraken moet maken en in een procedure vastlegt hoe ze hiermee omgaat. Figuur-7 geeft een indruk van de complexiteit die bijvoorbeeld speelt in het volgende voorbeeld:

1. Verzekering is afgesloten via een intermediair;
2. Intermediair heeft de verzekering ondergebracht in de volmacht;
3. De volmacht loopt bij een serviceprovider;
4. Bij schade boven een bepaalde limiet worden de persoonsgegevens gedeeld met de volmachtgever (verzekeraar);
5. Consument stapt over en dient verwijderverzoek in.



Figuur-7 – Recht om vergeten te worden: complexiteit ketenprocessen

Recht op rectificatie
Een consument heeft het recht om van de verwerkingsverantwoordelijke verbetering van onjuiste persoonsgegevens te verkrijgen. Dit moet zonder onredelijke vertraging gebeuren.

Recht op beperking van de verwerking
De consument heeft het recht om beperking van de verwerking te verkrijgen, wanneer bijvoorbeeld de juistheid van de gegevens door de consument wordt betwist of wanneer de persoonsgegevens niet meer nodig zijn voor de doelen van de verwerking, maar de consument ze nodig heeft voor de instelling, uitoefening of verdediging van een rechtsvordering.

Recht op overdraagbaarheid van gegevens
De consument heeft het recht om de persoonsgegevens die hem betreffen te verkrijgen. Ook mag hij deze in principe overdragen aan een andere verwerkingsverantwoordelijke.

Recht om derden inzage te geven
De consument heeft het recht om derden inzage te geven in zijn persoonsgegevens.

Voorbeeld
Ydenti (http://ydenti.nl/) biedt een soort schil om verschillende identiteit-gerelateerde diensten heen. Ydenti heeft zelf al een behoorlijk aantal relevante bedrijven op de lijst die de consument met een paar klikken kan benaderen voor specifieke verzoeken. Deze verzoeken liggen in het verlengde van de rechten die consumenten kunnen ontlenen aan de AVG. Zo kan een consument via het portaal alle leveranciers op de hoogte stellen van een verhuizing.

4.4 De belangrijkste voor de branche relevante bepalingen uit de AVG

De verzekeringsbranche en betrokken partijen bij de ROPG dienen met een aantal wijzigingen in de wetgeving rekening te houden. De volgende bepalingen gelden onder de AVG vanaf mei 2018:

- Een gegevens-beschermings-effectbeoordeling (PIA = Privacy Impact Assessment)

Een organisatie is in ieder geval verplicht om een effectbeoordeling uit te voeren als deze organisatie:

- systematisch en uitvoerig persoonlijke aspecten evalueert, of profilering toepast;
- op grote schaal bijzondere persoonsgegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

De PIA brengt risico's in kaart en definieert de benodigde maatregelen.

- **Functionaris Gegevensbescherming** (DPO = Data Privacy Officer). Instanties die aan bepaalde eisen voldoen, moeten een Functionaris Gegevensbescherming aanwijzen. Hij/zij ziet intern toe op een juiste verwerking en beveiliging van persoonsgegevens en de naleving van de AVG en andere wetgeving. De Artikel 29-werkgroep publiceerde onlangs een guidance waarin de Functionaris Gegevensbescherming voor verzekeraars verplicht is. Dit is nog niet definitief.

- De AVG kent net als de Wbp een 'meldplicht datalekken', maar onder een andere naam. De term in de verordening is een **inbreuk in verband met persoonsgegevens**. Dit is een inbreuk op de beveiliging die (al dan niet onbedoeld) op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Verder geldt:

- Instanties moeten alle inbreuken binnen 72 uur aan de AP melden, tenzij "het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen". Afhankelijk van de inbreuk op het recht van consumenten dienen ze die zelf ook in te lichten.
- Instanties moeten alle inbreuken administreren: "De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, inclusief de feiten over de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen." Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.
- Onder de AVG moeten verwerkingsverantwoordelijken dus een veel omvangrijker administratie bijhouden dan nu het geval is. Hoe lang ze het overzicht moeten bewaren volgens de nieuwe regels is nog onduidelijk.

Voor ketensystemen die persoonsgegevens over meerdere schakels uitwisselen, is sprake van gezamenlijke verantwoordelijkheid en is het wenselijk om goede afspraken te maken. Bijvoorbeeld dat meerdere partijen gezamenlijk de melding van een eventueel datalek doen. Openheid richting elkaar in geval van een datalek is hier ook van belang. Andere partijen in de keten zijn dan op hun hoede, maar krijgen ook de kans om verdere lekken tegen te gaan. Bijvoorbeeld als bij hen wordt ingelogd met gelekte data.

- De consument heeft het recht om niet te worden onderworpen aan een (voor hem) negatief besluit dat alleen is gebaseerd op een geautomatiseerde verwerking van persoonsgegevens. Profilering door middel van automatische verwerking valt hier ook onder. De verwerkingsverantwoordelijke moet een optie van menselijke tussenkomst bieden.

- The right to be forgotten ('recht om vergeten te worden') houdt in dat een consument het recht heeft al zijn persoonsgegevens te laten wissen. Dit betekent dat de gegevens die voor de verwerking aan derden zijn verschaft ook moeten worden gewist. Als ze openbaar zijn gemaakt, moeten voldoende maatregelen worden getroffen om die gegevens ook te wissen. Dit is alleen van toepassing als er ook geen verwerkingsgrond meer is voor verdere verwerking van die gegevens.

- Privacy by Design en Privacy by Default houden in dat ontwikkelaars bij de ontwikkeling van producten en diensten meteen al rekening houden met het waarborgen van privacy; ze moeten de passende technische en organisatorische maatregelen en ook dataminimalisatie toepassen. Aan de ene kant dus door ontwerp, zowel technisch als procedureel. Aan de andere kant door middel van standaardinstellingen.

De verzekeringsbranche werkt veel met softwarepakketten. Daarom is het belangrijk dat deze partijen dit voldoende voortvarend adresseren. Binnen de keten als geheel speelt dit vraagstuk ook bij de uitwisseling van gegevens tussen ketenpartijen.

Privacy by Design is mogelijk door het toepassen van technieken als pseudonimisering. Dit houdt in dat het verwerken van persoonsgegevens zo gebeurt dat deze persoonsgegevens niet meer aan een specifieke betrokkene te koppelen zijn zonder aanvullende gegevens te gebruiken. Dit is een goede methode om data te gebruiken zonder de privacy of bescherming van persoonsgegevens in het geding te brengen. Bijvoorbeeld bij medische gegevens voor analyses. Een andere toegepaste techniek is er een die uitsluitend noodzakelijke persoonsgegevens uitwisselt en verwerkt (dataminimalisatie). De optimale situatie verzamelt alleen de strikt noodzakelijke gegevens.

- Organisaties moeten nu bepaalde gegevensverwerkingen bij de AP melden, onder de AVG vervalt deze meldingsplicht. Zowel verwerkingsverantwoordelijken als verwerkers moeten hun verwerkingsactiviteiten bijhouden in een eigen register. Dit is ter vervanging van de meldplicht voor verwerking van persoonsgegevens, maar ook voor het hebben van een audit trail. Op verzoek moeten organisaties dit register met de AP delen. Ze moeten alle verwerkingsactiviteiten in het register vermelden. Van elke activiteit moeten ze een aantal gegevens benoemen, onder andere welke data het betreft, wat het doel is, wie verantwoordelijk is, de getroffen beveiligingsmaatregelen etc.

Voorbeeld werkgever
Een organisatie legt gegevens van werknemers vast. Deze activiteit moet de organisatie in het register vermelden. Hierbij kan het doel zijn adresgegevens voor het verzenden van post, rekeninggegevens voor het overmaken van salaris, etc. Op dit niveau leggen ze de activiteiten in het register vast. Het is dus niet nodig om alle medewerkers en alle handelingen apart in het register op te nemen.

Overigens is het register alleen verplicht voor organisaties met 250 werknemers of meer, of in het geval ze in grote mate persoonsgegevens verwerken.

- Organisaties die niet voldoen aan de AVG kunnen rekenen op verschillende sancties van de AP, waaronder fors hogere boetes. Boetes kunnen oplopen tot wel € 20 miljoen of 4% van de wereldwijde jaaromzet van een onderneming. Ze kan deze opleggen aan zowel verwerkingsverantwoordelijken als verwerkers.

4.5 De verantwoordelijkheid in de keten volgens de AVG

De wet onderscheidt verschillende rollen met betrekking tot gegevensverwerking. Afhankelijk van de rol die een partij speelt, varieert de verantwoordelijkheid die op die partij rust. Ook is het mogelijk dat een partij in de keten per situatie een andere rol heeft. Ieder type organisatie in de verzekeringsbranche kan een rol spelen in de keten met betrekking tot gegevensverwerking. Het is van belang om goed te begrijpen wie welke verantwoordelijkheid heeft.

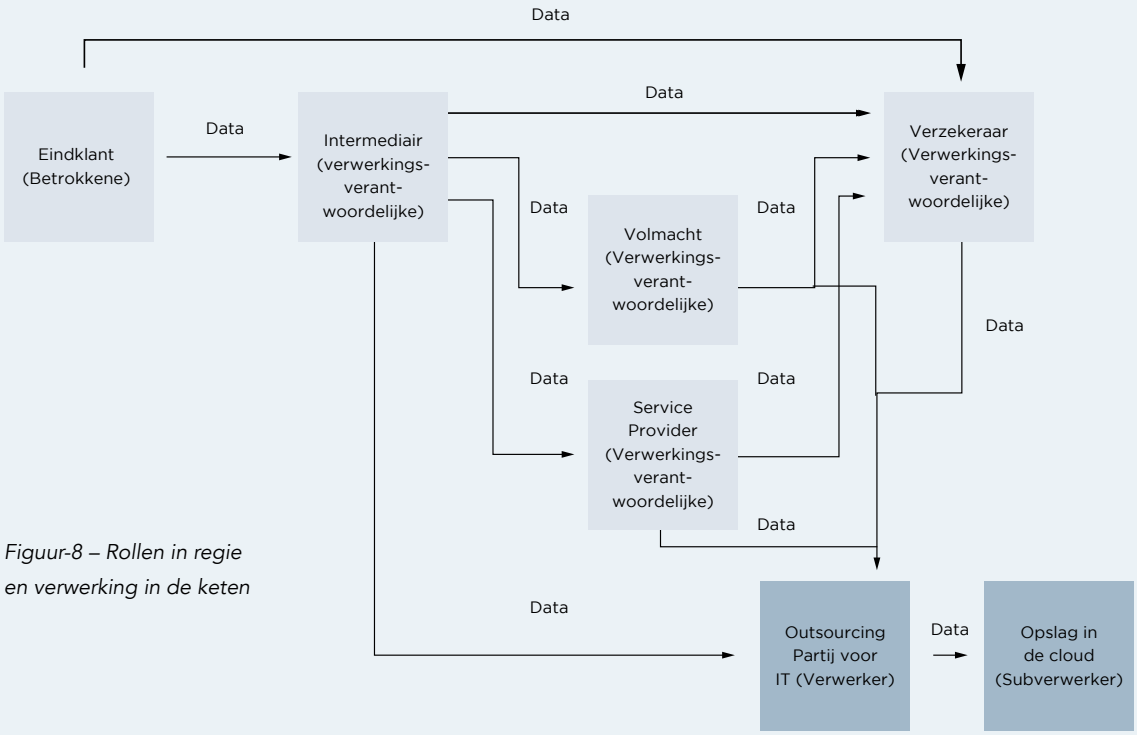
In de keten van gegevensverwerking onderscheiden we verschillende spelers. Zij hebben ieder een eigen functie en een gezamenlijke verantwoordelijkheid. De AVG benoemt de volgende spelers:

- **Betrokkene** (Data subject): natuurlijk persoon waarop de gegevens betrekking hebben. De betrokkene heeft regie over zijn of haar eigen persoonsgegevens.
- **Verwerkingsverantwoordelijke** (Controller): natuurlijk persoon, rechtspersoon of bestuursorgaan die zeggenschap heeft over het doel en de wijze van verwerking. De verwerkingsverantwoordelijke is onder andere verantwoordelijk om:
  - passende technische en organisatorische maatregelen te treffen;

- zich ervan te verzekeren dat een verwerker de juiste garanties biedt op het gebied van gegevensbescherming;
- zich ervan te verzekeren dat een verwerker alle verplichtingen in de verwerkersovereenkomst opneemt;
- de verantwoordelijkheid en de aansprakelijkheid van iedere verwerking vast te leggen.

- **Verwerker** (Processor): de verwerker van de gegevens werkt op basis van een verwerkersovereenkomst. De verwerker mag alleen die persoonsgegevens verwerken die vallen binnen het doel van de verwerkersovereenkomst. Indien de verwerker meer of iets anders wil doen, mag dat alleen met instemming van de verwerkingsverantwoordelijke.

Verschillende partijen in de keten kunnen de rol van verwerkingsverantwoordelijke hebben als zij beiden zeggenschap hebben over bepaalde persoonsgegevens. Figuur 8 toont de rollen en regie in de verwerking. Bij elke partij afzonderlijk moet duidelijk zijn of zij zelf het doel en de wijze van verwerking bepaalt of dat ze dit puur in opdracht van een andere partij doet. Het is dus mogelijk dat verschillende partijen in de keten voor bepaalde gegevens verwerkingsverantwoordelijke zijn.



Figuur-8 – Rollen in regie en verwerking in de keten

Voorbeeld
Een klant sluit via een intermediair een verzekering bij een verzekeraar af. In dit voorbeeld kan zowel de intermediair als de verzekeraar de verwerkingsverantwoordelijke zijn. Zij bepalen namelijk apart van elkaar hoe zij met de door de klant verstrekte persoonsgegevens omgaan.

- *De intermediair is verwerkingsverantwoordelijke, aangezien de tussenpersoon zeggenschap heeft over welke gegevens ze van de klant verstrekt, maar ook welke ze met de verzekeraar deelt en op welke wijze.*
- *De verzekeraar is verwerkingsverantwoordelijke, aangezien hij alle ontvangen gegevens vastlegt, het risicoprofiel bepaalt en zeggenschap heeft over hoe hij omgaat met de persoonsgegevens van de klant die hij heeft.*
- *De outsourcing partij is verwerker, aangezien hij op basis van een verwerkersovereenkomst de gegevens vastlegt op de wijze die hij van de verzekeraar kreeg.*

05

Kansen voor de verzekerings-branche

Uit de AVG vloeien onvermijdelijkheden en verplichtingen voort met impact op de keten. In het verlengde van de AVG en de diverse marktinitiatieven rond ROPG signaleren we ook kansen voor de verzekeringsbranche:

- Voordelen bieden aan de consument;
- Bijdrage leveren aan herstel van vertrouwen;
- Gebruikerservaring verbeteren;
- Nieuwe waardeproposities creëren;
- Drempels verlagen voor advies;
- Uitstraling van de branche verhogen door voorop te lopen in digitale dienstverlening;
- Kansen benutten voor samenwerking geformuleerd door de AVG.

5.1 Voordelen bieden aan de consument

5.1.1 Controle over persoonsgegevens, overzicht, gemak

Regie geeft de consument zicht en controle op de verwerking van persoonsgegevens. De legitimiteit van deze verwerking is afhankelijk van de verwerkingsgrond.

De consument kan regie uitoefenen door zijn gegevens in te zien, te beheren en/of te delen; dit kan in verschillende vormen plaatsvinden. Deze mogelijkheden van regie krijgt de consument bij organisaties die over zijn persoonsgegevens beschikken. Zo kan de consument bij zijn werkgever zijn salarisgegevens inzien en nagaan of alle berekeningen correct zijn uitgevoerd en bij zijn verzekeraar zijn eigen polisgegevens beheren.

Naarmate het aantal online toepassingen voor ROPG toeneemt, stijgt ook het belang van laagdrempelige toegang. Iedere consument worstelt met een stuwmeer aan gebruikersnamen en wachtwoorden. Doel moet zijn om consumenten gemak bij toegang te bieden. De consument kan met een beperkt aantal digitale sleutels (authenticatiemiddelen) overal inloggen. Gegevens worden toegankelijk na enkele handelingen, waarbij de consument idealiter niet voor elke omgeving opnieuw hoeft in te loggen.

5.1.2 Online security en privacy

Het ROPG-domein moet de consument een hoge mate van online privacy en veiligheid bieden, met Privacy by Design en Privacy by Default als norm. Privacy bij Design impliceert dat ze bij de start van het ontwerpen van een informatiesysteem al rekening houden met privacy. Privacy by Default betekent dat de instellingen van een programma, app, website of dienst maximale privacy betrachten. Het gaat niet alleen om opties die ze kunnen instellen, maar ook zaken als algemene voorwaarden moeten privacyvriendelijk zijn.

Als de trend zich doorzet blijven data zo veel mogelijk gedistribueerd opgeslagen. Privacy-hotspots worden daarom vermeden. Eventuele uitwisseling van persoonsgegevens wordt zo veel mogelijk afgeschermd van de betrokken partijen; dit betreft ook informatie over de gegevensuitwisseling.

Dataminimalisatie wordt vanzelfsprekend: online dienstverleners vragen niet méér informatie dan nodig. Denk bijvoorbeeld aan een leeftijdscheck waarbij in een bericht niet de volledige geboortedatum staat maar slechts of de consument ouder is dan een bepaalde leeftijd.

5.1.3 Nieuwe dienstverlening met meer gemak en lagere drempels
Dienstverleners gaan inspelen op het recht van overdraagbaarheid van gegevens. Dit betekent dat het afnemen van diensten bij een nieuwe dienstverlener makkelijker wordt, waarbij het opnieuw opgeven van al bekende gegevens achterwege kan blijven.

Regie betekent ook dat de consument zelf bepaalt welke dienstverleners toegang krijgen tot persoonsgegevens waarover de consument direct beheer voert. Dienstverleners ontvangen automatisch wijzigingen, zoals verhuizingen. Indien de consument daar toestemming voor geeft, kan een dienstverlener tijdig een aanbieding op maat doen.

De (veilige) beschikbaarheid van gegevens 'over sectoren heen' maakt gepersonaliseerde en nieuwe dienstverlening mogelijk, met verhoogde relevantie voor de consument. Indien de consument met enkele handelingen kan beschikken over al zijn financiële gegevens, wordt advies in het pensioen-, hypotheek- en AO-domein laagdrempeliger.

5.2 Bijdrage leveren aan herstel van vertrouwen

Consumenten weten niet welke informatie anderen over hen verzamelen, hoe ze die informatie gebruiken en met wie ze deze delen. Als iemand vreest dat zijn gegevens aan zorgverzekeraars worden doorverkocht, zal hij kunnen nalaten op internet te zoeken naar informatie die relevant is voor zijn medische klachten. Consumenten en politici hebben nu vaak het beeld dat aanbieders de persoonsgegevens enkel en alleen voor commerciële doeleinden aanwenden. Daardoor diskwalificeert de sector zich. De sector kan het vertrouwen herstellen door, middels samenwerking binnen ketens, te laten zien dat men op verantwoorde wijze omgaat met persoonsgegevens en een basisset aan garanties afgeeft. Maatschappelijk verantwoord gedrag naar kwetsbare groepen zoals digibeten is hierbij een belangrijk aspect.

Dataethiek gaat over morele vraagstukken van de herkomst, de integriteit, het omgaan met en de controle van persoonsgegevens. Dataethiek gaat ook over de acties die men neemt op basis van inzichten uit de analyse van data. In de basis gaat het over de vraag hoe consumenten vertrouwen hebben in de wijze waarop verzekeraars, volmachten, intermediairs en derden met data omgaan. Vertrouwen wordt een steeds belangrijker factor. Consumenten moeten er vertrouwen in hebben dat genoemde partijen op verantwoorde wijze data over hen verzamelen, opslaan en gebruiken. Op een manier die de consument ten goede komt, en de data goed beschermt tegen hackers en ongewenste verkoop aan derden. Wanneer verzekeraars, volmachten en intermediairs heldere kaders neerzetten en naleven voor persoonlijke regie op gegevens, is het voor de consument transparant hoe een bepaalde actor aan de gegevens komt en welke data ze verzamelen.

De DNB stelde recent dat gerichte dienstverlening kan bijdragen aan vertrouwensvorming, als de verzekeraars maar transparantie bieden. "Consumenten verwachten in toenemende mate ontzorging op een professionele en integrale wijze. Verzekeraars kunnen hierop inspelen door het klantbelang centraal te stellen. Daarbij moeten zij transparant zijn over de geboden zekerheden en duidelijk communiceren over de risico's en de kosten. Zo kunnen polishouders een verantwoorde keuze maken." Dit vertrekpunt kunnen we zeer goed hanteren binnen het ROPG-werkgebied. Richting consumenten kunnen we een algemeen eenduidig beeld ontwikkelen, omdat in de breedte de markt nog aan de start staat

5.3 Gebruikerservaring verbeteren

Het vergroten van de controle van consumenten op hun persoonsgegevens is het idee achter het recht op dataportabiliteit. Een consument kan zelf bepalen welke gegevens hij met wie deelt en ontkomt hiermee tegelijk aan vendor lock-in. Het voorkomt namelijk dat hij opnieuw moet beginnen bij een nieuwe partij. De nieuwe AVG vereist uitwisseling in machine-leesbare vorm en moedigt in dit verband aan om interoperabele formaten te ontwikkelen die gegevensoverdraagbaarheid mogelijk maken. Dit kunnen we doortrekken naar het ontwikkelen van manieren om informatie direct door te sturen naar andere partijen. Dit laatste is overigens een advies richting organisaties, geen verplichting. Voor verzekeringen zijn standaarden beschikbaar (AFD gegevensdefinities en berichtsoorten) die organisaties kunnen inzetten om het genoemde advies op te volgen.

De uitwisseling van persoonsgegevens hoeft niet altijd in het teken te staan van overstappen, maar kan bijvoorbeeld ook bijdragen aan het sneller opbouwen van een compleet klantbeeld bij een adviseur voor beheer en/of advies. Dataportabiliteit betekent niet per definitie klantverlies. Een klant kan bijvoorbeeld ook een product afnemen bij een andere verzekeraar waar zijn eigen verzekeraar niet in voorziet.

Het Verbond van Verzekeraars oefent wat betreft dataportabiliteit invloed uit via VNO-NCW en Insurance Europe. Insurance Europe publiceerde eind januari 2017 een position paper "Insurance Europe contribution to the Article 29 Working Party guidelines on the right to data portability". Insurance Europe stuurt er op aan dat voor wat betreft dataportabiliteit gegevens volstaan die nodig zijn voor het oversluiten. Hierbij vormt dataminimalisatie het vertrekpunt.

5.4 Nieuwe waardeproposities creëren

De beschikbaarheid van hoogwaardige data uit alle sectoren zal toenemen. In het publieke domein werkt de overheid aan een programma waarbij de gegevens in basisregistraties – met instemming van de burger – ter beschikking komen in het publieke domein. Als consumenten altijd regie kunnen voeren over persoonsgegevens in het algemeen en de financiële gegevens in het bijzonder die over hen zijn vastgelegd, dan wordt het aggregeren van financiële gegevens een stuk efficiënter. Hierdoor kan de (financiële) drempel voor advies verlaagd worden. Dit raakt direct intermediaire distributie. Een en ander veronderstelt wel dat sprake is van sector-overschrijdende gegevensuitwisseling. De consument zal bijvoorbeeld moeten beschikken over de gegevens van zijn leningen, de gegevens over zijn basisinkomen, de gegevens van pensioenen etc.

5.5 Drempels verlagen voor advies

De beschikbaarheid van hoogwaardige data uit alle sectoren zal toenemen. In het publieke domein werkt de overheid aan een programma waarbij de gegevens in basisregistraties ter beschikking komen in het publieke domein. Wel met instemming van de burger. Consumenten kunnen altijd regie voeren over persoonsgegevens in het algemeen en de financiële gegevens die over hen vastliggen in het bijzonder. Het aggregeren van financiële gegevens wordt een stuk efficiënter. Dit verlaagt de (financiële) drempel voor advies en raakt direct de intermediaire distributie. Eén en ander veronderstelt wel dat sprake is van sector-overschrijdende gegevensuitwisseling. De consument moet bijvoorbeeld beschikken over de gegevens van zijn leningen, basisinkomen, pensioenen etc.

5.6 Uitstraling branche verhogen door voorop te lopen in digitale dienstverlening

Voortvarende samenwerking biedt de verzekeringsbranche een aanvullende kans voorop te lopen in digitale dienstverlening en een voorbeeld te zijn voor andere sectoren. Dat is goed voor de uitstraling, maar bepaalt ook de mate waarin de branche invloed heeft op het ontwikkelen en handhaven van standaarden die breder worden ingezet dan binnen de branche zelf.

5.7 Kansen benutten voor samenwerking geformuleerd door de AVG

De AVG biedt expliciet ruimte aan sectoren/branches om invulling te geven aan de praktijk van bescherming van persoonsgegevens toegespitst op hun markt. Deze bepalingen bieden een basis voor het kiezen van één van de opties voor ROPG. Hieronder volgt een korte uitwerking van de betreffende bepalingen die samenwerking stimuleren op het gebied van gedragscodes, certificeringen en dataportabiliteit.

5.7.1 Gedragscodes

Brancheorganisaties of andere organen kunnen in samenwerking gedragscodes opstellen waarin ze verschillende bepalingen uit de AVG nader uitwerken en best practices ontwikkelen. Deze gedragscodes moeten we niet verwarren met interne gedragscodes of binding corporate rules. Gezamenlijke gedragscodes spelen in op het specifieke karakter en de specifieke behoeftes van de sector. Deze codes kunnen ze vervolgens aan de AP voorleggen ter goedkeuring als ze voldoende passende waarborgen bieden. Ook kan de AP een onafhankelijk en deskundig orgaan accrediteren dat zal toezien op naleving van de gedragscode binnen de branche/sector.

Verschillende branches zijn zelf aan de slag met het opstellen van gedragscodes. Zo stelde de VEDEK (brancheorganisatie voor de Onafhankelijke Dienstenaanbieders in de energiebranche) samen met VMNED (Vereniging van Meetbedrijven in Nederland) een gedragscode op voor de omgang met de data uit de slimme meter. Een belangrijke voorwaarde voor de AP is dat een representatief deel van de organisaties binnen de scope de gedragscode ondertekent.

Op dit moment bestaat al een gedragscode Verwerking persoonsgegevens financiële instellingen. Deze is opgesteld in 2010 en voldoet aan de WBP. De reikwijdte van deze gedragscode is beperkt tot banken aangesloten bij de Nederlandse Vereniging van Banken en verzekeraars aangesloten bij het Verbond van Verzekeraars. Het Verbond van Verzekeraars werkt zelf aan een nieuwe privacy-gedragscode. Deze zal het in 2017 tijdens de algemene ledenvergadering voorleggen aan zijn leden.

5.7.2 Certificeringen

Certificeringsmechanismen voor gegevensbescherming, gegevensbeschermingszegels en -merktekens kunnen de naleving van de AVG op een transparante manier aantonen. De toezichthoudende autoriteit en het Europese Comité kunnen certificaten vaststellen. Ook hier geldt dat ze een onafhankelijk en deskundig orgaan accrediteren voor het afgeven, verlengen en intrekken van certificeringen. De certificering is vrijwillig en op een transparante wijze toegankelijk voor iedere organisatie.

Zo biedt de brancheorganisatie voor data-gedreven marketingactiviteiten (DDMA = Data Driven Marketing Association) een Privacy Waarborg aan. Bedrijven die deze waarborg onderschrijven, verplichten zich tot een verantwoorde omgang met persoonsgegevens. De Privacy Autoriteit controleert of de bedrijven zich houden aan de wettelijke vereisten rond het recht op informatie, inzage, gericht gebruik en de toestemmingsvereiste. Ook controleert de Privacy Autoriteit of het bedrijf voldoende is toegerust op een verantwoorde verwerking van gegevens. Ze controleert bijvoorbeeld de aanwezigheid van een toegangsregeling voor toegang tot en verwerking van de data, beveiliging (ISO-gecertificeerd), het inschakelen van bewerkers en de aanwezigheid van bewerkersovereenkomsten. Het bij herhaling

niet voldoen aan de vereisten van de waarborg kan tot uitsluiting van het betreffende bedrijf leiden. De waarborg is nu gebaseerd op de Wbp, maar zal bij de introductie van de AVG daarop worden aangepast.

Een ander voordeel van de genoemde gedragscodes en certificeringen heeft te maken met de boetes die de AP oplegt. Hierbij houdt de AP rekening met de vraag of de betreffende instantie bij een dergelijk initiatief is aangesloten. Het is dus erg aantrekkelijk om aansluiting te zoeken. Uiteraard staat het partijen ook vrij om een gedragscode te ontwerpen die zij niet ter goedkeuring aan de AP voorleggen. Een dergelijke gedragscode zal uniformiteit met zich meebrengen, maar niet dezelfde waarde hebben als hiervoor uiteengezet.

5.7.3 Interoperabele formaten ten behoeve van dataportabiliteit

De consument kan op basis van de AVG een organisatie verzoeken om een digitaal verwerkbare kopie van de persoonsgegevens te leveren die hij eerder zelf heeft verstrekt. Dit moet gebeuren in een gestructureerd, gangbaar, machine-leesbaar en interoperabel formaat. Daarnaast kan een consument verzoeken zijn persoonsgegevens direct door te zenden aan een andere verwerkingsverantwoordelijke, mogelijk een andere organisatie binnen de branche. Dit laatste verzoek hoeven ze echter alleen te faciliteren als dit technisch mogelijk is voor beide partijen.
De AVG moedigt aan om interoperabele formaten te ontwikkelen die gegevensoverdraagbaarheid mogelijk maken. Dit kunnen we doortrekken naar het ontwikkelen van manieren om informatie direct door te sturen naar andere partijen. Dit is overigens een advies richting organisaties, geen verplichting.

De Artikel 29-werkgroep legde kortgeleden een eerste guidance voor waarin dataportabiliteit verder staat omschreven. Hier staan echter geen standaarden in beschreven. In de toekomst is het mogelijk dat er standaarden per branche komen. Naar verwachting zullen grote partijen (zoals Google, Amazon) hun eigen standaarden naar voren schuiven, maar in de praktijk zal blijken hoe de markt hierop reageert.

Voorbeeld
Een klant verhuist en beslist om een nieuwe inboedelverzekering af te sluiten, direct bij een andere verzekeraar. De klant kan van een aantal diensten gebruikmaken om zijn proces te vergemakkelijken en de bescherming van zijn persoonsgegevens te verzekeren, zoals dataportabiliteit bij het oversluiten. De 'oude' verzekeraar verschaft de persoonsgegevens in een elektronisch formaat, die de klant kan doorsturen naar de 'nieuwe' verzekeraar. Voor een grotere klanttevredenheid kan de 'oude' verzekeraar aanbieden om de gegevens rechtstreeks met de 'nieuwe' verzekeraar te delen.

De klant dient daarnaast een verzoek in bij zijn tussenpersoon om vergeten te worden. Dit betekent dat de tussenpersoon alle persoonsgegevens waar hij over beschikt, verwijdert en de verzekeraar verzoekt om hetzelfde te doen. De verzekeraar verwijdert vervolgens alle persoonsgegevens en verzoekt bijvoorbeeld zijn provider om hetzelfde te doen.

Opties voor samenwerking rond ROPG

In het vorige hoofdstuk kwamen de belangrijkste kansen voor de verzekeringsbranche aan bod. In het perspectief van deze kansen kunnen we ook de opties voor samenwerking rond ROPG in het non-competitieve domein in kaart brengen. De opties voor samenwerking rond ROPG staan in dit hoofdstuk centraal. We beschrijven de beschikbare opties, maar maken geen keuze.

Onderstaande tabel toont de diverse opties voor samenwerking, waarbij de intensiteit van die samenwerking van links naar rechts toeneemt. De optie dat alle partijen hun eigen gang gaan en zelf hun positie bepalen, bespreken we niet.

Laag ←	Intensiteit van samenwerking	→ Hoog
Bepalen van positie	**Ontwikkelen kaders en instrumenten**	**Implementeren toepassingen**
• Uitvoeren consumentenonderzoek • Organiseren rondetafelsessies • Defieniëren uitgangspunten * Opstellen whitepaper	• Bepalen welke gegevens verstrekt moeten worden • Ontwikkelen compliance raamwerk • Opstellen afwegingskaders • Formuleren gedragscodes • Initiëren en zeker stellen • Keurmerken en waarborgen • Ontwikkelen open API-raamwerk	• Omarmen breed inzetbare authenticatievoorzieningen • Toepassen gegevensuitwisseling ten behoeve van dataportabiliteit • Verder benutten Mijnverzekeringenopeenrij • Implementeren afsprakenstelsel branche • Implementeren afsprakenstelsel sector-overschrijdend

Het creëren van inzicht en overzicht staat niet in de tabel. Dit greenpaper is daarvoor namelijk een middel. Bij het creëren van inzicht/overzicht gaat het om het op een rij zetten van de opties voor samenwerking en uitdagingen. Dit biedt een kapstok voor het maken van keuzes. Het zorgt voor een gemeenschappelijk vertrekpunt en vocabulaire en vermindert kosten voor ketenpartijen bij de oriëntatie en het maken van keuzes.

6.1 Bepalen van positie

Bij het **bepalen van positie** brengen partijen het inzicht en het overzicht een stap verder door het maken van keuzes in welke richting de branche zich bij voorkeur wel/niet moet ontwikkelen.

Het consumentenonderzoek uit hoofdstuk 2 geeft geen eenduidig beeld wat de consument van ROPG verwacht. Additioneel kwalitatief en kwantitatief onderzoek gericht op ROPG in de verzekeringsbranche, biedt een handvat voor het maken van de genoemde keuzes.

Daarnaast is het nodig een richtinggevend dialoog tussen de belangrijkste stakeholders te voeren. Hierbij streven we naar een gezamenlijk voordeel en stellen we samen een plan op voor vervolgacties. Het gaat bij positiebepaling om de grote lijnen. Inzicht in de samenhang tussen de verschillende aspecten van ROPG is belangrijker dan een gedetailleerde analyse van alle aspecten afzonderlijk. Vervolgens werken partijen individueel oplossingen uit. Het voordeel van dit scenario is dat leveranciers van oplossingen zich kunnen richten op een aantal uitgangspunten. Dit maakt risico's rond investeringen beheersbaarder.

Enkele middelen om dit te ondersteunen:
- Uitvoeren representatief onderzoek onder consumenten. Hierbij staat de vraagkant ten aanzien van ROPG in de verzekeringsbranche centraal;
- Definiëren en vaststellen uitgangspunten; specificeren van de principes voor ROPG in het verlengde van rondetafelsessies;
- Opstellen whitepaper: een whitepaper kiest nadrukkelijk positie over hoe de branche omgaat met ROPG.

6.2 Kaders en instrumenten ontwikkelen

Het gaat hier onder andere om het vaststellen van een gemeenschappelijke, afgebakende set gegevens die verzekeraars etc. gaan leveren en waardoor we duidelijkheid creëren naar de buitenwereld (AP, AFM, consument etc.). Verder gaat het om het ontwikkelen van een gemeenschappelijk kader waarmee ketenpartijen op transparante, reproduceerbare wijze een eigen, goed onderbouwde afweging kunnen maken. Een afweging die rekening houdt met hun eigen context. Zo kunnen ze voldoen aan de AVG en inspelen op de kansen. Het kader moet voldoende flexibel zijn om nieuwe ontwikkelingen snel te accommoderen. Iedere organisatie genereert (vroeg of laat) zelf kaders rond ROPG. In dit verband is het de kunst om al deze kaders op elkaar af te stemmen en tot overeenstemming op brancheniveau te komen.

Bij het ontwikkelen van instrumenten bedoelen we gedragscodes, keurmerken en waarborgen met een richtinggevende, disciplinerende en sturende werking. Ook hier is dialoog en draagvlak op brancheniveau nodig.

6.2.1 Bepalen welke gegevens nodig zijn

Een belangrijk thema rond ROPG is de vraag welke gegevens een verzekeraar, volmacht of intermediair moet verstrekken op het moment dat de consument erom vraagt. Overheid en toezichthouders laten het afweten wat betreft een exacte duiding en interpretatie.
Dit leidt tot een Gordiaanse knoop: bescherming van de consument versus interpretatie en uitvoering. De slechte brug tussen doel en route levert grote risico's op voor de markt:

1. Ondernemerschap (kans op succes);
2. Durf (aansprakelijkheid/compliance);
3. Reputatie van de sector (dreigt verlamd te raken).

Het lijkt belangrijk om op brancheniveau afspraken te maken. Hoe ver gaat dat recht en wanneer verstrekken we wel/niet welke gegevens?

- Van wie zijn de gegevens uit de auto (of een ander apparaat in de Internet of Things) die bij een ongeluk betrokken is? Van de consument, de fabrikant, de wegbeheerder of de politie?
- Moet de consument inzage krijgen in een risicoprofiel dat op basis van zijn gegevens is opgesteld?
- Welke gegevens mogen partijen wel/niet vastleggen over 'klantbeelden'? Dit is een verzameling van gegevens over een consument. Welke gevolgen (aparte behandeling) mag een klantprofiel hebben? Als zo nieuwe gegevens ontstaan (bijvoorbeeld een risico-score), welke rechten heeft de consument dan met betrekking tot die gegevens?

6.2.2 Ontwikkelen compliance-raamwerk

We moeten voorkomen dat iedere ketenpartij zelf de wet- en regelgeving interpreteert. Hierdoor maken we onnodig veel kosten en ontstaan mogelijk ook verschillen in interpretatie en toepassing. Dit kan verwarrend werken voor de consument. Regelgevende en juridische eisen worden steeds strenger, ook vanuit Europa. Hierdoor neemt het belang van een robuust compliance-raamwerk op brancheniveau toe. Het raamwerk maakt interpretatie en toepassingen van wet- en regelgeving vanuit het collectief mogelijk.

Bij het Verbond van Verzekeraars is al één en ander beschikbaar in een compliance portal. De commissie Privacy van het Verbond zal extra duiding geven rondom de AVG. Hergebruik voor andere partijen dan verzekeraars wordt dan mogelijk ook bespreekbaar.

6.2.3 Opstellen afwegingskaders

Het streven moet zijn om steeds meer via de principes van persoonlijk datamanagement te werken; één van de oplossingen is een verdere invulling van Privacy by Design. Deze uitgangspunten geven organisaties houvast om de organisatie adequaat in te richten op inzage- en correctierecht, waarbij de consument bijvoorbeeld toestemming kan geven voor het gebruik van gegevens. Ook de Autoriteit Persoonsgegevens benadrukt dat Privacy by Design een passende wijze is om vorm te geven aan informatiebeveiliging, de borging van privacy en de bescherming van de persoonlijke levenssfeer.

Het formuleren van afwegingskaders zorgt ervoor dat we niet iedere keer het wiel opnieuw hoeven uit te vinden, en minder een beroep hoeven te doen op privacy-experts. Tegenwoordig werken volgens schattingen tussen de 1.000 en 2.000 privacy-adviseurs, in het bijzonder bij de grote multinationals. Volgens VNO/NCW zijn tot wel 25.000 specialisten nodig om aan de enorme vraag uit de markt te voldoen en om voor mei 2018 het gebruik van data in lijn te brengen met de Europese vereisten. Het gat tussen vraag en aanbod is volgens deskundigen zo groot dat het tot een goudkoorts onder interne en externe privacy-adviseurs leidt.
Volgens het periodieke Privacy-Governance-onderzoek van PWC onder ruim tweehonderd organisaties in Nederland, zegt één op de tien Nederlandse organisaties klaar te zijn voor nieuwe Europese privacywetgeving. Twee derde bereidt zich actief voor op de EU-verordening en een kwart is nog niet met de voorbereiding gestart.

6.2.4 Formuleren gedragscodes

Verzekeraars aangesloten bij het Verbond van Verzekeraars vallen al onder de gedragscode Verwerking Persoonsgegevens Financiële Instellingen (2010). Deze gedragscode bepaalt welke gegevens verzekeraars mogen verwerken en hoe ze dit moeten doen. De gedragscode werkt de algemene verplichtingen uit de Wet bescherming persoonsgegevens specifiek voor verzekeraars nader uit.
Het Verbond van Verzekeraars werkt zelf aan een nieuwe privacy-gedragscode. Deze legt het in 2017 tijdens de algemene ledenvergadering voor aan zijn leden. Voor de rest van de branche is het zaak om te beslissen om hierbij aan te sluiten, een eigen versie te maken of hier niet aan mee te doen.

Een optie is een gesloten norm op brancheniveau te ontwikkelen, met hierin beschrijvingen waaraan partijen minimaal moeten voldoen. Hierdoor kan de branche tegen lagere kosten sneller compliant zijn. Best practices kunnen verduidelijken hoe we met de norm moeten omgaan.

6.2.5 Initiëren en vaststellen keurmerken en waarborgen

Een gedragscode heeft een intern disciplinerende en sturende werking. Het keurmerk of de waarborg is een ander instrument dat meer op consumenten is gericht. Deze borgt kwaliteit, ondervangt bepaalde zorgen bij de consumenten, creëert mogelijkheden voor beroep en draagt zo bij aan de ‘accountability’ van een bedrijf.

6.2.6 Ontwikkelen open API-raamwerk

In toenemende mate maken toepassingen gebruik van webservices van andere organisaties. Het kenmerk van een webservice is dat twee machines direct met elkaar communiceren over een netwerk (synchrone communicatie). Bijvoorbeeld tariefberekening vanuit een vergelijker. Eén of meerdere webservices beschikbaar stellen aan derden heet API (Application Programming Interface). Vrij vertaald

zijn dit eenvoudig te gebruiken webservices om diensten of delen daarvan te ontsluiten. API's vormen voor steeds meer organisaties de sleutelrol in het aanbieden van transacties, het distribueren van content of het ontsluiten van een workflow tussen schakels in de keten. API's zijn toenemend randvoorwaardelijk voor (digitaal) zakendoen en brengen organisaties en branches tot het formuleren van een open API-raamwerk. De meerwaarde van een open API-raamwerk voor de verzekeringsbranche:

- het maakt inzichtelijk welke functies/services beschikbaar zijn;
- het zorgt waar mogelijk voor een eenduidige werking over partijen heen;
- het stelt normen voor beveiliging, authenticatie, performance en beschikbaarheid;
- het borgt een goede toegankelijkheid van onlinediensten, ook voor ROPG;
- het maakt cocreatie mogelijk waarbij derden (alleen of in een groep) toepassingen kunnen ontwikkelen op basis van / in het verlengde van aangeboden webservices.
- het voorkomt een 'vendor en data lock-in'. Consumenten kunnen hun gegevens gestructureerd langs een afsprakenstelsel opvragen zonder dat daar een (technisch) platform aan ten grondslag ligt. Zo is het mogelijk om te kunnen wisselen van aanbieder zonder dat daarbij direct alle 'eigen' data verloren gaan. Niet één partij bepaalt het ecosysteem.

6.3 Implementeren toepassingen

Het **implementeren** van werkende **toepassingen** voor ROPG stelt de consument in staat regie te voeren over zijn persoonsgegevens. Adequate authenticatievoorzieningen zijn randvoorwaardelijk. Afhankelijk van de toepassing stellen we requirements op, werken we ze uit in specificaties en starten we ontwikkel-, test-, pilot- en uitroltrajecten. Krachtenbundeling rond het ontwikkelen van toepassingen draagt bij aan verlaging van risico's en kosten en versnelling van implementatie. Dit alles met inachtneming van ieders commerciële belang. Dit is dus anders dan bij de invoering van afsprakenstelsels waar de uitdagingen liggen op het terrein van het traditionele kip-ei-vraagstuk en het reduceren van complexiteit.
De market entry-uitdaging is de uitdaging om een momentum te creëren waarbij zowel consumenten als dienstverleners belang hebben om mee te doen.

6.3.1 Omarmen breed inzetbare authenticatiemiddelen

Regie over persoonsgegevens is alleen mogelijk als we met voldoende zekerheid kunnen vaststellen of een persoon daadwerkelijk is wie hij beweert te zijn. Daarnaast veronderstelt regie door de consument ook dat het gaat om laagdrempelig in te zetten authenticatiemiddelen. Bij voorkeur middelen die breed inzetbaar zijn en we vaak gebruiken. Het perspectief voor de verzekeringssector is dat in 2017 alle Nederlanders met hun bancaire authenticatiemiddelen via iDIN kunnen inloggen bij alle online dienstverleners. Dit laatste onder de voorwaarde dat die dienstverleners dit mogelijk maken via een aansluiting op iDIN. Mijnverzekeringenopeenrij kan hier als hefboom fungeren.
Op langere termijn biedt Idensys ook mogelijkheden.

6.3.2 Toepassen gegevensuitwisseling voor dataportabiliteit

Voor verzekeringen zijn standaarden ontwikkeld (AFD, AFD-berichten, afspraken over syntax en transportmogelijkheden) die organisaties kunnen inzetten om het advies van de AVG op te volgen. Interoperabele formaten ontwikkelen die gegevensoverdraagbaarheid mogelijk maken. SIVI kan hiervoor het complete instrumentarium ontwikkelen. Dataportabiliteit draagt bij aan het door de DNB (december 2016) bepleite centraal stellen van de klant.

6.3.3 Verder benutten Mijnverzekeringenopeenrij

Het delen van data met derden en intermediairs is een kans die ontstaat in het verlengde van dit consumentenplatform. Een andere mogelijke functie van dit platform is het doorgeven van wijzigingen in persoonsgegevens aan alle relevante verzekeraars, volmachten en eventueel ook intermediairs.
De kwaliteit van de gegevens gaat hierdoor omhoog. De kwaliteit van de gegevens is nu vaak wel een issue, zeker als na het sluiten van de verzekering geen klantcontact meer is, bijvoorbeeld bij uitvaartverzekeringen.

6.3.4 Implementatie afsprakenstelsel

Het branchebreed uitrollen van een branchespecifiek of sector-overstijgend afsprakenstelsel is vooral een organisatorische uitdaging. Veel ketenpartijen vinden het vaak een goed idee, maar gaan pas meedoen als het een succes wordt, terwijl het pas een succes wordt als iedereen meedoet.

6.4 Tot slot

SIVI en de Werkgroep Strategische Verkenning SIVI 2016 geven met dit greenpaper een aanzet tot de strategische discussie rond samenwerking binnen onze branche. Een discussie die gaat over de meest optimale vormen van samenwerking binnen de nieuwe AVG-regelgeving, en in het verlengde van de kansen die de diverse ROPG-initiatieven bieden. Diverse ROPG-initiatieven en de nieuwe privacy wetgeving stellen de consument centraal. Door samenwerking in de verzekeringsbranche kan de consument gefaciliteerd worden om laagdrempelig regie te voeren over zijn persoonsgegevens; de consument bepaalt! Dit greenpaper levert een bijdrage aan de afwegingen die daar bij horen. Duidelijk is dat door samenwerking bijgedragen wordt aan herstel van vertrouwen van de consument in verzekeraars en intermediairs. In 2017 zal door SIVI actief de dialoog worden gezocht om te komen tot gerichte besluitvorming en acties op dit interessante en bovenal belangrijke dossier.

Nawoord

Een belangrijk doel van SIVI is het bijdragen aan een efficiënte en stabiele verzekeringssector:

- non-concurrentiële ketenintegratievraagstukken binnen de distributie gezamenlijk oppakken met de verwachting versnelling en kostenvoordelen te realiseren;
- ketenintegratiestandaarden ontwikkelen en onderhouden in een steeds sneller veranderende omgeving en het gebruik van standaarden voor digitaal zakendoen bevorderen.

Deze doelstellingen dragen bij aan het streven van de DNB naar een duurzame, stabiele, efficiënte en maatschappelijk dienstbare verzekeringssector.

SIVI ontwikkelt en beheert standaarden voor digitaal zaken doen in de verzekeringsbrance. Onafhankelijk en deskundig. Gebaseerd op inzichten om kosten te verlagen en waarde toe te voegen. Inzichten die verder reiken dan de standaarden alleen. SIVI analyseert trends, onderzoekt de impact van nieuwe technologieën en inspireert alle ketenpartners om samen nieuwe stappen te zetten. Met de ambitie om digitaal verkeer voor de sector en de consument te laten werken. De consument, die steeds hogere eisen stelt aan gemak, zekerheid en veiligheid en die 'vertrouwen' tegenwoordig met hoofdletters schrijft. Het succesvol bedienen van de digitale consument vraagt om de eenduidigheid van standaarden en de inspiratie van nieuwe mogelijkheden. SIVI wil een meer strategische dialoog met de branche ontwikkelen rond technologische vernieuwing en/of ketenoptimalisatie. Eén van de manieren waarop SIVI dit wil bereiken is door periodiek met een strategische werkgroep van vertegenwoordigers uit de branche een onderwerp uit te diepen. Deelnemers werken samen aan het creëren van een concrete deliverable rondom een door de deelnemers gekozen thema. De SIVI-werkgroep Strategische Verkenning 2016 koos het thema Regie Op Persoonsgegevens met als deliverable een greenpaper.

Dit greenpaper kwam tot stand in samenwerking met de volgende personen:

Organisatie	**Vertegenwoordiger**
Achmea	Emil Verheijen
Adfiz	Frank Colijn
a.s.r.	Paul van Raaij
Goudse	Bernardo Walta
Multisafe	Michael Mackaaij
Nationale Nederlanden	Kees Kool
Noordhollandsche van 1816	Cas Verhage
Verbond van Verzekeraars	Fred Treur
VIVAT	John Agterdenbos
Zicht	Gert Timmermans

Stichting SIVI
Pythagoraslaan 101
3584 BB Utrecht
Postbus 1092, 3700 BB Zeist

T 030 698 80 90
F 030 698 80 99
E info@sivi.org
I www.sivi.org

KvK 34204332
BTW NL813657593B01 IBAN
NL91INGB0670985406
BIC INGBNL2A