



Monitor Persoonlijk Data Management

– Regie op (Financiële) Gegevens –

- Bijlagen -



Utrecht, 1 augustus 2021

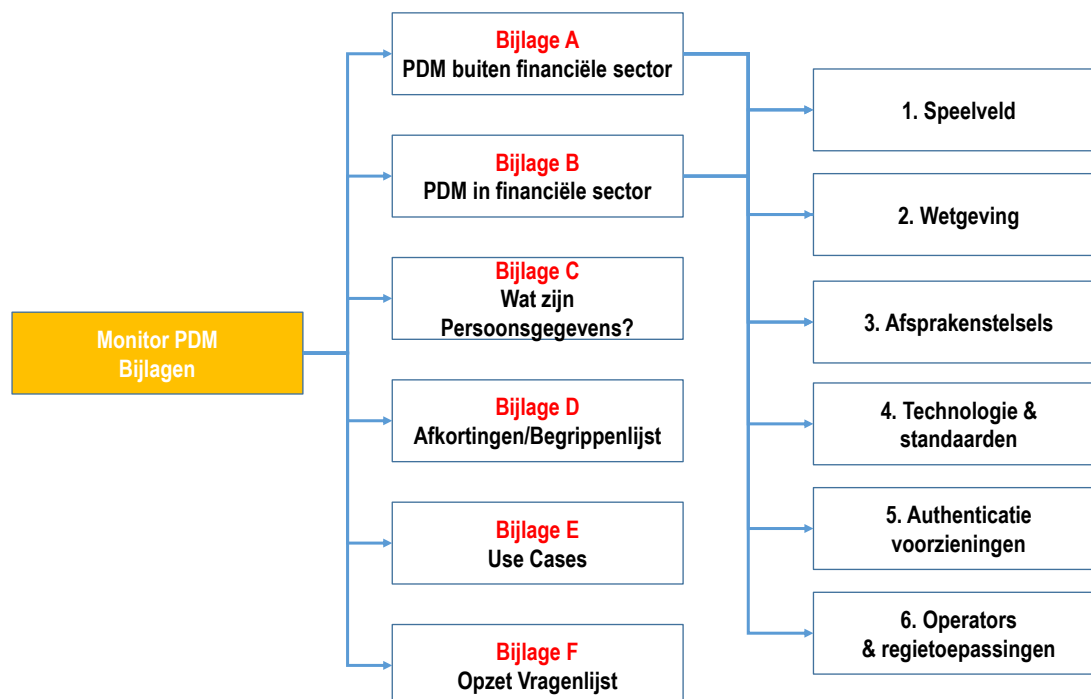
INHOUDSOPGAVE

KORTE INHOUDSOPGAVE PDM MONITOR.....	5
1. BIJLAGE A - PDM BUITEN FINANCIËLE SECTOR.....	6
1.1 SPEELVELD.....	7
1.1.1 Autoriteiten.....	7
1.1.2 Belangenorganisaties	9
1.1.3 Communities en programma's.....	12
1.1.4 Overheid	20
1.1.5 Wetenschappelijke instituten	28
1.2 WETGEVING.....	30
1.2.1 Wetgeving over eigendom van gegevens	30
1.2.2 Wet algemene bepalingen Burgerservicenummer (Wabb)	30
1.2.3 Algemene Verordening Gegevensbescherming (AVG).....	30
1.2.4 eIDAS	35
1.2.5 Wet Digitale Overheid (WDO)	36
1.2.6 Wet modernisering elektronisch bestuurlijk verkeer.....	37
1.2.7 Wet op de Identificatieplicht (WID)	37
1.2.8 Wet afwikkeling massaschade in collectieve actie (WAMCA).....	37
1.2.9 Archiefwet	38
1.2.10 Wet Geneeskundige Behandelovereenkomst (WGBO)	38
1.2.11 Wet cliëntenrechten bij elektronisch verwerking van gegevens	38
1.2.12 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)	39
1.2.13 Wegiz.....	39
1.2.14 Diverse wet- en regelgeving voor bronnen van aanbieders	40
1.2.15 Europa	40
1.3 AFSPRAKENSTELSELS	42
1.3.1 Inleiding	42
1.3.2 MedMij	42
1.3.3 Qiy.....	45
1.3.4 iSHARE.....	46
1.4 TECHNOLOGIE EN STANDAARDEN	46
1.4.1 Self Sovereign Identity (SSI)	47
1.4.2 Sovrin.....	47
1.4.3 Zero knowledge proof.....	47
1.4.4 Idemix	49
1.4.5 X-tee	50
1.4.6 NLX.....	51
1.4.7 NUTS.....	51
1.4.8 JLINC.....	51
1.4.9 Open Authorization (OAuth)	52
1.4.10 User Management Access (UMA)	52
1.4.11 OpenID, SAML.....	52
1.4.12 openBadges.....	53
1.4.13 PKIoverheid	53
1.4.14 OpenAPI Specification (OAS).....	54
1.4.15 REST-API Design Rules.....	54
1.5 AUTHENTICATIEVOORZIENINGEN	54
1.5.1 Elektronische toegangsdiensten (ETD)	55
1.5.2 eHerkenning	55
1.5.3 Digitale Bron Identiteit.....	56
1.5.4 iDIN	57
1.5.5 EduGAIN.....	58
1.5.6 SURFconext	58
1.5.7 DigiD	58
1.5.8 Itsme	59
1.5.9 Cleverbase ID	59

1.5.10	EduID.....	60
1.5.11	NotarisID.....	60
1.5.12	Attribuut gebaseerde authenticatie Medmij.....	60
1.5.13	Verimi.....	60
1.6	NATIONALE PDM-DIENSTEN.....	61
1.6.1	Inleiding.....	61
1.6.2	Blauwe Knop.....	61
1.6.3	MijnOverheid.....	61
1.6.4	IRMA.....	62
1.6.5	Dappre.....	63
1.6.6	Ivido.....	63
1.6.7	Health Apps.....	63
1.6.8	Diabetesdiensten.....	64
1.6.9	Emrex.....	64
1.6.10	Qlik2Share.....	64
1.6.11	Diplomaregister.....	65
1.6.12	FeatherFeed.....	65
1.6.13	JiD.....	65
1.6.14	MijnApp.....	66
1.6.15	Qii.....	66
1.7	INTERNATIONALE PDM-DIENSTEN.....	67
1.7.1	Inleiding.....	67
1.7.2	Geens NPO.....	67
1.7.3	MyDex.....	67
1.7.4	Meeco.....	68
1.7.5	Digi.me.....	68
1.7.6	Solid.....	69
1.7.7	Personium.....	70
1.7.8	MyFairData.....	70
1.7.9	MyDataShare.....	70
1.7.10	MyLife Digital.....	71
1.7.11	Cozy.....	71
1.7.12	iGrant.io.....	71
1.7.13	Comuny.....	71
1.7.14	Doccle.....	71
1.7.15	Kivra.....	72
1.7.16	BitsaboutMe.....	72
1.7.17	Fairdrop.....	73
1.7.18	Numbers.....	73
1.7.19	Onecub.....	73
1.7.20	OwnYourData.....	73
1.7.21	Polypoly.....	73
1.7.22	Streamr.....	73
1.7.23	VisionsTrust.....	74
2.	BIJLAGE B - PDM IN DE FINANCIËLE SECTOR.....	75
2.1	SPEELVELD.....	77
2.1.1	Autoriteiten.....	77
2.1.2	Belangenorganisaties.....	79
2.1.3	Communities en programma's.....	87
2.1.4	Overheid.....	88
2.1.5	Wetenschappelijke instituten.....	89
2.1.6	Digicampus.....	90
2.2	WETGEVING.....	90
2.2.1	PSD2.....	90
2.2.2	Wet op het financieel toezicht (Wft).....	93
2.2.3	Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).....	93
2.2.4	Hypotheekenrichtlijn MCD.....	94

2.2.5	<i>Pensioenwet</i>	94
2.2.6	<i>Wet gemeentelijke Schuldhulpverlening (Wgs)</i>	94
2.3	AFSPRAKENSTELSELS	94
2.3.1	<i>Zorgeloos Vastgoed</i>	94
2.4	TECHNOLOGIE EN STANDAARDEN	95
2.4.1	<i>Gegevensstandaard Persoonlijke Financiën (GPF)</i>	95
2.4.2	<i>SIVI All Finance Standaard (AFS)</i>	96
2.4.3	<i>Consumentendata standaard HDN</i>	98
2.4.4	<i>Ockto Brondata Service</i>	98
2.4.5	<i>Standaarden Betalingsverkeer</i>	99
2.4.6	<i>NextGenPSD2 Framework</i>	100
2.5	AUTHENTICATIEVOORZIENINGEN	100
2.6	PDM-DIENSTEN	100
2.6.1	<i>PDM-Diensten</i>	100
2.6.2	<i>Planningstools</i>	105
2.6.3	<i>Huishoudboekjes</i>	108
2.6.4	<i>Tools bij schuldhulpverlening en voorkomen van schulden</i>	110
2.6.5	<i>Klantmappen</i>	112
2.6.6	<i>Toegang tot klantmappen: Apps</i>	114
2.7	INTERNATIONALE PDM-DIENSTEN	115
2.7.1	<i>Yolt</i>	115
2.7.2	<i>DataYogi</i>	115
2.7.3	<i>N26 Online Bankieren</i>	115
2.7.4	<i>Swish</i>	115
2.7.5	<i>Satispay</i>	116
2.7.6	<i>Mint</i>	116
2.7.7	<i>Finanda</i>	116
2.7.8	<i>Plaid</i>	116
2.7.9	<i>Saltedge</i>	117
2.7.10	<i>Eurobits</i>	117
2.7.11	<i>Envestnet / Yodlee</i>	117
2.7.12	<i>MX</i>	117
2.7.13	<i>Finicity</i>	118
2.7.14	<i>CashEdge (Fiserv)</i>	118
2.7.15	<i>Kontamatik</i>	118
2.7.16	<i>Tink</i>	118
3.	BIJLAGE C - WAT ZIJN PERSOONSgegevens?	119
4.	BIJLAGE D – AFKORTINGEN- EN BEGRIPPENLIJST	121
4.1	AFKORTINGEN	121
4.2	GEDEFINIEERDE BEGRIPPEN	122
4.3	DEFINITIES	124
5.	BIJLAGE E – USE CASES	141
5.1	INLEIDING	141
5.2	FINANCIËLE APK	141
5.3	HET OPSTELLEN VAN EEN PERSOONLIJK FINANCIËEL PLAN	142
5.4	HYPOTHEEKADVIES	143
6.	BIJLAGE F – OPZET VRAGENLIJSTEN	146
6.1	VRAGENLIJST PDM-DIENSTEN	146
6.2	VRAGENLIJST PDM AFSPRAKENSTELSELS	148

KORTE INHOUDSOPGAVE PDM MONITOR



1. BIJLAGE A - PDM BUITEN FINANCIËLE SECTOR

Dit hoofdstuk richt zich op de initiatieven rond PDM buiten de financiële sector:

1. Speelveld;
2. Wetgeving;
3. Technologie en standaarden;
4. Authenticatievoorzieningen;
5. Afsprakenstelsels;
6. Operators.

Speelveld	Wetgeving	Afsprakenstelsels
Autoriteiten - Autoriteit Persoonsgegevens - European Data Protection Supervisor - European Data Protection Board - Autoriteit Consument en Markt - Agentschap Telecom	- Wetgeving over eigendom van gegevens - Wet algemene bepalingen Burgerservicenummer - Algemene Verordening Gegevensbescherming - eIDAS	- Elektronische Toegangsdiensten - Medmij - Qiy - iShare
Belangenorganisaties - Consumentenbond - Bureau Européen des Unions de Consommateurs - Bits Of Freedom - Patiëntenfederatie Nederland - Data Driven Marketing Association - Privacy Collective - Schluss	- Wet Digitale Overheid - Wet op de Identificatieplicht - Wet afwikkeling massaschade in collectieve actie - Archiefwet - Wet Geneeskundige Behandelovereenkomst - Wet cliëntenrechten bij elektronisch verwerking van gegevens	
Communities en programma's - Holland Health Data Coöperatie - Tada - Common Ground - Blauwe Knop Programma - Machtigen - i4Sociaal - EDUmij - Leven Lang Ontwikkelen - Dutch Blockchain Coalition - Data Sharing Coalition - Alliance for the Freedom of Car Repair - Sitra/IHAN - Personal Data Ecosystem Consortium - International Data Spaces Association	- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg - Wegiz - Diverse wet- en regelgeving voor bronnen van aanbieders - Europa: Data Act - Europa: Single Digital Gateway - Europa: Data Governance Act	
Overheid - Kabinet Rutte-III - Wetenschappelijke Raad voor het Regeringsbeleid - ICT Uitvoeringsorganisatie - Rijksdienst voor identiteitsgegevens - Estland - Australië		
Wetenschap - Stichting Privacy By Design - Privacy & Identity Lab - OpenPDS		

Technologie/Standaarden	Authenticatievoorzieningen	PDM-Diensten
- Self Sovereign Identity - Sovrin - Zero Knowledge Proof - Idemix - X-tee - NLX - NUTS - JLINC - OAuth - UMA - OpenId, SAML - OpenBadges - PKIOverheid - OpenAPISpecfication - REST-API Design Rules	- Elektronische Toegangsdiensten - eHerkenning - Digitale Bron Identiteit - iDIN - EduGain - SURFconext - DigiD - Itsme - Cleverbase ID - EduID - NotarisID - Attriboot gebaseerde authenticatie MedMij - Verimi	Nationaal - Blauwe Knop - MijnOverheid - IRMA - Dappre - Ivdo - Health Apps - Diabetesdiensten - Emrex - Qlik2Share - Diplomaregister - FeatherFeed - JiD - MijnApp - Qii Internationaal - GeensNPO - Mydex - Meeco - Digi.Me - Solid - Personium - MyFairData - MyDataShare - MyLife Digital - Cozy - iGrant.io - Comuny - Doccle - Kivra - BitsaboutMe - Fairdrop - Numbers - Onecub - OwnYourData - Polypoly - Streamr - VisionsTrust

1.1 Speelveld

Het speelveld rond PDM bestaat uit drijvende krachten achter de (door)ontwikkeling van technologie, standaarden, juridische kaders, oplossingen en governance rondom PDM.

Dit betreft op alfabetische volgorde:

- Autoriteiten
- Belangenorganisaties
- Communities en programma's
- Overheid
- Wetenschappelijke instituten

1.1.1 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.

1.1.1.1 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. Meest recent heeft de Autoriteit Persoonsgegevens geadviseerd ten aanzien gebruik van de Coronamelder.



AUTORITEIT
PERSOONSgegevens

1.1.1.2 European Data Protection Supervisor (EDPS)

De EDPS houdt toezicht op de verwerking van persoonsgegevens bij de instellingen en organen van de EU.

De EDPS heeft in 2014 het Internet Privacy Engineering Initiative (IPEN-initiatief¹) opgericht om de allernieuwste privacy techniek te promoten en vooruit te helpen. Het ondersteunt ingenieurs die werken aan (her) bruikbare bouwstenen, ontwerp patronen en andere tools voor geselecteerde internet use cases waar privacy in het geding is. Het slaat bruggen met privacy- en gegevensbeschermingsdeskundigen van andere disciplines en bevordert een breder begrip van de technologieën die de bescherming van persoonsgegevens mogelijk maken. Het algemene doel is om gegevensbescherming en privacy te integreren in alle fasen van het ontwikkelingsproces, van de fase van vereisten tot productie, afhankelijk van het ontwikkelingsmodel en de applicatieomgeving. IPEN biedt een repository van relevante bronnen op de IPEN Wiki², waardoor de bevindingen en kennisbank toegankelijk zijn voor alle deelnemers, ontwikkelaars en privacy-experts.

Juni 2020 publiceerde EDPS haar strategie tot 2024³.



1.1.1.3 European Data Protection Board (EDPB)

Omdat de AVG een Europese wet is, is het belangrijk dat deze in alle EU-landen op dezelfde manier wordt uitgelegd en toegepast. Zo krijgt iedereen daadwerkelijk dezelfde privacybescherming en is sprake van duidelijkheid voor organisaties die in meerdere EU-lidstaten actief zijn. De privacytoezichthouders uit de EU werken hiertoe samen binnen de EDPB⁴. Onder meer door gezamenlijk onderzoek te doen. Daarnaast brengt de EDPB adviezen en besluiten uit. Een andere belangrijke taak is uitleg geven over de interpretatie en toepassing van de AVG in de vorm van guidelines. Met de komst van de EDPB is de Artikel 29 werkgroep (WP 29) opgeheven.



1.1.1.4 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.



De Autoriteit Consument & Markt (ACM) maakt onderdeel uit van het International Consumers Protection and Enforcement Network (ICPEN). Hierin zijn 27 toezichthouders verenigd en zij deden recent een oproep aan leveranciers van apps. Apple meldt binnenkort (begin 2021) in zijn appstore

¹ https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

² https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards

³ https://edps.europa.eu/press-publications/press-news/press-releases/2020/shaping-safer-digital-future-new-strategy-new_en

⁴ <https://edpb.europa.eu/>

welke persoonlijke gegevens een app gebruikt⁵. Consumenten kunnen bij het uitzoeken van een app in de app store dit aspect dan meewegen in hun keuze voor een bepaalde app. Dit prikkelt aanbieders om met elkaar te concurreren op gunstige privacy voorwaarden.

1.1.1.5 Agentschap Telecom

Agentschap Telecom voert sinds maart 2016 toezicht uit op het “Afsprakenstelsel Elektronische Toegangsdiensden” (waaronder eHerkenning).

In 2019 onderzocht de beveiliging van IoT-consumentenapparaten⁶.

Het eindrapport bevat de resultaten van onderzoek naar de veiligheid van 22 IoT-consumentenapparaten, te weten internet routers, connected toys, IP-camera's, slimme sloten, babyfoons en slimme thermostaten. Uit het onderzoek is gebleken dat vier van de 22 apparaten bevindingen hadden die als 'kritiek' werden geclassificeerd. Versleuteling en informatie-uitwisseling zijn onderdelen die nog verder verbeterd moeten worden, in het bijzonder waar de verwerking van persoonsgegevens plaatsvindt.



Agentschap Telecom
Ministerie van Economische Zaken

1.1.2 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.

Verscheidende belangenorganisaties zijn actief op het terrein van privacy en bescherming van persoonsgegevens.

1.1.2.1 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. De Consumentenbond ontwikkelde een Privacymeter. Hierbij wordt gecontroleerd of bedrijven de AVG-wetgeving respecteren en of ze gegevens niet onnodig met derde partijen delen⁷. Een voorbeeld is het onderzoek naar internetbankieren. Nieuwe 'mobiele banken' gaan volgens de Consumentenbond minder goed om met online privacy dan banken die al een tijdje meedraaien.



De Consumentenbond en de Data Privacy Stichting – die optreedt voor slachtoffers van privacy-inbreuken in Nederland - startten in juli 2020 een actie tegen Facebook. De inzet is dat Facebook zijn gebruikers in Nederland compensatie moet betalen voor het schenden van hun privacy. De Consumentenbond en de Stichting verwijten Facebook dat het jarenlang privégegevens van zijn gebruikers en hun Facebook-vrienden verzamelde en deze gegevens zonder toestemming toegankelijk maakte voor derden. Daar verdiende het bedrijf veel geld mee.

Eind 2020 lanceerde de Consumentenbond de app Voordeelcoach⁸. De app geeft inzicht in welke verzekeraar of energieleverancier voor consumenten voordelig is en geeft een signaal af wanneer het interessant is om over te stappen naar een andere aanbieder. Oversluiten kan ook via de Voordeelcoach en consumenten kunnen schades direct afhandelen via de app. De Voordeelcoach biedt toegang tot autoverzekeringen, zorgverzekeringen en energiecontracten. Begin 2021 voegt de

⁵ <https://www.acm.nl/nl/publicaties/apple-informeert-consumenten-appstore-over-datagebruik-apps-na-oproep-toezichthouders>

⁶ <https://www.agentschaptelecom.nl/onderwerpen/slimme-apparaten/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur>

⁷ <https://www.consumentenbond.nl/internet-privacy/hoe-werkt-de-privacymeter>

⁸ <https://www.consumentenbond.nl/nieuws/2020/consumentenbond-helpt-consumenten-besparen-met-voordeelcoach-app>

Consumentenbond daar woonhuisverzekeringen aan toe. Voor de Voordeelcoach werkt de Consumentenbond samen met digitaal verzekeringsplatform Swift.Online.

Opmerking

In de toepassing kan een gebruiker aangeven bij welke verzekeraars (volmachten/serviceproviders ontbreken) polissen lopen. De Consumentenbond vraagt vervolgens – met machtiging van de gebruiker - de polisgegevens bij de verzekeraar op. Deze worden dan handmatig verwerkt. Een steekproef maakt duidelijk dat verzekeraars hier niet aan meewerken omdat de polis privacygevoelige gegevens bevat: " Een polisblad versturen we niet per e-mail omdat hier vertrouwelijke gegevens op staan".

1.1.2.2 Bureau Européen des Unions de Consommateurs (BEUC)

De BEUC is de Europese koepelorganisatie voor consumentenorganisaties zoals de Consumentenbond. De BEUC heeft een actieve agenda rond ROPG 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 Europese Commissie en het Europees Parlement). Ze maakt brieven aan hen openbaar, vaardigt persverklaringen uit, publiceert position papers en informeert het publiek.

September 2020 kreeg BEUC van de Europese Commissie de toezegging dat zij de kwaliteit en objectiviteit van financieel advies gaat beoordelen⁹.



1.1.2.3 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. Bits of Freedom ontwikkelde in 2018 een tool, My Data Done Right, die personen in staat stelt om met AVG-wetgeving in de hand bij bedrijven en instellingen alle informatie op te vragen die zij over hem/haar hebben. Zomer 2020 wordt gewerkt aan een nieuwe versie van de toolbox. BoF promoot in plaats van WhatsApp Signal¹⁰, een berichtenapp die eind-tot-eind-versleuteling mogelijk maakt door het opensource Signal-protocol.



1.1.2.4 Patiëntenfederatie Nederland

Deze federatie vertegenwoordigt ruim 200 patiëntenorganisaties en heeft privacybescherming als speerpunt. Met hun initiatief MedMij pakken ze een actieve rol op het terrein van regie op persoonsgegevens. MedMij gaat zorgen dat de consument de regie voert over zijn persoonlijke gezondheidsomgeving.

In een brief van 30 september 2020 aan de Tweede Kamer pleit de federatie voor hybride zorg, de optimale combinatie van zorg op afstand én op de locatie van de zorgverlener¹¹.

De Patiëntenfederatie is de trekker van de PGO-alliantie. Deze alliantie bestaat uit patiënten-, branche-, consumenten- en welzijnsorganisaties. De PGO-alliantie is gevormd vanuit het programma PGO on Air. De PGO-alliantie wil meer bekendheid geven aan PGO's¹².



⁹ <https://www.beuc.eu/publications/consumers-potentially-one-small-step-closer-fairer-and-better-quality-financial-advice/html>

¹⁰ <https://signal.org/nl/>

¹¹ <https://www.patiëntenfederatie.nl/downloads/kamerbrieven/658-gegevensuitwisseling-gegevensbescherming-ict-e-health-slimme-zorg-administratieve-lasten-okt-2020/file>

¹² <https://www.patiëntenfederatie.nl/pgo-alliantie>

1.1.2.5 Data Driven Marketing Association (DDMA)

DDMA is namens meer dan 300 de vereniging voor marketing en data. Doel is de data-driven marketingsector op een hoger plan te tillen. DDMA eist van haar leden dat zij handelen binnen het kader van de wet en de gedragscodes. Leden worden ondersteund met advies op het gebied van datasecurity en privacy. Tevens is het keurmerk Privacy Waarborg in het leven geroepen. Volgens de DDMA Privacy Monitor 2019¹³, een door GFK uitgevoerd onderzoek onder 1.008 respondenten (representatief voor de Nederlandse internetpopulatie) - zien weinig consumenten (29%) nog de voordelen terug van het delen van persoonlijke gegevens. Een ruime meerderheid van de Nederlanders (88%) wil ook meer controle over de eigen gegevens die ze aan bedrijven verstrekken. Ruim de helft van de mensen heeft bijvoorbeeld het idee dat zij niet kunnen voorkomen dat bedrijven hun gegevens delen met derden of informatie over hen verzamelen.



Overige bevindingen van DDMA:

- Transparantie wordt door 94% belangrijk bevonden en makkelijk te lezen algemene voorwaarden door 93%. Maar consumenten verwachten dat bedrijven meer doen dan alleen voldoen aan hun wettelijke verplichtingen op privacygebied. Ze vinden het ook belangrijk dat de voordelen van het verstrekken van hun gegevens vanaf het begin duidelijk worden gemaakt (93%) en dat hetgeen zij voor het delen terugkrijgen volkomen helder is (93%). Ook stellen mensen flexibiliteit op prijs: ze willen een online omgeving waarin ze zelf hun gegevens kunnen inzien en wijzigen (93%) en zelf kunnen bepalen wat voor soort en hoeveel gegevens ze willen delen (92%).
- De bereidheid tot delen van data hangt bij Nederlanders in eerste instantie vooral af van praktische aspecten, niet zozeer van eventuele voordelen die mensen eruit halen. Mensen kijken eerder naar het soort gegevens waar om gevraagd wordt (62%), veiligheid (61%) en het doel van de gegevensvraag (58%). Beloningen of stimuli zijn dus secundair aan de basiscondities waaronder organisaties naar gegevens vragen.
- Als wordt gevraagd welke beloningen mensen ertoe aanzetten hun gegevens te delen, dan zorgen vooral financiële beloningen voor een hogere deelkans. Directe financiële beloningen (40%), gratis producten of diensten (29%) en korting (27%) vormen de top 3.
- Bepaalde gegevens worden door mensen als persoonlijker of meer privé gezien dan andere. Financiële informatie scoort met 92% het hoogst, gevolgd door medische gegevens, vingerafdrukken en genetische informatie (allemaal 87%). Locatiegegevens zijn dit jaar extra op de radar gekomen van mensen. De mate waarin locatiegegevens als privé worden gezien is ten opzichte van 2018 met 15% gestegen tot 83%. Daar komt bij dat de meeste mensen het ook niet fijn vinden dat bedrijven weten waar ze zijn: slechts 20% heeft hier geen problemen mee.

Volgens de Privacy Monitor 2021 zijn Nederlanders positiever over datagebruik. Het aantal mensen dat sceptisch is over het gebruik van data door organisaties is gedaald (van 25% naar 20%). 63% is tevreden met de hoeveelheid informatie die zij aan organisaties geven. Ook vinden meer mensen (van 29% naar 34%) dat de dienstverlening beter wordt als zij data delen, al vormt deze groep nog steeds een minderheid¹⁴.

1.1.2.6 Privacy Collective

The Privacy Collective¹⁵ is een stichting gericht op compensatie voor het onrechtmatig gebruik van persoonsgegevens. Zij doen dat door een collectieve juridische procedure. In augustus 2020 dienden ze een massaclaim¹⁶ in tegen Salesforce en Oracle wegens misbruik van persoonsgegevens. De claim richt zich op het verzamelen, bundelen, verrijken en verkopen van digitale profielen van Nederlandse internetgebruikers, zonder dat zij daar toestemming voor hebben gegeven.



¹³ <https://privacy-web.nl/publicaties/ddma-privacy-monitor-2019-bewustzijn-en-begrip-van-privacy-en-data-uitwisseling/>

¹⁴ <https://privacy-web.nl/publicaties/ddma-privacy-monitor-2021-nederlanders-positiever-over-data/>

¹⁵ <https://theprivacycollective.eu/nl/>

¹⁶ <https://fd.nl/ondernemen/1353803/nederlandse-massaclaim-tegen-amerikaanse-techreuzen-vanwege-privacyschending>

1.1.2.7 Schluss

Schluss bouwt aan een community en werkt toe naar een coöperatie. Op eigen verzoek is Schluss derhalve opgenomen bij de belangenbehartigers. Bij Schluss staat soevereiniteit centraal. Daarmee bepaal je je eigen privacy. Schluss levert tevens een service voor opslag van, regie op en overzicht over persoonlijke gegevens. Dit kan gaan om bijvoorbeeld adresgegevens, medische of financiële gegevens. Identificatie en autorisatie wordt gewaarborgd via derden. De gebruiker bepaald wie toegang krijgt, voor welk doel en voor welke periode. Schluss biedt een overzicht van welke inzagen verleend zijn, zodat deze ook weer ingetrokken kunnen worden (afhankelijk van de juridische kaders). Schluss heeft een roadmap met mijlpalen:



- In 2023 staan de persoonsgegevens nog steeds gedistribueerd bij de verschillende organisaties. Maar de desbetreffende persoon bepaalt met wie de gegevens gedeeld mogen worden.
- In 2025 staan de persoonsgegevens in de kluis van de eigenaar. De persoon bepaalt wie deze gegevens mag gebruiken.

Regie na overlijden¹⁷

Per jaar overlijden er ongeveer 160.000 personen in Nederland. De Rijksdienst voor Identiteitsgegevens (regie), Koninklijke Notariële Beroepsorganisatie, Stichting Ontwikkeling Schluss, De Volksbank en Coöperatie DELA werken aan een proof-of-concept van de digitale kluis. Daarmee krijgt de burger een centrale positie binnen het data-ecosysteem rond de use case 'Overlijden en afwikkeling van nalatenschappen'. Een burger kan op een veilige manier een vertegenwoordiger aanwijzen die na het overlijden administratieve zaken kan regelen

POC hypotheekaanvragen

Volksbank, Topicus en Schluss werken aan een POC voor hypotheekaanvragen¹⁸. Hierbij worden data uit bronsystemen opgehaald.

1.1.3 Communities en programma's

De ontwikkeling van technologie, standaarden en juridische kaders worden veelal gedreven door communities en programma's in het speelveld van regie op persoonlijke gegevens. Deze groepen zijn een drijvende kracht achter veel initiatieven, maar zijn zelf niet als bijvoorbeeld 'PDM-Dienst' of technologie te beschrijven. Denk hierbij aan een community als MyData Global of het overheidsprogramma ROG (dat eerder is besproken). Dit soort netwerken en programma's worden door betrokkenen van groot belang geacht om regie op persoonlijke gegevens te realiseren.

1.1.3.1 Holland Health Data Coöperatie

Holland Health Data Coöperatie¹⁹ is een van de projecten binnen de Roadmap Next Economy, een initiatief van gemeentelijke en provinciale overheden in Zuid-Holland. De leden bepalen wat met hun data gebeurt. Een van de leidende principes is dat data veilig bewaard worden, en alleen versleuteld en na toestemming daarvoor, vrijgegeven worden voor gebruik door derden.



1.1.3.2 Tada

Tada²⁰ is een beweging/campagne voor een 'verantwoorde digitale stad', dit is een stad die zich houdt aan zes waarden als het aankomt op data en technologie:

- Inclusief
- Zeggenschap



¹⁷ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/innovatie/innovatiebudget/toekenning-innovatiebudget-2021/>

¹⁸ <https://schluss.org/nl/de-volksbank-versnelt-hypotheekproces-met-schluss/>

¹⁹ <http://hhdc.nl/>

²⁰ <https://tada.city/>

- Menselijke maat
- Legitiem en gecontroleerd
- Open en transparant
- Van iedereen – voor iedereen

In oktober 2017 is het manifest “Tada – duidelijk over data ” door 50 samenwerkende partners gelanceerd. In 2020 staat de realisatie van de uitgangspunten op de agenda. In het genoemde manifest wordt aangegeven dat het gaat om ‘data die overheden, bedrijven en andere organisaties uit de stad genereren en verzamelen’. Bewoners moeten hier zeggenschap over kunnen hebben volgens Tada. Tada heeft nadrukkelijk oog voor de ethische aspecten van nieuwe technologieën²¹. In de regio Amsterdam werkt een groep koplopers aan de ontwikkeling van de Amsterdam Data Exchange (AMdEX). AMdEX²² benadrukt de waarde van controle uit het Tada manifest. AMdEX moet weer controle geven over data die wordt gedeeld.

1.1.3.3 Common ground

Common Ground²³ is een programma voor hervorming van de gemeentelijke informatievoorziening. Het uitgangspunt is het meervoudig gebruiken van gegevens uit de bron. Op dit moment worden gegevens door gemeenten namelijk vaak gekopieerd, wat foutgevoelig is, sneller zorgt voor verouderde gegevens en het onoverzichtelijk maakt waar gegevens van een persoon staan.

Common Ground streeft naar: uniforme gegevens, ophalen van gegevens via API's, één gemeenschappelijke integratielaag (NLX) en data bij de bron.

Common Ground streeft naar de situatie dat de gegevens in alle relevante informatiesystemen worden gescheiden van de applicaties en processen waarin ze worden gebruikt. De gegevens wordt vervolgens vanuit één bron voor de verschillende ICT-oplossingen beschikbaar te komen. De gedachtegang is dat als gemeenten ROG krijgen, de burgers hierop mee kunnen liften.

Common Ground wil aantonen dat het ook in de praktijk werkt, en vaststellen wat nodig is om deze oplossingen in het hele land te kunnen gebruiken.



De oplossingen Registratie Vakantieverhuur en het Huishoudboekje moeten in 2021 werken en voor alle gemeenten beschikbaar zijn om in de uitvoeringspraktijk te gebruiken. Huishoudboekje²⁴ is een Open Source product waarmee burgers meer grip krijgen op hun financiële situatie. Het Huishoudboekje is voor financieel kwetsbare burgers waar vaak schuldenproblematiek speelt. De initiële ontwikkeling van het Huishoudboekje is gedaan door de gemeente Utrecht. VNG Realisatie heeft, in samenwerking met de gemeente Utrecht de regie op zich genomen om het Huishoudboekje geschikt te maken voor generiek gebruik en dat op te schalen naar andere gemeenten in Nederland. De kopgroep voor deze opgave bestaat uit de gemeente Utrecht en Rotterdam en zal de komende periode groeien tot maximaal 5 gemeenten. Met deze kopgroep wordt op basis van de Common Ground principes, een landelijke Open Source service ontwikkeld.

Na implementatie van het Huishoudboekje bij de gemeente Rotterdam eind 2020 is vastgesteld dat de applicatie niet genoeg schaalbaar is. In samenwerking met gemeente Nijmegen wordt ontwikkeld aan een nieuwe versie, welke in hoge mate voldoet aan acceptatiecriteria van alle gemeenten²⁵.

5-lagen model (zie figuur-1)

Common Ground software bestaat uit componenten in een architectuur op basis van het 5-lagen model²⁶. De onderste drie lagen van het model omvatten de standaardisatie van semantiek en syntax van de ontsluiting van de gegevensbronnen, de daarbij behorende gestandaardiseerde diensten (APIs) en de gemeenschappelijke integratiefunctionaliteit NLX. De bovenste twee lagen van het model

²¹ <https://tada.city/nieuws/opinie-de-blinde-vlekken-van-tada/>

²² <https://www.towardsamdex.org/>

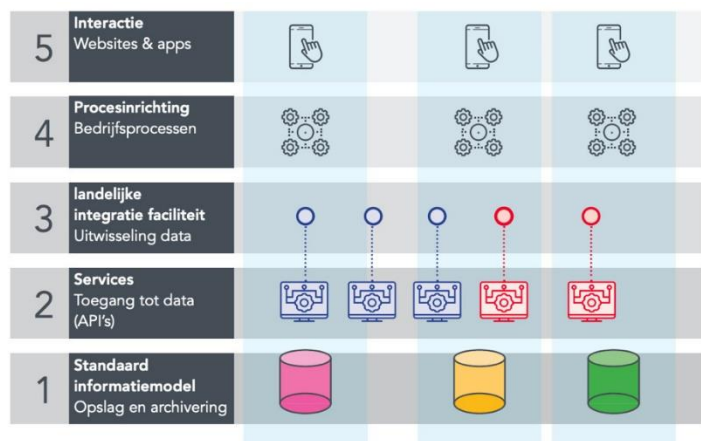
²³ <https://commonground.nl/> en <https://vng.nl/artikelen/common-ground>

²⁴ <https://publicaties.vngrealisatie.nl/2020/e-magazine/9/het-huishoudboekje-voor-alle-gemeenten/>

²⁵ <https://commonground.nl/groups/view/3b664abc-0842-4e3e-bce7-214e4c5f9b7c/team-huishoudboekje>

²⁶ <https://componentencatalogus.commonground.nl/5-lagen-model>

omvatten de inrichting en ondersteuning van processen en interactie met die processen voor burgers, bedrijven en medewerkers.



Figuur-1: Common Grond 5-lagen model

De 5-lagen:

1. **Data-laag**
Opslag en archivering. De data-laag bevat componenten die gegevens opslaan of archiveren. Voorbeelden van data-componenten zijn databasesystemen zoals Postgres en CouchDB, maar ook bestandsopslagsystemen zoals buckets of flat file storage.
2. **Servicelaag**
Toegang tot data (API's).
In de servicelaag bevinden zich componenten die API's aanbieden waarmee gegevens uit de data-laag ontsloten worden. API's worden bij voorkeur gestandaardiseerd in de vorm van OpenAPI 3 specificaties, zodat afnemende componenten garanties hebben over de inhoud van API-calls.
3. **Integratielaag**
Landelijke faciliteit voor uitwisseling van data.
NLX zorgt voor gemakkelijke, veilige verbindingen tussen organisaties. Ook regelt NLX generieke authenticatie en autorisatie, en logging.
4. **Proces-laag**
Bedrijfsprocessen. Binnen de proceslaag vallen de dienstverlenings- en bedrijfsprocessen.
5. **Interactie-laag**
Websites en apps. De interactielaag bestaat uit gebruikersinterfaces voor de eindgebruiker.

Onderstaande tabel laat de beweging in de verschillende lagen zien.

Laag binnen Common Ground	Beweging
Data-laag	In toenemende mate worden in het gegevenslandschap bij de overheid bronnen qua syntax en samenhang gestandaardiseerd door de bronhouder.
Servicelaag	- Groei in gebruik van API's waarmee gegevens uit de data-laag ontsloten worden. Tevens additionele toegevoegde waarde door filtering van gegevens (dataminimalisatie), en (technische) validatie van gegevens. - API's worden bij voorkeur gestandaardiseerd, onder meer in de vorm van OpenAPI 3 specificaties²⁷, zodat afnemende componenten garanties hebben over de inhoud van API-calls. - Steeds meer bronsystemen die relevant zijn voor regie op financiële gegevens worden via API's ontsloten. - De beweging is van screen scraping naar downloaden, naar API's.

²⁷ <https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification>

Laag binnen Common Ground	Beweging
Integratielaag	• Onder meer in overheids- en zorgdomein opkomst van grootschalige faciliteiten voor uitwisseling data, inclusief voorzieningen voor authenticatie, autorisatie, logging. Dit verlaagt beheerlasten en garandeert voldoen aan eisen vanuit compliance. • Inmiddels ontstaan de eerste standaarden nu binnen sectoren, bijvoorbeeld binnen de zorg sector is dat NUTS, die focust op informatie-uitwisseling tussen gebruiker en zorgverleners. Binnen het overheidsdomein is dat NLX, dat focust op de datauitwisseling tussen verschillende gemeentes.
Proceslaag	• Vooral processen voor het ophalen van gegevens worden ondersteund. • Indien relevant vinden ook functionele validaties plaats. • In deze laag moet ook toestemming van de persoon die gegevens deelt geregeld worden.
Interactielaag	• Steeds meer Apps beschikbaar, waarbij de gebruikerservaring centraal staat. • De Blauwe Knop is bijvoorbeeld een herkenbare knop beschikbaar in 'mijn-omgevingen' van uitvoeringsorganisaties DUO, CAK en UWV en op websites van een aantal gemeenten. De Blauwe Knop maakt het mogelijk voor burgers om hun persoonlijke data te downloaden van overheidswebsites en deze op termijn ook te gebruiken. idealiter levert de Blauwe Knop ook machine leesbare output. • Tevens wordt gewerkt aan een toepassing - de Rode Knop - waarmee inwoners via MijnApp aan een derde partij kunnen aangeven dat ze een ondersteunings- of schuldhulpverleningstraject van de gemeente ontvangen.

1.1.3.4 Blauwe Knop Programma

De Blauwe Knop²⁸ is een project dat is ontstaan vanuit het Kloosterhoeveberaad, met als doel mensen meer regie te geven op hun eigen gegevens. Het gaat hierbij om gegevens waar uitvoerders en gemeentes over beschikken (zoals diplomagegevens, kentekengegevens of NAW-gegevens). Het project De Blauwe Knop valt onder het programma Verbinden Schuldendomein van de VNG. Dit programma ondersteunt de invoering van vier nieuwe wetstrajecten waarmee SZW de schuldenproblematiek beter en sneller wil oplossen en voorkomen²⁹.

VNG Realisatie trekt dit initiatief samen met andere uitvoerders. Het Nederlandse programma is geïnspireerd door het 'Blue Button Initiative' voor het downloaden van zorggegevens in de VS³⁰. Daar is de 'Blue Button' ingezet voor burgers om te zorgen dat zij zorggegevens (zoals medische historie, overzichten van vaccinaties) overzichtelijk in kunnen zien en delen met zorgverleners of bij het wisselen van zorgverzekering.

RDW voert het project samen met VNG Realisatie uit. In het groeipad is voorzien dat de Blauwe Knop drie verschillende verschijningsvormen heeft³¹:

1. Blauwe Knop Basis: een downloadvoorziening om een gewaarmerkte set persoonlijke gegevens bij één organisatie te downloaden in pdf- of machineleesbaar-formaat, naar de telefoon, laptop, computer of tablet van de persoon.
2. Blauwe Knop Basis 2.0: een downloadvoorziening om één geaggregeerde, gewaarmerkte set persoonlijke gegevens vanuit meerdere organisaties te downloaden in pdf- en machineleesbaar-formaat naar de telefoon, laptop, computer of tablet van de persoon.
3. Blauwe Knop Plus: een voorziening om via een API (een interface tussen verschillende computersystemen) een gewaarmerkte set persoonlijke gegevens (mogelijk samengesteld vanuit

²⁸ <https://www.vngrealisatie.nl/producten/blauweknop>

²⁹ <https://vng.nl/rubrieken/onderwerpen/armoede-en-schulden>

³⁰ <https://www.healthit.gov/topic/health-it-initiatives/blue-button>

³¹ <https://rog.pleio.nl/news/view/57900558/blauwe-knop-programma-exploreert-onderzoekt-en-realiseert>

verschillende bronnen) van de bron beschikbaar te stellen aan andere partijen. In deze vorm, kan iemand bijvoorbeeld de Belastingdienst toestemming geven, inkomensgegevens te delen met zijn of haar wooncorporatie. Op die manier kan worden 'bewezen' dat hij of zij voldoet aan de criteria voor een specifieke huurwoning.

In de schuldhelpverlening zou één overzicht van alle schulden van een inwoner een hele stap vooruit zijn. Op dit moment is de gemiddelde doorlooptijd van de intake (landelijk) ongeveer 3 maanden, dat kan aanzienlijk sneller door gebruik te maken van de Blauwe Knop, aldus de RDW.

Vanaf begin 2021 tot juli 2021 is sprake van stilte rond de Blauwe Knop.

1.1.3.5 Programma Toekomst Gegevensuitwisseling Werk en Inkomen (TWI)

Opdrachtgever van Toekomst Gegevensuitwisseling werk en inkomen (TWI), een programma dat loopt vanaf 2017, is het ministerie van Sociale Zaken en Werkgelegenheid (SZW). De uitvoering is in handen van het Programma TWI, een gezamenlijk programma van het ministerie van SZW, UWV, SVB, VNG, Inlichtingenbureau en het Bureau Keteninformatisering Werk en Inkomen. Het programma TWI heeft als doel een stelsel te ontwikkelen waarbinnen burgers zelfstandig – met behulp van gegevens over henzelf en over hun persoonlijke levenssituatie – verantwoordelijkheid kunnen nemen voor (belangrijke) keuzes waar zij voor staan³². Men wil komen tot een Persoonlijke Inkomens Omgeving (PIO) voor iedereen. Vanuit dit dashboard kan iedere burger de zaken regelen die nodig zijn voor de dienstverlening van zowel overheden als private partijen die toegang hebben tot het TWI-stelsel.

1.1.3.6 Overheidsprogramma Machtigen

Het overheidsprogramma 'Machtigen'³³ moet het recht om iemand te machtigen verbeteren. Het programma streeft ernaar om machtigen gebruiksvriendelijker te maken, wettelijke vertegenwoordigers rechtstreeks zaken te laten doen met de overheid en nieuwe vormen van machtigen, zoals nabestaandenmachtiging, mogelijk te maken. Het programma bouwt voort op DigiD Machtigen³⁴. Machtigen kan ook van belang zijn in financiële processen, bijvoorbeeld wanneer iemand niet (meer) in staat is de eigen financiële situatie te regelen.

In een brief van 19 maart 2021 laat Knops de Tweede Kamer dat de voorbereidingen zijn afgerond voor de grootschalige aansluiting van de zorg op vrijwillig machtigen. Eind 2022 zouden 12.000 dienstverleners uit de zorg aangesloten moeten zijn.

1.1.3.7 i4Sociaal

i4Sociaal is een samenwerkingsprogramma van een aantal gemeenten³⁵. Binnen het i4Sociaal programma willen gemeenten Enschede, Deventer, Groningen, Zwolle, Leeuwarden en Zaanstad, samen met Dimpact, de 'systeem-en leefwereld' dichter bij elkaar brengen. Regie op eigen gegevens is daarbij belangrijk. Binnen het programma is het pilot platform MaximaalJezelf ontwikkeld. Inwoners kunnen op dit platform een profiel aanmaken. In dit profiel kan de inwoner gegevens toevoegen. Tevens is het mogelijk gegevens op te halen. De toegang loopt via DigiD.

Op basis van de gegevens (zoals bijvoorbeeld informatie over ondersteuning die een inwoner al ontvangt vanuit de UWV) kan de gemeente passende oplossingen bieden en informatie tonen. De gegevens van de inwoner moeten helpen om te bepalen of hij/zij recht heeft op een voorziening en het makkelijker en sneller maken voor hulpverleners om de situatie van de inwoner te begrijpen. Van de pilot wordt in de komende jaren een duurzaam platform gemaakt.



³² Deel! Januari 2021, Magazine van de overheid over Regie Op Gegevens

³³ <https://www.rijksicdashbord.nl/projecten/573449>

³⁴ <https://www.digitaleoverheid.nl/dossiers/digid-machtigen/>

³⁵ <https://www.dimpact.nl/i4sociaal>

1.1.3.8 EDUmij

Het idee 'EDUmij' is ontstaan vanuit de Informatiekamer, waar onderwerpen in de informatieketen binnen het onderwijs besproken worden. De Informatiekamer is een door OCW voorgezeten overleg van onderwijspartijen die acteren in de verschillende onderwijssectoren: OCW, DUO, de Onderwijsinspectie, PO-raad, VO-raad, MBO-raad, VH, VSNU, saMBO-ICT, Kennisnet en SURF. EDUmij levert een mechanisme of voorziening die het mogelijk maakt voor een lerende en zich ontwikkelende persoon om levenslang regie te voeren over eigen leer- en ontwikkelgegevens. Zoals bijvoorbeeld het verzamelen van zowel studiegegevens, als later behaalde certificaten en werkervaring in een overzichtelijk CV. Een voorbeeld is Europass³⁶, een toepassing van PDM rond talenten en diploma's. Op dit moment onderzoekt EDUmij nog in welke richting het zich moet gaan ontwikkelen: afsprakenstelsel, operator of faciliterend programma.



1.1.3.9 Leven Lang ontwikkelen

'Lifelong learning'³⁷ is een belangrijk thema voor de Europese Commissie. Het stimuleren van een leven lang ontwikkelen heeft de achterliggende gedachte dat personen inzetbaar blijven op de arbeidsmarkt, voldoening krijgen en participeren aan de maatschappij. Binnen de Nederlandse overheid is leven lang leren ook een thema op de politieke agenda en stimuleert dit met maatregelen als levenlanglerenkrediet³⁸. Leven lang ontwikkelen heeft een belangrijke relatie met persoonlijke gegevens. Er is op dit moment, naast het diplomaregister, beperkte mogelijkheid om resultaten die een persoon gedurende een leven verzameld in een overzicht inzichtelijk te maken. Personen kunnen hiervoor LinkedIn gebruiken, echter zijn de Cv's die daar opgebouwd worden volledig zelf verklarend en hebben daarmee een zeer lage betrouwbaarheid. De Europese commissie heeft de ambitie om deze situatie te verbeteren: 'taking appropriate steps to ensure that every European learner has access to their personal education data, so as to facilitate their opportunities for creating personal learning paths and profiles throughout their lives'³⁹. Eén van de uitkomsten hiervan is Europass, zie hiervoor onder EDUmij. Binnen Nederland is de SER gevraagd door OCW en SZW om een aanjagers rol te pakken op dit thema. Onder andere door te werken aan het in kaart brengen van vaardigheden van personen.⁴⁰



1.1.3.10 Dutch Blockchain Coalition

De Dutch Blockchain Coalition (DBC) is een initiatief vanuit overheid, educatief en private partijen die samenwerken aan verschillende blockchain ontwikkelingen. Ze houden zich onder andere bezig met use-cases rondom SSI, diploma registratie en pensioen waarbij blockchain een bijdrage levert. Veel van deze use-cases snijden aan het PDM, omdat er veelal ook persoonlijke data gedeeld wordt. Distributed ledgers and blockchains hebben een vertrouwensfunctie omdat hun infrastructuur geheel open is en elke gebruiker alle gegevens kan controleren en volgen. DBC is in 2017 ontstaan in Nederland en ze zetten zich in voor een ecosysteem waarin vrijheid, gelijkheid en veiligheid vooropstaan.



³⁶ <https://www.europass.nl/>

³⁷ <https://www.rijksoverheid.nl/onderwerpen/leven-lang-leren>

³⁸ <https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/wat-is-het-levenlanglerenkrediet>

³⁹ "Council conclusions on fostering lifelong learning by developing strategic approaches on continuous learning" prepared by the Presidency with a view to the Education Committee's meeting on 15 July 2019.

⁴⁰ https://www.ser.nl/-/media/ser/downloads/thema/scholing-ontwikkeling/voortgangsrapp_levenlangontwikkelen.pdf

1.1.3.11 Data Sharing Coalition

De Data Sharing Coalition⁴¹ is een open internationaal initiatief waarin een grote verscheidenheid aan organisaties samenwerkt om de waarde van cross-sectoraal datadelen te ontgrendelen. Het initiatief is in januari 2020 gestart nadat het ministerie van Economische Zaken en Klimaat de markt uitnodigde om de samenwerking op te zoeken voor het cross-sectoraal delen van data. Het doel van de Data Sharing Coalition is het stimuleren van cross-sectoraal delen van data onder controle van de rechthebbende(n) door het realiseren van interoperabiliteit tussen datadeelinitiatieven en het versterken van individuele initiatieven.



Gestreefd wordt naar generieke afspraken op het gebied van bijvoorbeeld:

- technische standaarden;
- semantiek van data;
- juridische afspraken;
- betrouwbare, herbruikbare digitale identiteiten.

Deze generieke afspraken legt de Data Sharing Coalition vast in het 'harmonisatiecanvas'. In 2018 maakte Innopay al een rapport dat hierop aanstuurde⁴². Een van de adviezen was om een oplossing te realiseren die interoperabiliteit tussen bestaande en nieuwe afsprakenstelsels en platforms garandeert. Innopay sprak de volgende ambitie uit. Binnen 5 jaar:

- Is een generiek afsprakenstelsel voor datadeelinitiatieven op basis van cross-sectorale principes ontwikkeld waaruit vele nieuwe cross-sectorale use cases zijn ontstaan;
- Zijn er tenminste tien afsprakenstelsels die sectoraal en cross-sectoraal datadelen tussen bedrijven mogelijk maken, mede dankzij het generieke afsprakenstelsel voor datadeelinitiatieven;
- Zijn nieuwe, cross-sectorale use cases van datadelen een belangrijke pijler onder het realiseren van maatschappelijke en economische doelstellingen.

1.1.3.12 MyData Global

MyData Global⁴³ is een non-profit organisatie met leden over de hele wereld die de zes principes van de MyData declaration⁴⁴ onderschrijven. Deze principes gaan verder dan wat voorgeschreven wordt door de GDPR:

- “Human-centric control of personal data
- Individual as the point of integration
- Individual empowerment
- Portability: access and re-use
- Transparency and accountability
- Interoperability”



In de genoemde MyData declaration worden deze principes verder toegelicht.

MyData is voornamelijk een netwerk. Het doel van MyData is om personen de regie over gegevens (terug) te geven. Binnen de MyData community zijn specialisten en onderzoekers van zowel publieke als private partijen te vinden die zich bezighouden met regie op persoonsgegevens.

MyData publiceert een overzicht van MyData Operators⁴⁵. Organisaties die de MyData Operator status aanvragen, moeten aantonen hoe ze mensgerichte gegevenscontrole creëren en hoe de gegevens en waarde in hun ecosystemen stromen.

⁴¹ <https://datasharingcoalition.eu/>

⁴² <https://docplayer.nl/150980153-Generiek-afsprakenstelsel-voor-datadeelinitiatieven-als-basis-van-de-digitale-economie.html>

⁴³ www.mydata.org

⁴⁴ <https://mydata.org/declaration/>

⁴⁵ <https://mydata.org/mydata-operators/>

1.1.3.13 Alliance for the Freedom of Car Repair (AFCAR)

ANWB, BOVAG, FOCWA, RAI After-market, VACO, Verbond van Verzekeraars en VNA zijn aangesloten bij AFCAR, een Europese alliantie die pleit voor nieuwe (Europese) wetgeving en handhaving van bestaande regelgeving om de keuzevrijheid van de consument met betrekking tot voertuigdata te borgen. Consumenten moeten de regie hebben over de door hen gegenereerde voertuigdata. Dit wordt ook bepleit in recent onderzoek van Ecorys in opdracht van het ministerie van Infrastructuur en Waterstaat en het ministerie van Economische Zaken en Klimaat⁴⁶. Het rapport geeft een scala aan beleidsopties en interventies.



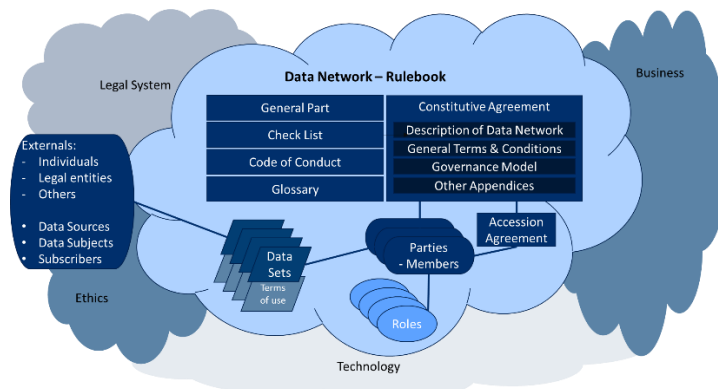
Delen voertuigdata⁴⁷

Hiervoor genoemde organisaties bepleiten in een brief van medio juni 2021 aan formateur Hamer dat de consument de regie moet krijgen over de eigen voertuigdata. De organisaties zijn voorstander van het wettelijk verankeren van een Secure On-Board Telematics Platform (S-OTP): een neutraal en veilig platform voor het ongecensureerd delen van voertuigdata. S-OTP maakt eerlijke concurrentie en onafhankelijk ondernemerschap in de automotive sector mogelijk, aldus de organisaties.

1.1.3.14 Sitra/IHAN

IHAN⁴⁸ is een programma vanuit het Finse innovatie-fonds Sitra. De intentie van IHAN is om een governance framework, architectuur definities en requirements op te stellen voor de componenten van een door data gedreven wereld. Een belangrijke stap hierin is de IHAN blauwdruk⁴⁹ die omschrijft wat de componenten van het IHAN ecosysteem doen, waaronder een 'IHAN identifier' voor personen. De genoemde blauwdruk beschrijft gedetailleerde functionele vereisten voor de verschillende rollen in het IHAN ecosysteem.

In juni 2020 publiceerde Sitra – dat expliciet naar een eerlijke data-economie streeft – een Rulebook-sjabloon met als doel om een gemakkelijk toegankelijke handleiding te bieden over het opzetten van een datanetwerk en om algemene voorwaarden vast te leggen voor overeenkomsten voor het delen van gegevens. Het delen van gegevens heeft volgens Sitra veel voordelen. Het kan gegevensgebruikers toegang geven tot gegevens voor



onderzoeksdoeleinden of voor de ontwikkeling van hun producten en diensten. Door gegevens te delen, kunnen gegevensbronnen ook hun producten of diensten verbeteren en de ontwikkeling van toegevoegde waarde of diensten door derden ondersteunen. Het bestaan van rijke ecosystemen die nieuwe producten en diensten creëren, kan erg aantrekkelijk worden voor gebruikers. Een toename van het aantal gebruikers van services moedigt op zijn beurt nieuwe product- en serviceontwikkelaars en gebruikers aan om zich bij het data-ecosysteem aan te sluiten. Dit netwerkeffect kan de waarde van een specifieke dienst en zelfs het hele ecosysteem verhogen. Bovendien kan het delen van gegevens de transactiekosten van het verzamelen van gegevens verlagen met minimale organisatorische veranderingen.

⁴⁶ Onderzoek naar het delen van voertuigdata en interfaces, Ecorys, Rotterdam, 27 januari 2020

⁴⁷ <https://www.verzekeraars.nl/publicaties/actueel/pleidooi-voor-neutraal-platform-delen-voertuigdata>

⁴⁸ <https://www.sitra.fi/en/projects/ihan-proof-concept-pilots/#what-is-it-about>

⁴⁹ <https://media.sitra.fi/2018/11/14144842/261018-ihan-blueprint-2.0.pdf>

1.1.3.15 Personal Data Ecosystem Consortium

Personal Data Ecosystem Consortium (PDEC)⁵⁰ is een handelsvereniging zonder winstoogmerk met leden over de hele wereld. De ambitie is het ecosysteem voor persoonlijke gegevens te activeren en te verbreden. Een ecosysteem waarin mensen en hun data centraal staan, dat organisaties in staat stelt om persoonsgerichte datalogistiek te realiseren. De ledenlijst is indrukwekkend⁵¹.



1.1.3.16 International Data Spaces Association (IDSA)

IDSA bestaat uit een praktijkgemeenschap en een netwerk van knooppunten en samenwerkingsverbanden ter ondersteuning van het delen van kennis en het opbouwen van vereiste vaardigheden in de data-economie in heel Europa en daarbuiten. IDSA levert ook inbreng voor de Data Act.

**INTERNATIONAL DATA
SPACES ASSOCIATION**



De Europese Commissie benoemt in haar datastrategie negen Data Spaces. Dit is verder uitgewerkt door IDSA⁵². Het beschrijft de beschikbaarheid van grote gegevenspools, een infrastructuur om gegevens te gebruiken en uit te wisselen, evenals geschikte beheersmechanismen als sleutel. Het is gebaseerd op een peer-to-peer-benadering van gegevensuitwisseling en vereist geen centrale gegevensopslag.

1.1.4 Overheid

1.1.4.1 Kabinet Rutte-III

Eén van de speerpunten van het kabinet Rutte-III is om mensen meer regie op hun gegevens te geven. Door inzage in die gegevens, door inzage in het gebruik daarvan, door de mogelijkheid van correctie, en door deze te kunnen delen met derden. In juli 2019 heeft het kabinet de Tweede Kamer over de aanpak rondom ROG geïnformeerd door middel van de beleidsbrief⁵³ "Regie Op Gegevens". Waarin de beleidsvoornemens en aanpak geschetst worden.⁵⁴

Nieuw spoor: delen gegevens

Het kabinet wil deze bestaande regiemogelijkheden uitbreiden met een belangrijk nieuw spoor, door burgers in staat te stellen hun eigen gegevens zelf, digitaal te delen met private dienstverleners, zoals zorgverleners, onderwijsinstellingen, schuldhulpverleners of woningcorporaties. Volgens het kabinet kunnen deze hierdoor hun klanten betere diensten leveren, en wordt de administratieve rompslomp beperkt.



Kader

Het kabinet denkt daarbij aan een kader met de volgende ijkpunten:

1. de burger is zelf verantwoordelijk voor de beslissing om gegevens te delen met private dienstverleners en geeft daarvoor expliciete toestemming;
2. voor de burger is helder welke gegevens hij deelt, voor welk doel deze worden gebruikt, en wat de (mogelijke) consequenties van verstrekking zijn;
3. duidelijk is wanneer de toestemming voor het gebruik van de gegevens eindigt en de dienstverlener de verstrekte gegevens weer verwijdt;
4. het delen van gegevens is op basis van vrijwilligheid en de bereidheid om gegevens digitaal (in plaats van op papier) te delen speelt geen rol voor het wel of niet verkrijgen van een dienst;
5. een burger die dat wil heeft op of via één centrale plek (bijvoorbeeld MijnOverheid) overzicht via welke intermediairs hij met welke dienstverleners gegevens deelt c.q. heeft gedeeld, en waar hij moet zijn om zijn toestemming voor het delen van gegevens kan intrekken;

⁵⁰ <http://pde.cc/>

⁵¹ <http://pde.cc/directory/>

⁵² <https://www.internationaldataspaces.org/>

⁵³ <https://www.rijksoverheid.nl/documenten/brieven/2019/07/11/beleidsbrief-regie-op-gegevens-nadere-uitwerking>

⁵⁴ <https://www.digitaleoverheid.nl/dossiers/rog-regie-op-gegevens/>

6. dienstverleners en intermediairs voldoen aan de AVG, en vragen dus niet meer gegevens dan nodig voor het verlenen van die dienst en bewaren deze niet langer dan nodig;
7. dienstverleners en intermediairs voldoen aan de Wet digitale overheid, en werken dus binnen de wettelijke mogelijkheden en beperkingen ten aanzien van het gebruik van het BSN en van authenticatiemiddelen zoals DigiD;
8. dienstverleners en intermediairs maken als het om basisgegevens gaat waar mogelijk gebruik van gegevens uit de authentieke bron.

Behoefte aan ROG

In 2019 zijn er meerdere onderzoeken afgerond naar de manier waarop gebruikers regie op hun gegevens willen houden. Uit de onderzoeken komt naar voren dat de behoefte aan regie niet direct herkend wordt en dat de behoefte vooral latent aanwezig is. In bepaalde situaties en door slimme procesinrichting kan de behoefte aan ROG duidelijk worden en tot gebruik gaan leiden⁵⁵.

Kader ROG⁵⁶

Waarom een kader? Gezamenlijk afspraken maken zodat mensen regie over hun eigen persoonlijke gegevens kunnen hebben, en het invullen van randvoorwaarden zorgt voor vertrouwen waardoor dienstverlening, samenwerking en handel zich ongehinderd kunnen ontwikkelen, terwijl privacybelangen en digitale rechten beschermd worden. Deze afspraken en randvoorwaarden vormen met elkaar een **‘vertrouwensinfrastructuur’** en zijn het doel voor het kader voor ROG. Het kader voor ROG is géén afsprakenstelsel, maar is een kader dat een basis legt waaraan RoG-afsprakenstelsels en RoG-implementaties zich houden.

Principes voor ROG

De hoofdprincipes:

- Mens Centraal: door mensen de mogelijkheid te bieden om regie op hun eigen persoonlijke gegevens te hebben, krijgen zij meer grip op hun persoonlijk leven.
- Digitale autonomie: door vergroting van inzicht in – en invloed op – persoonlijk gegevensverkeer, verstevigen personen hun positie ten opzichte van aanbieders en afnemers. Deze ontwikkelingen op het gebied van digitale zelfbeschikking van mensen vragen erom in goede banen te worden geleid.
- Inclusiviteit: ROG kan en moet eraan bijdragen dat zoveel mogelijk mensen vrijelijk deelnemen aan het (digitale) maatschappelijke leven, met al hun persoonlijke verschillen in mogelijkheden, omstandigheden en culturen.

De inrichtingsprincipes

- Vertrouwen: afsprakenstelsels voor, en implementaties van ROG vergroten het vertrouwen van personen, aanbieders en afnemers, in ROG.
- Transparantie: personen, aanbieders en aanvragers zijn open en eerlijk over hun intenties en gedrag in ROG.
- Interoperabiliteit: afsprakenstelsels voor, en implementaties van ROG borgen de koppelbaarheid tussen de diensten en gegevens van betrokken personen, aanbieders en afnemers.
- Dataminimalisatie: afsprakenstelsels voor – en implementaties van – ROG, zorgen voor uitwisselingen van persoonlijke gegevens, die passend zijn bij de behoefte van de persoon, en de vraag van de afnemer.

Kaders

- Juridische kaders, waarbij in deze versie een analyse is gemaakt van de AVG op het concept van ROG;
- Functionele kaders, met als belangrijkste bouwblokken de rollen, functionaliteiten, interactiemodel en compliance maatregelen;
- Technische kaders, met als bouwblokken bericht- en datastandaarden, identity en access management (identificatie, authenticatie en autorisatie), integratie/connectiviteit, metadata en beveiliging;

⁵⁵ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nldigibeter/toegankelijk-begrijpelijk-en-voor-iedereen/>

⁵⁶ Kader voor Regie Op Gegevens, voorstudie, maart 2019

- Organisatorisch en operationeel kader.

Roadmap

- Kenmerkend aan horizon 1 is dat organisaties op hun eigen manier enkele persoonlijke gegevens uit hun administraties digitaal ter beschikking stellen op een digitale manier. Een persoon ontvangt een kopie van zo'n set van zijn/haar gegevens, waarna de persoon zelf desgewenst een handeling kan verrichten (opvragen bij partij A en doorsturen naar partij B). Denk hierbij aan gecertificeerde Pdf's, een download knop (Blue Button) of digitale kluisjes.
- Op horizon 2 maken gegevenshouders gegevens uit de bron, digitaal toegankelijk voor personen en andere organisaties. Ze werken mee aan de uitwisseling van gegevens onder de regie van de betreffende persoon. Hierbij kan een persoon aangeven dat partij A een specifiek gegeven of een set van gegevens kan inzien voor een bepaald doel en een bepaalde periode. Hiervoor is een set van afspraken nodig hoe en onder welke voorwaarden partijen gegevens aan personen ter beschikking stellen.
- Tot slot is in horizon 3 de persoon volledig zelf in regie over zijn gegevens. Een persoon doet een bewering (ik ben 18 – of – ik heb een kind gekregen) en een bevoegde instantie kan deze bewering attesteren. Gegevens zijn hierdoor digitaal in beheer bij de persoon zelf met een attest/verificatie door een bevoegde instantie. Voorbeelden hiervan zijn terug te vinden in self-sovereign identity en attribute-based authentication.

Referentiearchitectuur

In de zomer van 2020 startte het programma Regie Op Gegevens met het opstellen van een Referentie Architectuur voor delen van overheidsgegevens met derden onder regie van de burger. De uitvoering ligt bij ICTU. De referentiearchitectuur geeft inzicht in het WAT (kaders voor processen en gegevens) en niet in het HOE. Het HOE (techniek) is een zaak voor de leveranciers van de PDM-oplossingen.

Tevens begon PBLQ met een verkenning naar de juiste verdeling van verantwoordelijkheden rond de rekenregels die bij dataminimalisatie in het delen van gegevens nodig zijn: wie stelt vast, beheert, actualiseert, past toe, en vertrouwt de logica die van persoonsgegevens beweringen maakt die voor een (private) dienst relevant zijn? Wat moet hierin meewegen?

NORA/Go principes zijn leidend: de programma's Regie Op Gegevens en het stelsel van basisregisters stemmen hun referentiearchitecturen op elkaar af, waarbij de NORA/GO principes leidend zijn.

Naar een afsprakenstelsel

Begin 2020 verscheen een paper waarin de elementen van een afsprakenstelsel worden beschreven⁵⁷. Onderstaande tabel geeft hiervan een beeld.

⁵⁷ Afsprakenstelsels, governance en invulling, uitgegeven door -Programma Regie Op Gegevens, 28 februari 2020

Overzicht en structuur van het ecosysteem	Technische specificaties
Doel van het ecosysteem	Standaarden
Reikwijdte van het ecosysteem	Interfaces
Belanghebbenden en (potentiële) deelnemers	Interoperabiliteit
Services van het ecosysteem	Service Levels
Structuur en governance van het ecosysteem	Betrouwbaarheidsniveaus
Documentatie die het afsprakenstelsel definieert	Identificatie / authenticatie
Juridische grondslag en binding	Semantiek en data-mapping
Definities	Metadata transacties
Governance van het ecosysteem	Metadata gegevens
Besturende entiteit	Change & Release Procedure
Contactgegevens van de besturende entiteit	Security vereisten
Verantwoordelijkheden van de besturende entiteit	Risicovolle onderdelen en beheersing
Deelname aan de besturende entiteit(en)	Fraude en misbruik
Participatie in besluitvorming	Specifieke beveiligingseisen
Advies	Event logging
Rollen en verantwoordelijkheden deelnemende partijen	Archivering en opslag
Rollen in het ecosysteem	Audit trails
Verantwoordelijkheden per rol	Continuïteit van het ecosysteem en dienstverlening
De toetredingsprocedure voor een deelnemer	Incident & Response Planning
Overige betrokken partijen	Privacy vereisten
Diensten/services en gegevens in het ecosysteem	Juridische elementen
Diensten aan gebruikers en afnemers	Contracten
Interne transacties binnen het ecosysteem	Intellectueel eigendom
Toepassingen en applicaties	Klachten en geschillen
	Aansprakelijkheid
	Geheimhouding en vertrouwelijkheid
	Wet- en Regelgeving
	Normenkaders

Maatschappelijke kosten-batenanalyse (MKBA, maart 2020)⁵⁸

De vraag is 'wat het delen van gegevens zou opleveren en zou kosten, zowel maatschappelijk gezien als bedrijfseconomisch?' Deze maatschappelijke kosten-batenanalyse (MKBA) brengt, vanuit het perspectief van de maatschappij, in beeld wat de voor- en nadelen zijn van het concept ROG. Gezien de veel omvattendheid van ROG, wordt de MKBA toegespitst op enkele life events. Een life event is een belangrijke gebeurtenis in het leven van een persoon.

De life events waarop dit onderzoek zich richt zijn

- het overlijden van een naaste;
- het huren van een sociale huurwoning;
- het afsluiten van een hypothecaire lening ten behoeve van het kopen van een huis.

De belangrijkste baten van de life events zijn kwalitatief van aard en hebben betrekking op diverse partijen in de maatschappij.

De maatschappij profiteert in de vorm van:

- burgers hebben grip en zicht op zijn persoonlijke gegevens bij de overheid;
- verbeterde (en nieuwe vormen van) dienstverlening, door het makkelijk digitaal combineren van gevalideerde gegevens, uit verschillende bronnen;
- tijdsbesparing en minder stress/irritatie bij burgers;
- efficiencywinst bij marktpartijen en overheden;
- duidelijkheid over gegevens;
- risico op (woon)fraude neemt af;
- minder onrechtmatigheid;
- minder marktbelemmeringen.

De drie life events laten zien dat de te kwantificeren baten de kosten fors overstijgen:

- Overlijden naaste: de baten ter hoogte van ruim 65 miljoen euro over een periode van 15 jaar, wegen op tegen de kosten van bijna 5 miljoen euro over dezelfde periode (contante waarden,

⁵⁸ <https://www.digitaleoverheid.nl/nieuws/update-nl-digitaal-data-agenda-overheid-2020-naar-tweede-kamer/>

2020). Hierbij is ervan uitgegaan dat er geen Zero-Knowledge-Proof oplossing nodig is. De kosten nemen met circa 10 miljoen euro toe, indien dit wel noodzakelijk is.

- Sociale huurwoning: tegenover de benodigde investeringen van in totaal 15 miljoen euro over een periode van 15 jaar staan baten van ruim 64 miljoen euro (contante waarden, 2020). Een relatief groot deel van de baten komt door de besparing bij de burgers. De kosten overstijgen licht de baten voor woningcorporaties. Overigens kunnen de baten voor de corporaties nog wel verder toenemen, indien de accountants hun efficiencywinst doorberekenen in lagere tarieven.
- Afsluiten hypothecaire lening: de benodigde investeringen (inclusief beheer) bedragen in totaal bijna 8 miljoen euro. De baten zijn over de gehele periode van 15 jaar ruim 220 miljoen euro (contante waarden, 2020), ongeveer gelijk verdeeld tussen de burgers en de hypotheekverstrekkers. Hiermee worden de kosten ook voor dit life event ruim goedgemaakt.

De MKBA laat ook duidelijk zien dat de baten primair bij de burgers en private dienstverleners liggen, en dat de overheid een deel van de investeringen moet doen om ROG veilig en betrouwbaar mogelijk te maken.

Juridisch eigendom van gegevens

Voor wat betreft het juridische eigendom van gegevens gaf het kabinet medio juni 2020 duidelijkheid. De rechten en plichten rond de persoonsgegevens van een burger kunnen op een andere manier beschermd worden, is de conclusie van de toelichtende brief. Deze rechten en plichten zijn geregeld in de Algemene Verordening Gegevensbescherming (AVG)⁵⁹.

Juridisch kader (status augustus 2020)

Voorstellen om de spelregels van ROG te verankeren in regelgeving bevinden zich nog in een ontwerpfasen. Voor gegevens die herleidbaar zijn naar een persoon, is de basis voor ROG in een amendement Online Identiteit bij het wetsvoorstel Digitale Overheid opgenomen⁶⁰. Dit amendement regelt een unieke online identiteit voor elke burger en legt de één-bron-gedachte daarmee vast in de wet.

Voor elke burger met een Burgerservicenummer, die in de basisregistratie personen (BRP) is opgenomen, komt er een online identiteit: een digitale voorziening die de basis vormt voor de één-bron-gedachte. Met dezelfde waarborgen als dat nu gebeurt in de BRP worden persoonsgegevens in de digitale voorziening behandeld. Natuurlijke personen krijgen hiermee de mogelijkheid om hun eigen gegevens in te zien alsmede de verstrekkingen en het verplicht gebruik daarvan en waar mogelijk ook hun eigen gegevens zoals die door overheden en diensten gebruikt worden te corrigeren of te delen.

Met deze bevoegdheid wordt geregeld dat de gegevens van de burger in deze nieuwe digitale voorziening, onder een unieke online identiteit, gekoppeld worden aan de BRP, voor de overheid en haar bestuursorganen en eventuele andere organisaties voortaan als enige bron gelden. Van die gegevens moet gebruik worden gemaakt volgens één-bron-gedachte. De overheid baseert zich daarmee dan dus altijd op de gegevens vanuit de unieke online identiteit en niet meer op kopieën of door de bestuursorganen individueel verzamelde gegevens. Ook is er één duidelijk punt waar alle overheidsorganen de gegevens moeten ophalen wanneer zij handelingen verrichten ten aanzien van een burger.

De online identiteit wordt voor geselecteerde persoonsgegevens een unieke bron voor de overheid. Met de online identiteit en daaronder liggend de digitale voorziening weten mensen die hun gegevens daarin bekijken ook zeker dat precies die gegevens gebruikt worden. Ook kan met hiermee de burger meer regie over zijn persoonsgegevens worden gegeven. Als de stap naar een unieke online identiteit is gezet zijn er vele andere voordelen denkbaar voor de digitaliserende overheid en samenleving, bijvoorbeeld in de sfeer van de bestrijding van adresfraude, identiteitsfraude maar ook in de medische wereld of onderwijs.

⁵⁹ <https://www.digitaleoverheid.nl/nieuws/kamerbrief-geeft-duidelijkheid-burger-geen-eigenaar-van-persoonsgegevens/>

⁶⁰ https://www.eerstekamer.nl/wetsvoorstel/34972_wet_digitale_overheid

Vertrouwen⁶¹

Om het gewenste vertrouwen bij de burger te krijgen zullen er (naast dataminimalisatie) maatregelen getroffen moeten worden ten aanzien van:

- Transparantie in de persoonsgegevens die ingewonnen worden (welke en waarvoor);
- Transparantie in de algoritmen die gebruikt worden (welke en waarvoor);
- Transparantie en duidelijke normering over de Persoonlijke Digitale Omgevingen die gebruikt worden (welke andere gegevens worden over die burger verzameld en wat gebeurt daarmee);
- In voorkomende gevallen toetsing vooraf om als dienstverlener deel te mogen nemen aan een (sectoraal) samenwerkingsverband;
- Toezicht op de naleving (bijvoorbeeld bij het aangaan van leverovereenkomsten tussen overheid en dienstverlener of d.m.v. afsprakenstelsels).

1.1.4.2 Wetenschappelijke Raad voor het Regeringsbeleid (WRR)

Burgers willen graag zelfredzaam zijn, maar niet iedereen blijkt daar op elk moment toe in staat, aldus de WRR⁶². Dat komt mede door veranderingen in de omgeving waarin ze dagelijks functioneren. De burger heeft meer verantwoordelijkheid genomen en gekregen.

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Minder baanzekerheid, gezond moeten leven en teruglopende inkomsten vanwege de crisis vragen veel flexibiliteit. Veel wordt verwacht van burgers. Soms is sprake van een **redzaamheidsparadox**: de grote nadruk op eigen verantwoordelijkheid verkleint de zelfredzaamheid van burgers juist. Keuzevrijheid is een ideaal dat vrijwel iedereen onderschrijft, maar het kan ook mentale belasting en keuzestress met zich meebrengen. Dat speelt nog sterker op het moment dat een individu, al dan niet door eigen toedoen, met gezondheidsproblemen of schulden te maken krijgt of zijn baan verliest.

De redzaamheidsparadox speelt bijvoorbeeld bij pensioenopbouw, aldus de WRR. Zo zijn voor de grote meerderheid van de Nederlanders “meer keuzemogelijkheden en vrijheid op pensioengebied eerder een probleem dan een oplossing”. Grotere keuzevrijheid kan op korte termijn de autonomie vergroten, maar deze op lange termijn juist schaden, namelijk als men de verkeerde keuzes blijkt te hebben gemaakt en onvoldoende pensioen heeft opgebouwd. Tegen de tijd dat duidelijk wordt dat men de verkeerde keuzes heeft gemaakt, is het te laat om die nog te herstellen. Het is natuurlijk verstandig om werknemers al aan het begin van hun carrière te informeren over noodzaak van en mogelijkheden voor pensioensparen, maar het is naïef te denken dat hiermee het probleem ook is opgelost. Of om te denken dat mensen hun pensioen niet belangrijk vinden als ze keuzes maken die voor de lange termijn niet positief uitpakken⁶³.

Beleid dat zich richt op het vergroten van de mentale vermogens van burgers dient de autonomie van burgers zo min mogelijk aan te tasten en per saldo de redzaamheid van burgers te vergroten. De overheid kan zeker stimuleren dat deze programma's worden aangeboden, maar het wordt paradoxaal wanneer zij deze wil verplichten. Men kan mensen niet dwingen autonoom te zijn, aldus de WRR.

1.1.4.3 ICT Uitvoeringsorganisatie (ICTU)

ICTU is een onafhankelijke advies- en projectenorganisatie binnen de overheid. ICTU helpt overheden bij het verbeteren van hun dienstverlening met ICT, in dienst van het openbaar bestuur.

ICTU

MARE Research: wat willen mensen?

MARE Research⁶⁴ deed in 2019 in opdracht van ICTU kwalitatief onderzoek naar wat mensen willen. Mensen uiten niet uit zichzelf een directe behoefte aan (meer) ROG, omdat ze op basis van de

⁶¹ Bron: Referentiearchitectuur Regie Op Gegevens, ICTU 2021

⁶² Weten is nog geen doen, WRR 2017

⁶³ Krijnen, J. M., M. Zeelenberg and S.M. Breugelmans (2015). 'Decision importance as a cue for Deferral'. Judgment and Decision Making, 10 (5): 407.

⁶⁴ Inzichten uit onderzoek Hoe denken mensen over regie op gegevens? Via <https://rog.pleio.nl/>

huidige praktijk zich niet bewust zijn dat zij meer regie zouden kunnen hebben. Doorpratend over het concept blijkt dat ze meer regie echter wel heel wenselijk vinden. Een toekomstbeeld waarin de burger centraal wordt gesteld en meer regie krijgt op zijn eigen gegevens wordt positief ontvangen door mensen. Er is volgens MARE een volgorde aan te brengen in de behoeften rondom het uitwisselen van gegevens:

- Primaire behoeften
 - Gebruiksvriendelijker en gemakkelijker maken ("Minder gedoe");
 - Snellere afhandeling;
 - Meer overzicht van de te zetten stappen.
- Secundaire behoeften
 - Minder vaak opnieuw dezelfde gegevens moeten aanleveren rondom één en dezelfde (levens)gebeurtenis;
 - Vaker automatisch doorgeven van gegevens (zij het alleen tussen overheden onderling);
 - Minder 'onnodige' berichtgeving indien situatie ongewijzigd is, zoals een standaard periodieke bevestiging;
 - Meer feedback of informatie over voortgang;
 - Betere bescherming van privacy door meer inzicht in en controle op welke gegevens bij welke organisaties bekend zijn.

Wanneer mensen zelf drie aspecten van ROG mogen prioriteren, wordt volgens MARE Research de volgende volgorde aangegeven:

1. Systeem van toestemming. Wanneer de burger bepaalt welke organisatie gegevens mag verwerken (zoals het gebruiken en delen van gegevens) biedt dat overzicht, veiligheid (privacy) en zal dat de efficiëntie ten goede komen.
2. Overzicht van gegevens per organisatie. Een dergelijk overzicht brengt transparantie in de tot nu tot onoverzichtelijke situatie en biedt de mogelijkheid om te controleren.
3. Mogelijkheid tot aanpassen of verwijderen. Dit stelt in zekere mate gerust omdat fouten of verouderde data aangepast kunnen worden en daarmee schade kan worden voorkomen.

Over het delen van gegevens - die de overheid heeft - buiten deze overheid is men aanmerkelijk minder enthousiast, aldus MARE Research.

Mensen hechten volgens MARE Research⁶⁵ minder waarde aan de mogelijkheid om inzicht te krijgen in welke gegevens precies gebruikt zijn voor het verlenen van een specifieke dienst. Zij denken dat met het geven van dit soort inzichten het juist ingewikkelder en tijdrovender wordt.

TrueTalk: wat willen mensen?

TrueTalk ontmoette in opdracht van ICTU in totaal 61 mensen van alle rangen en standen voor dialogen van 15-20 minuten⁶⁶. Mensen hebben volgens het onderzoek weinig met ROG. Ze kunnen zich slecht een voorstelling maken bij het thema. Het onderwerp levert - alleen desgevraagd - een wolk van passieve reacties op, die zeer uiteenlopend zijn. Het concept 'ROG' is qua abstractieniveau voorbij de denkhorizon van de gemiddelde deelnemer, en het kost deelnemers moeite om een concrete voorstelling te maken van het concept.

True Talk plaatst hierbij de volgende kanttekeningen:

- Het onderwerp 'zorg' binnen 'ROG' slaat wel aan: hierbij zagen mensen een (praktisch) voordeel in het kunnen delen van hun gegevens.
- Mensen ervaren weinig problemen in het huidige 'regelwerk', ze vertrouwen de overheid redelijk. Regelwerk hoort er 'gewoon' bij. Burgers zien niet snel de voordelen (gemak en verminderen risico's) van het programma.
- Mensen ervaren in de huidige situatie geen grip: "Iedere organisatie weet alles en daar heb ik geen grip op." Men reageert gelaten en beetje negatief.
- Digitalisering maakt mensen minder bereikbaar door de overheid. Het wordt eerder negatief dan positief ontvangen. Grote groepen mensen haken af, en zien meer risico's en minder kansen.

⁶⁵ Kwalitatief onderzoek: Burgerperspectief op Regie Op Gegevens, MARE: 2019341, 18 december 2019

⁶⁶ TrueTalk, Regie Op Gegevens, Een verkennend onderzoek, (RoG) ICTU, 11 december 2019

- Mensen hebben geen scherp beeld van waar de overheid begint en eindigt. Gevraagd naar bekendheid met overheidsorganisaties werden ook grote organisaties als verzekeraars, zorginstellingen en nutsbedrijven genoemd.

1.1.4.4 Rijksdienst voor Identiteitsgegevens (RvIG)

RvIG beheert onder meer de Basisregistratie Personen (BRP) en is verantwoordelijk voor de technische systemen voor de opslag en uitwisseling van persoonsgegevens. RvIG geeft de Burgerservicenummers uit, die de basis vormen voor de uitwisseling van die gegevens.



Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Virtueel identiteitsbewijs (vID) en SSI

vID is een mogelijke digitale variant van het vertrouwde paspoort of de ID-kaart, met dezelfde hoge veiligheidseisen als het huidige fysieke document⁶⁷. vID is een nieuwe virtuele verschijningsvorm van een reis- of identiteitsdocument in de vorm van een app op je mobiel. RvIG maakt hierbij gebruik van Self sovereign identity⁶⁸, ofwel SSI, een ontwikkeling waarmee mensen zelf de regie krijgen over hun eigen gegevens. Het gaat dan om gegevens over iemands identiteit, maar ook bijvoorbeeld over een diploma of een registratie bij de Kamer van Koophandel. Dit worden ook wel 'verklaringen' genoemd, die zijn gekoppeld aan een specifieke persoon, via een digitale identiteit. Met SSI beschikt een persoon zelf over eigen digitale verklaringen, en over zijn/haar digitale identiteit, in plaats van overheden of (grote) technologiebedrijven. SSI maakt het ook mogelijk dat een persoon, op een veilige manier, alleen gegevens deelt die voor een bepaalde (rechts)handeling nodig zijn, wat de privacy vergroot.

1.1.4.5 Estland (e-estonia)

Vanaf 1994 heeft de overheid van Estland (1,3 miljoen inwoners) gewerkt aan een digitale overheidsinfrastructuur onder het concept e-estonia.⁶⁹ Begin deze eeuw leidde dit tot de introductie van de X-road infrastructuur voor gegevensuitwisseling en e-ID en digital signature services. Stap voor stap heeft Estland, op basis van een uitgangssituatie waar er helemaal geen infrastructuur was, zich ontwikkeld tot een geavanceerde e-overheid infrastructuur. Volgens een benchmark vanuit het perspectief van de EU zijn Estland, Oostenrijk en Malta koplopers in Europa⁷⁰.



Estland biedt regie op bijvoorbeeld de eigen (medische) gegevens: inzage is mogelijk in wie deze raadpleegde. Misbruik kan worden bestraft. 'So officials watch out because the citizen is watching you'⁷¹.

Volgens een recent Nederlands rapport⁷² wordt in Engeland, Roemenië, Finland en Estland de personal data industrie zowel organisatorisch als financieel geholpen. Estland wordt als het gaat om het aanjagen van digitalisering door velen als lichtend voorbeeld gezien. Estland schat dat ze met het invoeren van een digitale handtekening jaarlijks 4% van hun BNP besparen⁷³. Estland blinkt niet zo zeer uit door het toepassen van de aller modernste technieken, maar doordat ze digitale dienstverlening letterlijk voor iedereen toegankelijk hebben gemaakt⁷⁴.

⁶⁷ <https://magazines.rvig.nl/idee/2019/10/vid-het-id-van-de-toekomst>

⁶⁸ <https://magazines.rvig.nl/idee/2019/10/ssi>

⁶⁹ <https://e-estonia.com/>

⁷⁰ <https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2019-trust-government-increasingly-important-people>

⁷¹ <https://www.ictu.nl/impressie-plenaire-sessie-e-estonia-digitale-overheid-van-de-toekomst>

⁷² <https://kennisopenbaarbestuur.nl/media/255847/greenpaper-regie-op-gegevens-durf-te-doen.pdf>

⁷³ <https://ibestuur.nl/nieuws/wordt-de-burger-eigen-databaas>

⁷⁴ <https://www.overheidincontact.nl/estland-laet-grenzen-digitaal-verdwijnen/>

1.1.4.6 Australië⁷⁵

Ook buiten Europa zijn er initiatieven rond toegang tot en deling van persoonlijke data. Vooral interessant zijn de ontwikkelingen rond Open Data in Australië⁷⁶, mede gelet op de vele publicaties⁷⁷. Daar is naar analogie van de AVG een Consumer Data Right (CDR) gedefinieerd. Daarin is ook de uitwisseling van data over verschillende sectoren via specifieke standaarden geïntroduceerd.



Voor het Consumer Data Right (CDR) gelden deze vier uitgangspunten:

1. It should be consumer focused;
2. It should encourage competition;
3. It should create opportunity's;
4. It should be efficient and fair.

Het CDR wordt voor meerdere sectoren van toepassing verklaard, waarbij Open Data gefaseerd wordt ingevoerd voor verschillende sectoren, zoals banken (Open Banking), energie (Open Energy), gevolgd door de telecomsector (Open Telco). Daarnaast bepaalt de leidende toezichthouder de Australian Competition & Consumer Commission (ACCC) de sectoren die in scope van Open Data vallen.

Denkbare sectoren zijn transport, platformbedrijven, social media-platformen enzovoort.

Als leidende toezichthouder voor het CDR is gekozen voor de ACCC, deels vergelijkbaar met de rol van De Nederlandse Bank bij het vaststellen van het verlenen van accreditaties. De Consumer Data Standards worden vastgesteld door een aparte entiteit, de Data Standards Board.

Onderdeel van de standaarden zijn principes⁷⁸. Naast technische principes – onder meer voor API's – zijn principes voor consumentervaring gespecificeerd.

Bijvoorbeeld:

- De ervaring van de CDR-consument is intuïtief en is gericht op de attitudes, behoeften, gedragingen en verwachtingen van de consument, waarbij wordt opgemerkt dat deze in de loop van de tijd kunnen veranderen.
- De CDR is toegankelijk en inclusief. Een breed scala aan mensen is in staat om het CDR-ecosysteem te openen, te gebruiken en te begrijpen, ongeacht hun achtergrond, situatie, ervaring of persoonlijke kenmerken.
- De CDR is begrijpelijk. Bij interactie met de CDR kunnen consumenten het volgende begrijpen:
 - met wie hun gegevens worden gedeeld;
 - welke informatie wordt gedeeld;
 - wanneer het delen begint en stopt;
 - waar gegevens van en naar worden gedeeld;
 - waarom hun gegevens worden opgevraagd; en
 - hoe ze het delen en gebruiken van hun gegevens kunnen beheren en controleren.

De interactie van de consument met de CDR is zo eenvoudig mogelijk, maar gaat niet ten koste van geïnformeerde toestemming, controle door de consument, transparantie, privacy of begrip.

Toestemming wordt op een bepaald moment verleend en is slechts zo actueel als de oorspronkelijke bedoeling van de consument.

1.1.5 Wetenschappelijke instituten

De wetenschap stimuleert de publieke en politieke meningsvorming over privacy en bescherming van persoonsgegevens. Voorbeelden zijn het Rathenau Instituut (met onder meer aandacht voor cyber weerbaarheid⁷⁹), de Universiteit van Tilburg⁸⁰ en de Radboud Universiteit. Bekende namen aan de laatste instelling zijn Bart Jacobs en Jaap-Henk Hoepman. De heer Jacobs is onder andere de

⁷⁵ <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0>

⁷⁶ <https://www.opendataaustralia.org/>

⁷⁷ <https://www.opendataaustralia.org/resources>

⁷⁸ <https://consumerdatastandardsaustralia.github.io/standards/#principles>

⁷⁹ <https://www.rathenau.nl/nl/digitale-samenleving/cyberweerbaar-met-nieuwe-technologie>

⁸⁰ Zie bijvoorbeeld de publicaties van Lokke Morel en Bert-Jaap Koops.

geestelijke vader van IRMA en de heer Hoepman hoofddocent privacybevorderende protocollen en privacy by design.

1.1.5.1 Stichting Privacy By Design

Vanuit de Radboud Universiteit is de Stichting Privacy By Design ontstaan. Deze stichting wil in algemene zin de ontwikkeling en het gebruik van open, privacyvriendelijke en goed-beveiligde ICT bevorderen. De stichting richt zich tegenwoordig vooral op ontwikkeling en gebruik van IRMA.



1.1.5.2 Privacy & Identity Lab (PI.lab)

Het Privacy & Identity Lab (ook bekend als het PI.lab⁸¹) is opgericht op 11 november 2011 als een samenwerking tussen de Radboud Universiteit Nijmegen (RU), Stichting Internet Domeinregistratie Nederland (SIDN), Tilburg Institute of Law, Technology, and Society (TILT) en TNO. Doel van deze samenwerking is het oprichten van een multidisciplinair, nationaal en internationaal expertisecentrum voor onderzoek en innovatie op het gebied van digitale privacy en identiteit.



In juli 2020 richtte het PI.lab zich op anonimisering door meerpartijenberekening. De analyse van gegevens uit verschillende bronnen wordt steeds belangrijker. Naast het creëren van meerwaarde leidt het proces van het combineren van verschillende datasets tot nieuwe inzichten, betere besluitvorming en robuuster onderzoek (inclusief marktonderzoek), naast sterkere producten en diensten. Tegelijkertijd zijn relevante gegevens vaak te gevoelig om terloops met anderen te delen. Het PI/lab stelt zich derhalve de vraag: hoe kunnen organisaties informatie veilig delen zonder onderliggende gegevens van gevoelige aard prijs te geven? Een innovatieve oplossing om de functionaliteit van een gedeelde database te genereren zonder de gegevens te hoeven onthullen, is Multi-Party Computation (MPC). MPC is een 'toolbox' van cryptografische technieken waarmee verschillende partijen gezamenlijk data kunnen berekenen, net alsof ze een gedeelde database hebben.

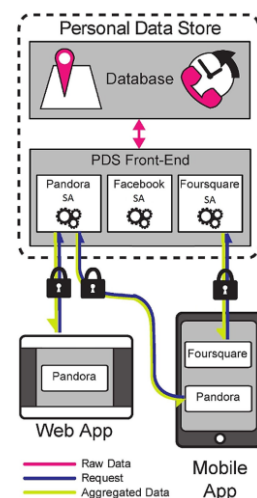
1.1.5.3 TNO⁸²

Hoe kunnen de barrières voor het delen van gegevens overwonnen worden? Dit doet TNO door samen te werken binnen consortia, door te laten zien dat innovatieve methoden werken (proof of concept) en door kennis in te zetten op specifieke (technische)gebieden zoals Secure Multi-Party Computation (MPC), International Data Spaces(IDS), betrouwbare Artificial Intelligentie (AI) en zelf-soevereine identiteit (SSI).

1.1.5.4 OpenPDS

OpenPDS⁸³ is een initiatief van het Massachusetts Institute for Technology (MIT). openPDS biedt een service en framework voor persoonlijke dataservices. De resultaten zijn als open source beschikbaar. Het is primair een research initiatief.

OpenPDS is van overtuigd dat het zeer moeilijk zal zijn om gegevens zoals geolocatie te anonimiseren met behoud van de waarde van de gegevens. Daarom zet openPDS het probleem op zijn kop met behulp van een innovatief SafeAnswers- framework. Met SafeAnswers kunnen applicaties vragen stellen die zullen worden beantwoord met behulp van de persoonlijke gegevens van de gebruiker. In de praktijk sturen applicaties code om tegen de gegevens te worden uitgevoerd en het antwoord wordt naar hen teruggestuurd. openPDS/SafeAnswers verzendt code, geen gegevens. .



⁸¹ <https://pilab.dev/>

⁸² <https://www.tno.nl/nl/aandachtsgebieden/informatie-communicatie-technologie/roadmaps/data-sharing/>

⁸³ <https://openpds.media.mit.edu/#architecture>

1.2 Wetgeving

Recente wetgeving zoals AVG, PSD2 en de aankomende Wet Digitale Overheid hebben een duidelijke invloed op de ontwikkelingen van het PDM-landschap. Deze wetten zijn niet specifiek gefocust op PDM, maar scheppen wel randvoorwaarden. Zo schuift door de AVG de macht over data meer in de richting van de persoon en heeft PSD2 ervoor gezorgd dat betaalgegevens onder bepaalde voorwaarden ontsloten moeten kunnen worden.

1.2.1 Wetgeving over eigendom van gegevens

Het Nederlandse rechtsstelsel kent geen bepaling over het eigendom van gegevens en data. Het eigendomsbegrip in het Burgerlijk wetboek is alleen van toepassing op stoffelijke zaken, en dat zijn gegevens en data niet⁸⁴. Er zal daarom volgens de auteurs te rade moeten worden gegaan bij minder expliciete wetgeving, bijvoorbeeld wetgeving die ingaat op de vraag wie rechthebbende is op de gegevens of data of wie aanspraak kan maken op de datadrager. Dat maakt de discussie en de uitkomst soms wat diffuus. Belangrijker voor dit juridisch kader is evenwel dat gegevens veilig en betrouwbaar, met regie van de burger, kunnen worden verwerkt.

1.2.2 Wet algemene bepalingen Burgerservicenummer (Wabb)

Overheidsorganen kunnen bij de uitvoering van hun taak gebruik maken van het Burgerservicenummer (BSN; artikel 10 Wabb) en moeten daar ook zoveel mogelijk gebruik van maken in de onderlinge communicatie (artikel 11 Wabb). Anderen dan overheidsorganen kunnen alleen gebruik maken van het BSN voor zover dat bij of krachtens de wet is geregeld. Dat geldt bijvoorbeeld voor zorgverleners, huisartsen, zorgverzekeraars en (collectief) pensioenverzekeraars. Denkbaar is dat aanbieders in het kader van een PDM-dienst een document ter beschikking stellen aan de burger, waarbij het BSN wordt vermeld. Hoewel het de burger in dat geval vrijstaat het document te verstrekken aan de afnemer inclusief het BSN, zal niet iedere afnemer gelet op het voorgaande bevoegd zijn het BSN te verwerken.

1.2.3 Algemene Verordening Gegevensbescherming (AVG)

1.2.3.1 Inleiding

De Algemene verordening gegevensbescherming (AVG)⁸⁵ gaat over het rechtmatig omgaan met persoonsgegevens. De AVG is de Nederlandse implementatie van de Europese verordening GDPR⁸⁶ (General Data Protection Regulation) en is vanaf 25 mei 2018 van toepassing. De belangrijkste regels voor omgang met persoonsgegevens zijn hierin vastgelegd. Deze regels hebben gezorgd voor een uitbreiding en versterking van de privacy-rechten van personen. In 2017 schreef SIVI een greenpaper over ROPG⁸⁷. 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. Gelet op het belang van de AVG wordt hierna uitleg gegeven over het belang van deze wetgeving. De AVG geeft toezichthouders, zoals de Autoriteit Persoonsgegevens in Nederland, de bevoegdheid om boetes op te leggen aan overtreders van deze verordening. De AVG is een van de belangrijkste aanjagers van PDM in Europa: het heeft ervoor gezorgd dat rechten van personen omtrent persoonlijke data en de manier waarop organisaties daarmee omgaan, sterk op de kaart gezet. Zowel politiek, binnen organisaties en in de media. De rechten op inzage, rectificatie, vergetelheid en dataportabiliteit raken daarnaast sterk aan PDM: PDM-Diensten richten zich onder meer op het faciliteren van de uitvoering van deze rechten door de persoon. Door applicaties aan te bieden die gegevensuitwisseling mogelijk maken, terwijl deze rechten in acht worden genomen.



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.

⁸⁴ Juridisch kader voor Regie Op Gegevens, Sandra van Heukelom-Verhage en Nina Bontje, 24 januari 2020

⁸⁵ <https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg>

⁸⁶ <https://gdpr-info.eu/>

⁸⁷ <https://www.sivi.org/actueel/regie-op-persoonsgegevens/>

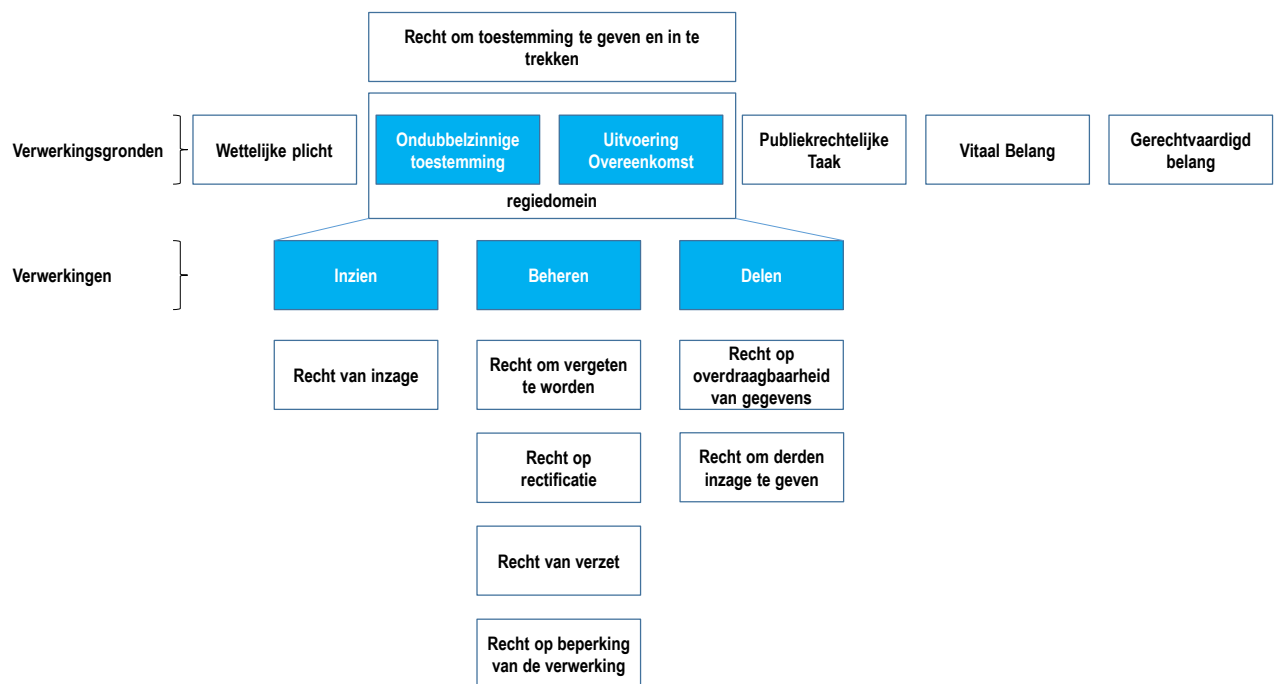
Minimaal één van de gronden moet van toepassing zijn; een combinatie van gronden is ook mogelijk. De AVG werkt de volgende zes gronden uit:

1. Toestemming
2. Uitvoering van een overeenkomst
3. Wettelijke plicht
4. Algemeen belang/openbaar gezag
5. Vitaal belang
6. Gerechtvaardigd belang

Afsluiten verzekering

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.

Figuur-2 geeft een overzicht wat onder het regiedomein wordt verstaan in het kader van de AVG. Het overzicht geeft de verschillende verwerkingsgronden en verwerkingen weer. In blauw staan de aspecten waar regie betrekking op heeft.



Figuur-2: Toelichting van het regiedomein conform AVG

1.2.3.2 Rechten voor consumenten

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 het verwerkingsverantwoordelijke besluit de gegevens te anonimiseren, mag ze deze bewaren, op voorwaarde dat ze niet tot een individu te herleiden zijn.

Inzien klantgegevens

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.

1.2.3.3 Dataportabiliteit

Artikel 20 van de Algemene Verordening Gegevensbescherming (AVG) introduceert het recht op dataportabiliteit. Het recht op dataportabiliteit (overdraagbaarheid van gegevens) houdt in dat de consument het recht heeft de persoonsgegevens "die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen", en deze gegevens "aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden tegengewerkt door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt". Het doel van dit nieuwe recht is de positie van consumenten te versterken en hen meer controle over hun gegevens te geven.

De Europese Unie ziet het recht op dataportabiliteit als een belangrijk middel in de vrije stroom van persoonsgegevens binnen de EU. Het zou concurrentie in de hand moeten werken. Consumenten

zouden makkelijker van dienstverlener kunnen veranderen, wat de ontwikkeling van nieuwe diensten binnen de digitale eenheidsmarktstrategie aanmoedigt. De consument heeft volgens Artikel 20 namelijk ook "het recht dat de persoonsgegevens, **indien dit technisch mogelijk is**, rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden."

De Europese toezichthouders doen een oproep aan alle belanghebbenden en brancheorganisaties om binnen hun domein samen te werken aan een set van standaarden en formaten om het recht op dataportabiliteit vorm te geven.

Leidend document

De Artikel 29-werkgroep heeft in april 2017 de (definitieve) Guidelines on the right to data portability gepubliceerd die meer uitleg geven over het recht op dataportabiliteit.

De NVB⁸⁸ vraagt "de Nederlandse overheid om op Europees niveau verdere invulling te geven aan het bestaande recht op dataportabiliteit en het recht op vergetelheid zoals vastgelegd in de AVG, waardoor data-eigenaren grip op en controle hebben over hun persoonlijke data. De overheid wordt gevraagd om hiervoor een wettelijk kader te creëren, waarmee verplichte cross-sectorale data-deling mogelijk wordt gemaakt, zodat de kansen van de data-economie zo breed mogelijk kunnen worden benut. De consument zou meer centraal moeten worden gezet bij veilige en efficiënte data-toegang en data-deling. Er ontstaat een toenemende data-macht bij enkele partijen. Om de balans te herstellen, is versterking nodig van de positie van individuen en bedrijven in hun rol als data-eigenaren.

"Verder zou de overheid randvoorwaarden moeten scheppen voor een afsprakenstelsel dat de positie van de data-eigenaar – de consument – versterkt als het gaat om de regie van en controle op zijn data. De AVG en PSD2 geven hierbij houvast. Maar bieden nog niet de juiste randvoorwaarden om daadwerkelijk controle en inzicht te bieden bij data-deling. Het gedachtegoed van PSD2 kan wel worden gebruikt voor veilige en efficiënte toegang tot en deling van persoonlijke data."

Welke gegevens wel en niet

De wettelijke basis: digitale persoonsgegevens verstrekt door de consument

Dit betreft alle digitale persoonsgegevens die een dienstverlener van de consument verwerkt; ófwel met toestemming van de consument, ófwel om een overeenkomst met de consument uit te voeren. De dienstverlener dient bij een verzoek tot dataportabiliteit alle persoonsgegevens beschikbaar te stellen die de desbetreffende consument aan hem heeft verstrekt.

Observed data

De Artikel 29-werkgroep stelde dat het niet alleen om gegevens gaat die consumenten actief en bewust hebben verstrekt (bijvoorbeeld e-mailadres, gebruikersnaam, leeftijd etc.), maar ook om de gegevens die consumenten indirect hebben 'verstrekkt' door een dienst of apparaat te gebruiken: zogenaamde observed data. Hieronder vallen bijvoorbeeld de zoekgeschiedenis, locatiegegevens of andere (ruwe) data als de hartslag die via een fitnesstracker is vastgelegd.

Hoewel de Europese Commissie deze redenering van de Artikel 29-werkgroep aanvankelijk betwistte⁸⁹, volgt de Nederlandse toezichthouder (de Autoriteit Persoonsgegevens) de richtlijn van de Artikel 29-werkgroep⁹⁰: "Het gaat ook om de gegevens die klanten aan u hebben 'verstrekkt' door uw dienst of apparaat te gebruiken. Bijvoorbeeld de zoekgeschiedenis of locatiegegevens van uw klanten. Of andere (ruwe) data als de hartslag die via een fitnesstracker is vastgelegd."

Afgeleide gegevens hoeven niet verstrekt te worden

De dienstverlener hoeft bij een verzoek om dataportabiliteit géén afgeleide gegevens te verstrekken. Onder afgeleide gegevens (inferred data) vallen persoonsgegevens die de dienstverlener zelf heeft gegenereerd door bijvoorbeeld uitvoerige analyse of het opstellen van een – op basis van verstrekte

⁸⁸ <https://www.vvponline.nl/nieuws/banken-pleiten-voor-balans-tussen-eigenaar-en-gebruiker-van-data?mid=k52XqW5jmGSYkQ==>

⁸⁹ <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/>

⁹⁰ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#wat-houdt-het-recht-op-dataportabiliteit-in-6345>

gegevens berekende – kredietscore of klantprofiel⁹¹. Hieronder vallen dus ook gegenereerde adviesdossiers, waarvan het soms wel degelijk wenselijk kan zijn deze te verstrekken bij een verzoek om dataportabiliteit. De dienstverlener is hier echter, in tegenstelling tot bij een inzageverzoek, niet toe verplicht: het recht op inzage is breder dan het recht op dataportabiliteit.

Gegevens die waarde hebben voor de consument

De verstrekte data dienen waarde voor de consument te hebben. Dat wil zeggen: het heeft geen nut om meer data aan te bieden dan de consument behoeft. Omdat het enerzijds onwenselijk is om voor de consument te bepalen wat wel en niet waardevol is, en dit per individu zal verschillen, en het anderzijds voor consumenten lastig zal zijn om uit alle (onder meer machineleesbare) data zelf selecties te maken, bieden de dataverstrekkingen idealiter zelf een selectiemogelijkheid aan voorafgaand aan het proces van downloaden/exporteren.

Metagegevens meeleveren

Een dienstverlener moet niet alleen de feitelijke inhoud leveren, maar ook zoveel mogelijk relevante metagegevens meeleveren. Zoals tijdstip, afzender, geadresseerde etc. Hierdoor blijft de betekenis van de overgedragen informatie zo goed mogelijk bewaard.

Wettelijke basis: gestructureerd, gangbaar en machineleesbaar formaat

Bij het recht op dataportabiliteit moeten dienstverleners de gegevens verstrekken in een vorm die het voor consumenten gemakkelijk maakt om hun gegevens te hergebruiken en door te geven aan een andere organisatie, als ook direct inleesbaar te maken voor de nieuwe organisatie. Dienstverleners zijn daarom wettelijk verplicht om de gegevens in een gestructureerd, gangbaar en machineleesbaar formaat te verstrekken. Die laatste eis wordt hieronder verder toegelicht.

Overweging 21 van Richtlijn 2013/37/EU¹⁷ definieert 'machineleesbaar' als een bestandsformaat met een zodanige structuur dat softwaretoepassingen gemakkelijk specifieke gegevens in het document kunnen identificeren, herkennen en extraheren. Gegevens die zijn gecodeerd in bestanden die in een machinaal leesbaar formaat zijn gestructureerd, zijn machinaal leesbare gegevens. Machinaal leesbare formaten kunnen open of geïncapsuleerd zijn; zij kunnen al dan niet formele standaards zijn. Documenten die zijn gecodeerd in een bestandsformaat dat een automatische verwerking beperkt – doordat de gegevens niet of niet gemakkelijk uit de documenten kunnen worden gehaald – vallen hier niet onder.

Experts stellen⁹² dat het gebruik van open formats (zoals CSV, XML en JSON) de meest voor de hand liggende optie is voor het porteren van data. Open formats vallen immers niet onder de bescherming van intellectueel eigendom, en kunnen zodoende zonder restricties worden geïmplementeerd. Daarnaast zijn ze gebaseerd op open standaarden, zijn ze goed gedocumenteerd en worden ze met grote regelmaat geüpdatet en ontwikkeld. Dit sluit goed aan bij het doel van het recht op dataportabiliteit: meer interoperabiliteit en leveranciersafhankelijkheid bereiken.

Standaard voor dataportabiliteit

SIVI publiceerde in 2018 een standaard voor dataportabiliteit⁹³, gebaseerd op de gegevensstandaard AFD. Het gebruik is tot nu toe zeer beperkt, afgaande op het aantal vragen dat hierover bij SIVI is gesteld.

1.2.3.4 Gedragscodes

Een branche of sector die een gedragscode heeft opgesteld, kan aan de AP vragen om deze goed te keuren. De AP keurt een gedragscode goed als deze aan de eisen voor een gedragscode voldoet. Het is hierbij vooral belangrijk dat de gedragscode een concrete uitwerking van de AVG biedt. De organisatie die de gedragscode heeft opgesteld, moet ook zorgen voor toezicht op de gedragscode door het instellen van een toezichthoudend orgaan. Dit orgaan controleert de naleving van de gedragscode, beoordeelt of aangesloten partijen in aanmerking komen om de gedragscode toe te

⁹¹ De Wft kent ook een verplichting om te stellen klantprofiel met volledig door de klant verstrekte gegevens. Deze moeten bij een verzoek tot dataportabiliteit volgens de richtlijnen beschreven in 2.3.2 wel aan de klant geleverd worden.

⁹² https://www.oi.ut.ee/sites/default/files/oi/data_portability_noormaa_sulskute_terjuhana.pdf

⁹³ <https://www.sivi.org/actueel/standaard-voor-dataportabiliteit/>

passen en behandelt klachten over inbreuken op de gedragscode. De AP moet het toezichthoudend orgaan accrediteren.

De AP heeft eind augustus 2020 de Data Pro Code van branchevereniging NLdigital goedgekeurd⁹⁴. Dit is een gedragscode waarbij organisaties in de ICT-sector zich kunnen aansluiten. Veel van de leden van NLdigital treden voor hun opdrachtgevers op als verwerker van persoonsgegevens. De Data Pro Code is bedoeld om deze bedrijven te helpen om aan de verplichtingen uit de Algemene verordening gegevensbescherming (AVG) te voldoen.

1.2.3.5 Evaluatie AVG

Het beeld bij experts is dat het bewustzijn van privacy door de AVG is toegenomen⁹⁵. Zowel bij bedrijven als bij burgers. Bij de AP komen jaarlijks ruim 20.000 klachten binnen. Het bedrijfsmodel van de grote technologiebedrijven en datahandelaren is echter grotendeels ongemoeid gebleven. Zij verzamelen nog steeds data, combineren die tot profielen en verkopen die aan derde partijen voor advertenties. Een belangrijke oorzaak is dat de toezichthouders niet veel aan handhaving hebben gedaan. Serieuze boetes zijn op de vingers van één hand te tellen. De financiën en de slagkracht van 28 Europese toezichthouders zijn over het algemeen bescheiden. Privacydeskundigen maken zich ook zorgen over de centrale rol die toestemming speelt in de AVG. Als een consument eenmaal toestemming heeft gegeven, mag er veel. Maar is de doorsnee consument wel in staat tot een geïnformeerde keuze?

- 'Je kunt de verantwoordelijkheid voor een faire digitale maatschappij niet baseren op een systeem waar burgers toestemming moeten geven voor verwerkingen die ze niet begrijpen'
Lokke Moerel, hoogleraar ICT/Recht Tilburg en privacyadvocaat
- 'De AVG heeft zeker bijgedragen aan bewustwording van privacy, maar echt begrijpen wat er met je data gebeurt is wat anders. Zelfs de echte experts komen er nauwelijks achter wat onder de motorkap van techbedrijven plaatsvindt.'
Marietje Schaake, docent aan Stanford University in de Verenigde Staten

Boetes

Het aantal GDPR-boetes is in Europa bijna 60,2 miljoen euro⁹⁶. Opmerkelijk is dat het grootste deel van de boetes aan een handvol bedrijven wordt uitgedeeld. Boetekampioen, met ruime voorsprong, blijkt Italië te zijn, dat in zijn eentje voor meer dan 45,5 miljoen euro aan boetes oplegde. In het aantal boetes blijkt Spanje de leider te zijn, met 76 stuks. In totaal werd in Spanje echter voor nog geen twee miljoen euro geïnd.

Het jaarverslag van de Autoriteit Persoonsgegevens geeft aan dat de AP in 2019 4 boetes oplegde voor overtredingen van de AVG. Deze overtredingen gingen over toegang tot medische dossiers, verkoop van ledengegevens, biometrie (vingerafdrukken) en inzagerechten. Daarnaast legde de AP 7 keer een corrigerende maatregel op.

1.2.4 eIDAS

De Europese eIDAS-verordening voor erkenning van nationale elektronische identificatie-oplossingen is op 29 september 2018 ingegaan^{97,98}. De verordening bepaalt dat publieke organisaties en private organisaties met een publieke taak Europees erkende inlogmiddelen moeten accepteren binnen de digitale dienstverlening. Deze verplichting geldt onder meer voor organisaties die gebruik maken van DigiD. De Europese Unie wil hiermee regelen dat het makkelijker en veiliger wordt om binnen Europa online zaken te regelen. Bij een eIDAS login wordt in ieder geval een minimale set van



⁹⁴ <https://autoriteitpersoonsgegevens.nl/nl/nieuws/gedragscode-nldigital-goedgekeurd-door-ap>

⁹⁵ <https://fd.nl/ondernemen/1345538/privacywet-mist-na-twee-jaar-nog-steeds-tanden>

⁹⁶ <https://www.computable.nl/artikel/nieuws/overheid/7044097/250449/ruim-zestig-miljoen-euro-aan-gdpr-boetes-uitgedeeld.html>

⁹⁷ <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32014R0910>

⁹⁸ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/eidas/>

persoonsgegevens uitgewisseld met de betreffende dienstverlener. Deze set bestaat uit voornaam en achternaam en geboortedatum en persistent identifier (denk aan een BSN). Optioneel kunnen ook adres, geslacht, geboorteplaats en familienaam (naam bij geboorte) worden opgevraagd.

eIDAS betekent dus dat een burger woonachtig in een bepaald EU-land met een middel uit dat land (mits erkend door EU) kan inloggen bij de Nederlandse overheid, pensioenuitvoerders en zorgverzekeraars. eIDAS is slechts beperkt uitgerold.

Status eIDAS (medio 2021)⁹⁹

In onderstaande tabel zijn EU-lidstaten opgenomen in de verschillende fasen van het erkenningsproces. Een EU-lidstaat kan één of meerdere stelsels met bijbehorende eID's hebben in de verschillende fasen van het erkenningsproces. Er worden alleen EU-lidstaten weergegeven.

Erkend en actief in NL	Erkend niet actief in NL	In erkenningsproces
België Duitsland Estland Italië Kroatië Letland Luxemburg Portugal Slowakije Spanje Tsjechië	Denemarken	<u>Positief oordeel lidstaten:</u> <u>Nog geen oordeel lidstaten:</u> Frankrijk Malta Zweden

Eind augustus 2020 werd DigiD erkend als middel onder eIDAS¹⁰⁰.

1.2.5 Wet Digitale Overheid (WDO)

De WDO is een kaderwet: regelt functionaliteiten en kadert in lagere regelgeving verder in. Om techniek verantwoorde de ruimte te bieden is wendbaarheid en flexibiliteit noodzakelijk. De systematiek is stapsgewijs, in tranches. Nu ligt de eerste tranche voor. De WDO¹⁰¹¹⁰² - voorheen wet generieke digitale infrastructuur - is in februari 2020 aangenomen door de tweede kamer, maar ligt op moment van schrijven nog bij de eerste kamer. De WDO betreft een infrastructuur voor het authenticeren van burgers; publieke dienstverleners zijn verplicht de authenticatiemiddelen die zijn toegelaten onder de WDO te accepteren. In ieder geval zullen dit DigiD en eHerkenning zijn. De gegevens die onder WDO kunnen worden uitgewisseld zijn ook de gegevens die de toegelaten authenticatiemiddelen kunnen verwerken. Voor DigiD is dat voorlopig BSN en voor eHerkenning is dat op dit moment een pseudoniem van de gebruiker, een KvK nummer van het bedrijf namens wie deze handelt en een machtiging hiervoor.



De WDO biedt nu de mogelijkheid om bij AMvB open standaarden te verplichten en gaat private middelen erkennen, waarmee ingelogd kan worden bij de overheid. Die middelen worden daarmee breder bruikbaar dan nu en kunnen ook gebruikt worden om bij onder meer verzekeraars in te loggen. Dat laatste kan nu ook al, maar burgers/consumenten beschikken dan over breed inzetbare middelen. Die genoemde private middelen zouden overigens ook aangeboden kunnen worden door buitenlandse spelers.

De Eerste Kamer stelde in augustus 2020 de vraag aan minister Knops waarom bij de Wet Digitale Overheid niet uitgegaan wordt van attriboot gebaseerde authenticatie, open source en een decentraal

⁹⁹ Dashboard eIDAS editie juli 2021

¹⁰⁰ <https://www.digitaleoverheid.nl/nieuws/digid-erkend-als-europees-inlogmiddel/>

¹⁰¹ <https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34972>

¹⁰² <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/>

systeem. Hierbij kan bijvoorbeeld gedacht worden aan IRMA. Zowel attribuuat gebaseerde authenticatie als IRMA worden verderop in dit rapport besproken.

Vragen van de Eerste Kamer bij het wetsvoorstel digitale overheid (WDO) leidden uiteindelijk tot een wetswijziging. Met deze zogeheten 'novelle' wordt privacybescherming steviger in de wet verankerd. Er komt een wettelijk verbod op het verhandelen van gegevens en de principes 'privacy by design' en 'open source' worden in de wet opgenomen. Hierdoor wordt inloggen bij de overheid veiliger en betrouwbaarder. De aangekondigde wijziging (juni 2021 naar de Tweede Kamer gestuurd) betekent dat de Wet digitale overheid voorlopig niet in werking zal treden.

De tweede tranche van de WDO regelt verdere integratie: er ontstaat een integraal domein voor burgers en bedrijven. De weg is dan vrij voor het geïntegreerde burger-, bedrijfs- en organisatiemiddel. Daarbij zal er in ieder geval een geïntegreerd publiek middel beschikbaar zijn voor toegang tot overheidsdienstverlening. Daarnaast streven we naar een aanbod van private geïntegreerde burger-, bedrijfs- en organisatiemiddelen, en zullen we daarop sturen. Inwerkingtreding hiervan zal op zijn vroegst in 2024 zijn¹⁰³.

Tevens onderzoeken de ministeries van Binnenlandse Zaken en Financiën de ontwikkeling van een publiek middel voor bedrijven op basis van een juridische grondslag in de aanstaande uitvoeringsregelgeving behorend bij de WDO. Dit middel zal dan in eerste instantie alleen ingezet worden voor dienstverlening van de Belastingdienst, tot de tweede tranche van de WDO van kracht wordt en het middel breder ingezet zal worden. De invoering van het publieke middel voor het inloggen bij de Belastingdienst vindt plaats na het van kracht worden van de WDO. Het streven is het publieke middel vanaf de tweede helft van 2022 voor het inloggen bij de Belastingdienst beschikbaar te stellen en vanaf dan de compensatieregeling te vervangen.

1.2.6 Wet modernisering elektronisch bestuurlijk verkeer

Vanaf 2021 heeft de burger recht om elektronische berichten aan bestuursorganen te zenden op de door het desbetreffende bestuursorgaan aangegeven wijze¹⁰⁴. Met het voorstel, de Wet modernisering elektronisch bestuurlijk verkeer, wordt de Algemene wet bestuursrecht gewijzigd. De wet regelt dat burgers en bedrijven het recht krijgen om elektronisch zaken te doen met de overheid.

1.2.7 Wet op de Identificatieplicht (WID)

Deze wet wijst wettelijke identificatiemiddelen aan¹⁰⁵. Op de website van SZW staat een stappenplan voor werkgever om te voldoen aan de identificatieplicht¹⁰⁶.

Bij diverse authenticatieproviders binnen eHerkenning kan een machtigingenbeheerder (met middel op betrouwbaarheidsniveau 3) op relatief eenvoudige wijze voor collega's die in loondienst zijn, middelen op niveau 3 aanvragen. Een voorbeeld is het proces bij KPN/Recon¹⁰⁷. Deze medewerkers hoeven dan zelf geen identiteitsbewijs te overleggen. Ze hoeven zich niet te identificeren anders dan hun e-mailadres en telefoonnummer te bevestigen. De gegevens van de medewerkers kunnen via een CSV-bestand – dat aangemaakt wordt vanuit het personeelsinformatiesysteem - verstrekt worden. Het komt erop neer dat alle aanbieders van eHerkenningmiddelen behalve Digidentity meeliften op de wettelijke identificatieplicht van de werkgever.

1.2.8 Wet afwikkeling massaschade in collectieve actie (WAMCA)

Deze wet van 1 januari 2020 maakt de weg vrij voor het indienen van collectieve schadeclaims tegen organisaties die op grote schaal persoonsgegevens verwerken. Een burger zich mag laten

¹⁰³ Brief van Knops aan de Tweede Kamer, 14 juli 2021

¹⁰⁴ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-modernisering-elektronisch-bestuurlijk-verkeer/>

¹⁰⁵ <https://www.rijksoverheid.nl/onderwerpen/identificatieplicht>

¹⁰⁶ <https://www.inspectieszw.nl/onderwerpen/stappenplan-verificatieplicht>

¹⁰⁷ <https://www.recon.nl/eherkenning/machtigingenbeheerder/>

vertegenwoordigen door een belanghebbende stichting of vereniging; nu dus ook voor het vorderen van een schadevergoeding namens het individu. Voor individuen wordt het dus makkelijker om gezamenlijk in één procedure hun schade te claimen bij de (civiele) rechter. De verwachting van experts dat dit een vlucht gaat nemen¹⁰⁸.

The Privacy Collectieve diende in augustus 2020 een massaclaim¹⁰⁹ in tegen Salesforce en Oracle wegens misbruik van persoonsgegevens. De claim richt zich op het verzamelen, bundelen, verrijken en verkopen van digitale profielen van Nederlandse internetgebruikers, zonder dat zij daar toestemming voor hebben gegeven. De schadeclaim zou kunnen oplopen tot 10 miljard euro.

1.2.9 Archiefwet

De archiefwet is wetgeving uit 1995¹¹⁰ waarin beheer en toegang van overheidsarchieven geregeld wordt. Bewaartermijnen kunnen kort zijn, bijvoorbeeld een paar jaar, of lang, bijvoorbeeld tientallen jaren. Als de bewaartermijn voorbij is, moeten overheden de documenten vernietigen. In selectielijsten wordt vastgelegd welke informatie overheidsorganisaties willen bewaren en voor hoelang. De archiefwet is met name relevant voor overheidspartijen en PDM-oplossingen in de publieke sector, omdat deze wet in bepaalde gevallen betekent dat het recht op 'verwijderen' van gegevens niet op gaat. Hierbij kan bijvoorbeeld gedacht worden aan de plicht om een subsidiebeschikking te bewaren. Het recht op vergetelheid/gegevenswissing (artikel 17 AVG) geldt niet voor archiefinstellingen¹¹¹.



1.2.10 Wet Geneeskundige Behandelovereenkomst (WGBO)

De Wet op de geneeskundige behandelovereenkomst (WGBO¹¹²) regelt de rechten en plichten van de patiënt. Patiënten hebben recht op informatie en moeten toestemming geven voor een behandeling. Ook regelt de WGBO de privacy van de patiënt, het recht op een second opinion, het inzage-recht van patiënten in hun eigen medisch dossier en de vertegenwoordiging van patiënten als zij niet zelf kunnen beslissen. Daarnaast verplicht de WGBO zorgverleners om een medisch dossier bij te houden.

1.2.11 Wet cliëntenrechten bij elektronisch verwerking van gegevens

De Wet cliëntenrechten bij elektronische verwerking van gegevens is sinds juli 2017 van kracht. Deze wet verankert de rechten van patiënten over inzage en uitwisseling van gegevens binnen de gezondheidszorg. 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:

- De patiënt 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.
- De patiënt kan besluiten om slechts een deel van zijn gegevens beschikbaar te stellen en dus niet al zijn gegevens.
- De patiënt 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.

¹⁰⁸ <https://fd.nl/opinie/1346106/privacywet-avg-zal-in-toekomst-belofte-van-megaboetes-en-massaclaims-inlossen>

¹⁰⁹ <https://fd.nl/ondernemen/1353803/nederlandse-massaclaim-tegen-amerikaanse-techreuzen-vanwege-privacyschending>

¹¹⁰ <https://wetten.overheid.nl/BWBR0007376/2018-07-28>, en <https://www.rijksoverheid.nl/onderwerpen/archieven/archieven-van-de-overheid>

¹¹¹ <https://kia.pleio.nl/file/download/55812839/presentatie-yvonne-welings-avg-archiefwet-13-01-2010pdf>

¹¹² <https://www.rijksoverheid.nl/onderwerpen/rechten-van-patient-en-privacy/rechten-bij-een-medische-behandeling/rechten-en-plichten-bij-medische-behandeling>

1.2.12 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)

De wet aanvullende bepalingen verwerking persoonsgegevens in de zorg¹¹³ (Wabvpz). De Wabvpz regelt meer dan de cliëntenrechten, namelijk de randvoorwaarden voor elektronische gegevensuitwisseling in de zorg en de beschikbaarheid van gegevens via een elektronisch uitwisselingssysteem.

Sinds 1 juli 2017 mogen zorgaanbieders op basis van deze wet alleen gegevens beschikbaar stellen in een elektronisch uitwisselingssysteem als de patiënt daar uitdrukkelijk toestemming voor gegeven heeft. Daarnaast moet het systeem kunnen identificeren welke zorgverlener toegang wil tot dit systeem en met zekerheid vaststellen dat die zorgverlener ook werkelijk is wie hij zegt dat hij is (authenticatie). Ook moet het systeem gericht rechten voor toegang tot patiëntgegevens aan zorgverleners kunnen toekennen (autorisatie) en moet het mogelijk zijn te controleren wie toegang heeft (gehad) tot deze gegevens (logging).

Per 1 juli 2020 hebben patiënten recht op (kosteloze) elektronische inzage in hun dossier. Daarnaast moet de patiënt op verzoek een elektronisch overzicht ontvangen van de logging-gegevens van zijn medisch dossier.

Per een nader vast te stellen data moeten burgers hun eigen gegevens digitaal kunnen inzien (online inzage) en kunnen aangeven welke soort gegevens met welke zorgaanbieders mogen worden uitgewisseld bij behandeling (gespecificeerde toestemming). Gespecificeerd betekent dat burgers straks kunnen specificeren welke categorie van gegevens met welke categorie zorgverleners wel of niet gedeeld mag worden. De invoering zou plaats vinden per 1 juli 2020 maar is uitgesteld vanwege de praktische haalbaarheid¹¹⁴¹¹⁵.

Gespecificeerde toestemming

Deze brief gaat over gespecificeerde toestemming. Deze gespecificeerde toestemming geldt nadrukkelijk alleen voor die situaties waarin gegevens beschikbaar worden gesteld voor nog onbekend later gebruik. Als een zorginfrastructuur zo werkt is door die infrastructurele keuze gespecificeerde toestemming aan de orde. Terwijl het zorgproces daar helemaal niet om vraagt. In vrijwel alle gevallen gaat het immers om een behandelrelatie waarbinnen gegevens gewoon mogen worden uitgewisseld.

Het programma GTS heeft onderzoek gedaan naar een praktische uitwerking van gespecificeerde toestemming. Uit de eerste praktische uitwerking van de wet werden 160 toestemmingsmogelijkheden door PBLQ als juridisch optimum betiteld. Meerdere partijen, waaronder leden van de Tweede Kamer, plaatsten vraagtekens bij de haalbaarheid van dit hoge aantal toestemmingsmogelijkheden. Het programma GTS heeft daarom een alternatief scenario uitgewerkt met 28 toestemmingsmogelijkheden. Het Adviescollege toetsing regeldruk (ATR) heeft een oordeel uitgebracht over de werkbaarheid (van de uitwerking van) gespecificeerde toestemming. De ATR concludeert dat gespecificeerde toestemming niet van een werkbare invulling is te voorzien.

Kamerbrief 4 oktober 2019, Gespecificeerde Toestemming Structureel

1.2.13 Wegiz

De ministerraad stemde in april 2021 in met het wetsvoorstel elektronische gegevensuitwisseling in de zorg (Wegiz). Het doel van de wet is het stap voor stap verplichten van elektronisch of digitaal uitwisselen van medische gegevens tussen zorgverleners. Het wetsvoorstel heeft eerder al de gang naar de Raad van State afgelegd.

¹¹³ <https://wetten.overheid.nl/BWBR0023864/2020-07-01>

¹¹⁴ <https://www.avghelpdeskzorg.nl/onderwerpen/wabvpz/gespecificeerde-toestemming>

¹¹⁵ <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/04/kamerbrief-over-gespecificeerde-toestemming-structureel>

1.2.14 Diverse wet- en regelgeving voor bronnen van aanbieders

Bepaalde aanbieders van gegevens (ook wel genoemd: bronhouders) zullen aan specifieke wet- en regelgeving zijn gebonden met betrekking tot het verstrekken van gegevens. Gedacht kan worden aan het kadaster (Kadasterwet), de Kamer van Koophandel (Wet op de Kamer van Koophandel) en de Belastingdienst (artikel 67 AWR)¹¹⁶.



1.2.15 Europa

1.2.15.1 Privacy¹¹⁷

Privacy ("het recht om met rust gelaten te worden") is als grondrecht opgenomen in het Europees Verdrag voor de Rechten van de Mens (EVRM, art. 8), het Europees Handvest (art. 7) en de Grondwet. Grondrechten zien in beginsel op de verhouding tussen overheid en burger: de overheid respecteert de grondrechten van de burger (de zg. verticale werking). Daarnaast is in artikel 8 van het Handvest een expliciet recht op bescherming van de persoonsgegevens opgenomen. Met de AVG gelden ten aanzien van persoonsgegevens dezelfde regels tussen burgers (natuurlijke en rechtspersonen) onderling.

1.2.15.2 Data Strategie en Data Act

Begin 2020 kondigde de Europese Commissie haar nieuwe Data Strategie aan. Daarmee beoogt zij de introductie van een nieuwe Data Act. Die benadrukt nogmaals het versterken van individuele rechten om eigen data te hergebruiken. De scope van het huidige voorstel ligt op niet-persoonlijke data (zogenaamde industrial data). Voorbeelden¹¹⁸:

- real-time verkeersvermijdingsnavigatie kan tot 730 miljoen uur besparen. Dit vertegenwoordigt tot € 20 miljard aan arbeidskosten.
- real-time melding van vertraagde treinen kan 27 miljoen werkuren besparen. Dit komt neer op € 740 miljoen aan arbeidskosten.

De Nederlandse Vereniging van Banken bepleit om de scope van een Europese Data Strategie, en daarmee de nieuwe Data Act, uit te breiden tot de toegang tot en het delen van persoonlijke data.

1.2.15.3 Single Digital Gateway (SDG)

Op de langere termijn vormt de Europese verordening Single Digital Gateway¹¹⁹ (SDG) uit 2018 een verdere impuls voor eenmalige verstrekking van gegevens aan overheden. Deze heeft als doel om Europese burgers en bedrijven via één loket toegang te bieden tot informatie, procedures en ondersteuning voor het wonen, werken en ondernemen in andere lidstaten. De primaire focus ligt daarbij op circa twintig veelgevraagde, grensoverschrijdende diensten, zoals het registreren van een auto of het claimen van pensioenrechten. "De poort zal volledige toegang bieden tot een breed scala aan onlineprocedures om hen te helpen wanneer zij willen verhuizen, werken, studeren of op pensioen willen gaan, of wanneer zij in een ander land een onderneming willen opzetten of een activiteit willen uitoefenen. Dit is een belangrijke verwezenlijking voor de digitale eengemaakte markt"¹²⁰.

Uiterlijk in 2023 hebben Europese burgers en bedrijven het recht de noodzakelijke gegevens daarvoor slechts één keer te verstrekken. In opdracht van de ministeries BZK en EZK is een analyse gemaakt door ICTU om de verwachte effecten voor dienstverleners in kaart te brengen¹²¹. Inmiddels is besloten om op basis van actuelere informatie de kosten nader te inventariseren en te bezien waar gemeenschappelijke oplossingen de individuele implementatie kunnen ondersteunen.

¹¹⁶ Juridisch kader voor Regie Op Gegevens, Sandra van Heukelom-Verhage en Nina Bontje, 24 januari 2020

¹¹⁷ Referentiearchitectuur Regie op Gegevens, ICTU

¹¹⁸ <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy>

¹¹⁹ <https://www.youtube.com/watch?v=Znkoz0-P3sc>

¹²⁰ <https://www.consilium.europa.eu/nl/press/press-releases/2018/06/20/digital-single-gateway-easier-access-to-online-information-and-procedures/>

¹²¹ Verordening Single Digital Gateway Impactanalyse, ICTU april 2019

Overheidsorganisaties die vallen onder de verordening moeten ervoor zorgen, dat de informatie die hoort bij de betreffende dienstverlening en zogenoemde hulp- en ondersteuningsdiensten, niet alleen in de landstaal wordt aangeboden, maar ook in een veelgebruikte Europese taal. In Nederland is de keuze gemaakt voor het Engels als tweede taal.

Tevens dienen lidstaten bepaalde procedures die te maken hebben met belangrijke “life events” voor burgers en bedrijven volledig online én in een andere EU-taal beschikbaar te stellen. Deze procedures – in NL veelal aangeduid met de term “digitale overheidsdiensten” zijn onder meer:

- het laten registreren van een adreswijziging;
- het aanvragen van een nieuw paspoort of nieuwe identiteitskaart;
- het registreren van een motorvoertuig;
- het beroep doen op pensioenuitkeringen van publieke en semipublieke instellingen.

1.2.15.4 Data Governance Act

De Europese Commissie (EC) wil met de ‘Data Governance Act’ datadelen tussen landen en sectoren binnen de EU makkelijker en betrouwbaarder maken¹²². De kern van de verordening is dat zogenaamde data-intermediairs gaan functioneren als een neutrale partij die data-houders en data-gebruikers met elkaar verbindt. Deze intermediairs moeten een Europees alternatief bieden voor de grote techbedrijven; ze moeten aan strenge eisen gaan voldoen om hun neutraliteit te waarborgen. En ze mogen de gegevens niet op eigen initiatief verhandelen.

De verordening bestaat uit:

- Maatregelen voor meer vertrouwen in datadeling;
- EU-regels over neutraliteit voor de betrouwbaarheid data-intermediairs;
- Maatregelen om het gebruik van bepaalde overheidsdata in makkelijker te maken; bijvoorbeeld hergebruik van bepaalde gezondheidsgegevens;
- Manieren om Europese burgers en bedrijven zeggenschap te geven over het gebruik van hun data.

1.2.15.5 Digitale Wallet/Identiteitskaart EU¹²³

De Europese Commissie kondigde juni 2021 de introductie aan van een digitale portemonnee, die niet alleen als digitale ID-kaart moet dienen. In de app moeten mensen bijvoorbeeld ook diploma's, een huwelijksakte, bankpassen of doktersrecepten kunnen opslaan¹²⁴.

Gebruikers zullen zelf kunnen bepalen welke persoonsgegevens zij met onlinediensten willen delen. Publieke diensten en bepaalde particuliere diensten zullen verplicht worden om de Europese digitale identiteit te erkennen; vanwege de beveiligingskenmerken die deze identiteit zal krijgen, zal het echter voor alle **particuliere dienstverleners** interessant zijn om deze te erkennen voor diensten die sterke authenticatie vereisen, wat nieuwe zakelijke mogelijkheden zal bieden.

Voor dit initiatief bouwt de Commissie voort op het bestaande grensoverschrijdende rechtskader voor betrouwbare digitale identiteiten, het Europese initiatief voor elektronische identificatie en vertrouwensdiensten (**eIDAS-verordening**).

De Europese portemonnee voor digitale identiteit zal voortbouwen op nationale systemen die al bestaan in een aantal lidstaten. De portemonnee zal op nationaal niveau door de lidstaten aan hun burgers en inwoners worden verstrekt. Iedereen zal de mogelijkheid hebben om een Europese portemonnee voor digitale identiteit op zijn eigen smartphone of apparaat te downloaden, installeren en gebruiken.

Het voorstel voorziet in een hoog niveau van beveiliging. De Commissie zal standaarden, technische specificaties en operationele aspecten voorstellen en met de lidstaten overeenkomen om te garanderen dat de portemonnees voor digitale identiteit van de lidstaten aan de hoogste beveiligingseisen voldoen. De lidstaten zullen hun portemonnees certificeren om te garanderen dat zij

¹²² https://www.digitaleoverheid.nl/nieuws/ec-stelt-nieuwe-regels-datadeling-voor/?pk_campaign=nieuwsbrief-19-2020

¹²³ <https://www.nu.nl/tech/6137359/brussel-wil-digitale-id-kaart-waarmee-je-ook-kunt-inloggen-bij-grote-websites.html>

¹²⁴ https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

aan deze eisen voldoen. Persoonsgegevens zullen online alleen worden gedeeld als de burger in kwestie die informatie wil delen.

1.3 Afsprakenstelsels

1.3.1 Inleiding

Set van vastgelegde specificaties, regels en afspraken om samenwerking en zekerheid te garanderen op het gebied van technische functionaliteiten, beveiliging en privacy voor het uitwisselen van persoonlijke data. Afsprakenstelsels geven hiermee richting of stellen eisen aan PDM oplossingen. Eisen kunnen van technische aard zijn, bijvoorbeeld door het gebruik van bepaalde standaarden af te dwingen, maar kunnen bijvoorbeeld ook ingaan op het verdienmodel van een PDM-oplossing. Soms zijn de afsprakenstelsels sectorspecifiek zoals MedMij en soms generiek zoals Qiy.

iDEAL en GSM zijn aansprekende voorbeelden van afsprakenstelsels voor betalen en mobiel telefoneren. De consument kan hierdoor van aanbieder veranderen, zelf bepalen via welke bank hij/zij betaalt en met iedereen bellen.

Afsprakenstelsels komen tot stand door samenwerkingen van deelnemers die streven naar een gemeenschappelijk (eco)systeem met de andere partijen, in een voorspelbaar en samenhangend geheel. Afsprakenstelsels halen winst uit het standaardiseren van overeenkomsten, waardoor bilaterale contracten, die onderling kunnen verschillen, niet nodig zijn. Veel stelsels halen ook winst uit afspraken over (aansluiten bij) standaarden, of werken aan het neerzetten van standaarden en het concretiseren van afspraken die niet (volledig) door wet- en regelgeving afgedekt worden¹²⁵. De deelnemende partijen worden gestuurd door middel van juridisch afdwingbare en onafhankelijke specificaties, regels en afspraken die de werking van dit multi-party systeem regelt. Het is opgericht voor een bepaald doel en geeft deelnemers zekerheid dat iedereen de regels volgt die bij de rol horen, aldus Mettau.

Op het terrein van PDM zijn ook afsprakenstelsels in ontwikkeling. De kracht van deze afsprakenstelsels is dat de gegevens bij de bron blijven staan en dat 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. Een afsprakenstelsel voor PDM kan sectoronafhankelijk zijn. Dit is een **horizontaal afsprakenstelsel**. Een voorbeeld is 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.

In het rapport "Analyse Governance afsprakenstelsels voor Programma Regie Op Gegevens" van PBLQ uit 2019 worden afsprakenstelsels vergeleken en aanbevelingen gedaan richting de ontwikkeling van het programma ROG van de overheid¹²⁶.

1.3.2 MedMij

MedMij¹²⁷ is een Nederlandse standaard voor het veilig uitwisselen van gezondheidsgegevens tussen de burger en zorgprofessionals. Deze uitwisseling vindt plaats via een PGO, een persoonlijke gezondheidsomgeving. Vanuit een PGO met een MedMij-label kunnen medische gegevens worden verplaatst naar een andere PGO met MedMij-label. Of dit ook geldt voor gegevens die een persoon bijhoudt, dat is nog niet bekend. MedMij stelt eisen aan de PGO's en data aanbieders, deze eisen zijn opgenomen in het MedMij afsprakenstelsel. Organisaties die hier aantoonbaar aan voldoen mogen het MedMij-label gebruiken. De ontwikkeling van MedMij is mogelijk gemaakt met ondersteuning vanuit het ministerie van Volksgezondheid en Zorgverzekeraars Nederland. Tijdens de projectfase was de Patiëntenfederatie, in samenwerking met Nictiz, de trekker



¹²⁵ Mettau 2018: afsprakenstelsels in de praktijk

¹²⁶ Analyse governance afsprakenstelsels voor programma regie op gegevens (2019) via <https://rog.pleio.nl/>

¹²⁷ <https://www.medmij.nl/>

van de ontwikkeling van MedMij. Het afsprakenstelsel is nu in beheer genomen door Stichting MedMij. Naast de governance functies die MedMij heeft, onder andere incident management en operationeel beheer, stelt het eisen aan de functionaliteiten van PGO's in het afsprakenstelsel op het gebied van consent, opslag van gegevens, authenticatie, businessmodel en gegevensuitwisseling.

Status

- Dienstverleners in het zorgaanbiedersdomein: zorgaanbieders werken met dienstverleners in het zorgaanbiedersdomein. Zij zijn de leveranciers van informatiesystemen in een zorginstelling. Begin 2021 hebben 12 aanbieders het Medmij-label¹²⁸.
- Dienstverleners in het persoonlijke domein: zorggebruikers met een persoonlijke gezondheidsomgeving hebben te maken met een dienstverlener in het persoonlijke domein. Deze dienstverlener is veelal de leverancier van de PGO. Begin 2021 hebben 32 aanbieders het Medmij-label¹²⁹.
- Het is op dit moment nog niet mogelijk om aan je PGO de medische gegevens te koppelen. Medische gegevens zijn de gegevens die de zorgverlener of apotheek van jou bijhoudt in het medisch dossier. Dat is uiteindelijk wél de bedoeling¹³⁰.
- Op dit moment is het alléén nog mogelijk om eigen gezondheidsgegevens in te voeren in een PGO. Nog niet medische gegevens van bijvoorbeeld huisarts of ziekenhuis. Ook kunnen gegevens nog niet gedeeld worden.
- Het MedMij Afsprakenstelsel voorziet in het opvragen of delen van gegevens door de persoon zelf en kent (nog) geen mogelijkheden om (digitaal) toestemming te verkrijgen van een wettelijk vertegenwoordiger of de ouderlijke verantwoordelijke. Er worden daarom voorlopig alleen gegevens en/of gezondheidsinformatie van personen van 16 jaar en ouder verstrekt door of gedeeld met de zorgaanbieder.

De grootste belofte van PGO's aan patiënten heeft betrekking op de mate waarin patiënten zelf regie hebben over hun gegevens. Burgers worden datamakelaars op het gebied van de eigen gezondheid. Rond PGO's zijn nog wel een aantal aandachtspunten¹³¹:

- Het belangrijkste technische obstakel is het ontbreken van een goede wijze van identificatie en authenticatie.
- Wet- en regelgeving (AVG, Wabvpz, en WGBA) blijken een belangrijke stimulerende factor voor de opkomst van PGO's. PGO's vormen een belangrijke technische oplossing om te voldoen aan de verplichtingen met betrekking tot gegevensuitwisseling binnen de zorg, de online inzage en gespecificeerde toestemming. Minder aandacht bestaat voor gegevensuitwisseling die buiten de zorg plaatsheeft en ook door de komst van PGO's wordt gefaciliteerd.
- Duurzame verdienmodellen rond PGO's zijn onzeker.
- Wanneer mensen gegevens uit dossiers willen verwijderen die niet kloppen of als ze er niet in hun verdere zorgprocessen door 'achtervolgd' willen worden, bieden de onderzochte PGO's hierin een beperkte ondersteuning. Alleen gegevens die door henzelf zijn toegevoegd, bijvoorbeeld zelfmetingen, kunnen worden bewerkt of verborgen. Gegevens geregistreerd in de verschillende medische dossiers blijven een verantwoordelijkheid van de betreffende zorgverleners (zoals vastgelegd binnen de WGBA) en kunnen niet worden bewerkt of verborgen. Wijzigingen hierin zullen officieel bij de betreffende zorgverlener of zorginstantie moeten worden aangevraagd. De PGO's bieden nog geen officiële functionaliteit om deze wijzigingen aan te vragen.

¹²⁸ <https://www.medmij.nl/overzicht-medmij-deelnemers/>

¹²⁹ <https://www.medmij.nl/overzicht-medmij-deelnemers/>

¹³⁰ <https://www.pgo.nl/kies-een-pgo/>

¹³¹ <https://www.rathenau.nl/nl/digitale-samenleving/persoonlijke-gezondheidsomgevingen-data-beheer>

Kritische kanttekening bij digitale gezondheidsregie

Volgens het Rathenau instituut krijgen burgers met digitale gezondheidsregie meer verantwoordelijkheden, zowel tijdens ziekte als tijdens gezondheid. Het is onduidelijk of en hoe de grote diversiteit aan burgers, waaronder (chronische) patiënten, deze verantwoordelijkheden kunnen en willen oppakken. “Wanneer de mogelijkheden tot handelen op basis van terugkoppeling aan burgers steeds meer gebaseerd zijn op analyses (big data analyse, machine learning, voorspellende geneeskunde) van gekoppelde gegevens, kan het zijn dat burgers (on)bewust gestuurd worden in de keuzes die zij maken. Het is dus maar de vraag of burgers ‘eigen’ keuzes maken en daarmee zelfstandig regie voeren over hun gezondheid. Samengevat blijkt uit ons onderzoek dat de huidige opzet van online inzage en PGO's gevolgen kan hebben voor bredere maatschappelijke waarden, en dat daarmee de gevolgen voor de burgers om eigen regie over de gezondheid te voeren soms moeilijk zijn te overzien.”

Het Rathenau instituut ziet drie wijzen waarop autonomie ter discussie gesteld kan worden:

1. Geven digitale gezondheidsgegevens mij echt wel het inzicht dat nodig is om keuzes te maken over mijn eigen gezondheid?
2. Hoe vrijwillig is mijn deelname aan die digitale gezondheidsregie eigenlijk?
3. Welke keuzes maak ik nog zelf? Waar doen apps dat bijvoorbeeld voor mij?

Niezen, M.G.H., & P. Verhoef (2018). Digitale gezondheidsregie: meer gegevens, meer grip? Den Haag: Rathenau Instituut.

Het Rathenau Instituut stelt voor¹³², dat de partijen die betrokken zijn bij de inrichting van het systeem voor digitaal inzien en delen van gezondheidsgegevens, goed nadenken over wat dit betekent voor onze publieke waarden. Publieke waarden, die nu nog niet voldoende zijn meegenomen in het ontwerpproces, moeten goed geïmplementeerd kunnen worden.

Het gaat dan bijvoorbeeld om:

- autonomie
 - kan de burger écht de keuze maken en overzien?
- rechtvaardigheid
 - is iedereen in staat gezondheid digitaal te beheren of krijg je een tweedeling in mensen die het wel en niet kunnen?
- solidariteit
 - wordt van iedereen verwacht actie te ondernemen op basis van de gegevens?

Het Rathenau Instituut rapporteerde in 2019¹³³ over vier parallel opkomende digitale diensten

1. online portalen in de geestelijke gezondheidszorg
2. leefstijl- en medische apps (health apps)
3. persoonlijke gezondheidsomgevingen (PGO's, persoonlijke datakluisjes)
4. burgerplatforms (collectieve databases)

Volgens het Rathenau Instituut krijgen burgers niet alleen zelf meer regie over gezondheidsgegevens, maar geven deze regie juist ook af. Vooral de monopolisering van gezondheidsdata door grote bedrijven is een punt van zorg, waardoor de machtsverhouding tussen bedrijven en burgers nog schever komt te liggen dan hij al is. Maar ook de kwaliteit van de gegevens die worden gedeeld en gebruikt en de transparantie van de analyses is minder te controleren. Dit roept vragen op over juistheid van adviezen en over wie aansprakelijk is als het mis gaat.

¹³² Digitale gezondheidsregie Meer gegevens, meer grip? <https://www.rathenau.nl/nl/maakbare-levens/digitale-gezondheidsregie>

¹³³ Niezen, M.G.H., Edelenbosch, R., Van Bodegom, L. & Verhoef, P. (2019). Gezondheid centraal – Zorgvuldig data delen in de digitale samenleving. Den Haag: Rathenau Instituut

Het Rathenau Instituut pleit voor een code of conduct onder ontwikkelaars en aanbieders van de diensten, ook bij toepassing van kunstmatige intelligentie, zorgt bijvoorbeeld voor een bredere verantwoordelijkheid en bewustzijn dan databeveiliging en privacy alleen. Hierbij refereert het Rathenau Instituut aan de Artificial Intelligence Impact Assessment van TNO/ECP¹³⁴.

Voorts zou volgens het Rathenau Instituut de regie van de overheid op digitalisering in de zorg zou niet meer gericht moeten zijn op het stimuleren van zoveel mogelijk delen van data, maar op het onderkennen van de goede initiatieven, die juist in een zorgcontext ontwikkeld worden. Organiseer een platform of ander mechanisme dat best practices in beeld brengt van zowel de technologische oplossing als de implementatie en evaluatie hiervan in de praktijk, luidt het advies.

1.3.3 Qiy

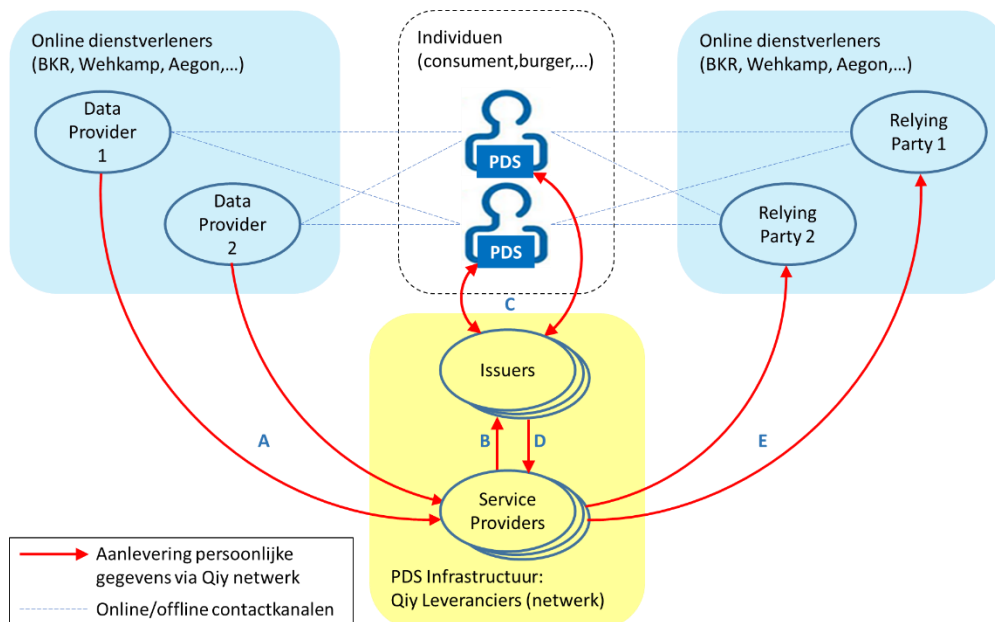
De Stichting Qiy werkt sinds 2007 aan het Qiy Scheme. Dit afsprakenstelsel richt zich op alle individuen, organisaties en apparaten die persoonsgegevens verwerken. In tegenstelling tot MedMij beperkt Qiy zich niet tot een specifieke sector.

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



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-3 maakt de rol die de verschillende partijen spelen binnen het Qiy Network inzichtelijk.



Figuur-3: Uitwisseling van persoonsgegevens via het Qiy Network

¹³⁴ Zie onder meer: <https://airecht.nl/blog/2018/artificial-intelligence-impact-assessment>

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 (Serviceproviders). 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.

1.3.4 iSHARE

Het afsprakenstelsel iSHARE¹³⁵ is ontwikkeld in de sector logistiek in 2017. Het stelsel richt zich met name op gegevensuitwisseling tussen organisaties. Partijen hanteren dezelfde manier van identificatie, authenticatie en autorisatie om elkaar toegang te verstrekken tot data¹³⁶. De afspraken hierover zijn erg gedetailleerd en zorgen ervoor dat zelfs partijen die elkaar niet kennen, gegevens kunnen uitwisselen op basis van 'gedelegeerde autorisaties'. Daarnaast stelt het stelsel eisen aan consent: de eigenaar van gegevens moet altijd de toegang tot data kunnen wijzigen. Over gegevensuitwisseling zelf doet iSHARE geen uitspraken.



Het afsprakenstelsel wordt beheerd door de Stichting iSHARE. De stichting ziet toe op naleving van afspraken, beheert processen voor toetreding en faciliteert verbeteringen van het stelsel. De partijen die deelnemer zijn aan het stelsel worden vertegenwoordigd in een Council of Participants. De Change Advisory Board adviseert over doorontwikkeling van het stelsel. Het betreft hier niet direct uitwisseling van persoonsgegevens, echter is iSHARE wel interessant in deze context vanwege de 'gedelegeerde autorisaties' die elders ook toegepast kan worden. Een gedelegeerde autorisatie dient als bewijs dat een onbekende partij A direct of indirect opereert in naam van een bekende partij B. Deze autorisatie is gebaseerd op de delegatie die is uitgegeven door partij B. Op basis daarvan kan de partij C besluiten om wel of geen gegevens te delen met partij A¹³⁷. iSHARE timmert ook qua toepassing flink aan de weg¹³⁸.

1.4 Technologie en standaarden

Technologie

Technische concepten en protocollen maken de gegevensuitwisseling binnen een PDM-oplossing mogelijk. De technologieën zijn op het eerste oog niet zichtbaar voor de gebruiker, maar zijn wel essentieel voor het functioneren van PDM-Diensten. Dergelijke technologieën kunnen tevens landen in referentie-architecturen¹³⁹.

- Een concept is een abstract idee of plan van hoe bepaalde technologie kan werken om een proces te laten verlopen. Technologische concepten kunnen doorgroeien tot protocollen, standaarden of worden toegepast binnen een PDM-operator. Voorbeelden zijn blockchain en zero knowledge proofs.
- Een protocol beschrijft hoe bepaalde processen zoals communicatie tussen een data aanbieder en operator verlopen en zijn vaak implementaties van concepten. Protocollen zijn nog niet officieel erkend als standaard. Een voorbeeld van een protocol is Idemix, wat gebruik maakt van zero knowledge proofs en wordt toegepast in IRMA voor gegevensuitwisseling.

Standaarden

Dit zijn afspraken over informatie of over een proces, dit kan zowel op het niveau van semantische als technische standaarden. Veelal vastgelegd in documenten met erkende status. Standaarden worden onderhouden vanuit standaardisatie organisaties zoals het NEN en aanbevolen of verplicht gesteld¹⁴⁰

¹³⁵ <https://www.ishareworks.org/>

¹³⁶ <https://ishareworks.atlassian.net/wiki/spaces/IS/overview>

¹³⁷ <https://ishareworks.atlassian.net/wiki/spaces/IS/pages/75399169/Enable+data+exchange+based+on+delegations+-+even+between+unknown+parties>

¹³⁸ <https://www.logistiek.nl/search?q=iShare>

¹³⁹ Voorbeelden van referentie-architecturen zijn NORA en GEMMA, maar ook andere oplossingen zoals Common Ground, Blauwe Knop of commerciële oplossingen gebruiken een referentie-architectuur.

¹⁴⁰ Op basis van 'Pas toe of leg uit'-beleid, zie <https://forumstandaardisatie.nl/node/229>

door bijvoorbeeld Bureau Forum Standaardisatie¹⁴¹. OAuth 2.0, OpenID Connect, SAML, UMA, zijn standaarden bij het verkrijgen van toegang tot diensten waarbij ROG een rol speelt.

De concepten, protocollen en standaarden voor gegevensuitwisseling die hierna worden beschreven zijn gericht op de toepassing van technologie. Een eindgebruiker kan deze niet “zomaar” gebruiken, maar ze maken deel uit van oplossingen die de eindgebruiker wel ziet/ervaart.

Standaarden van de W3C voegen veel waarde toe; denk aan Decentralized Identifiers (DID) en Verifiable Credentials (VC).

1.4.1 Self Sovereign Identity (SSI)

SSI is een digitale identiteit waarbij de gebruiker en diens privacy centraal staat¹⁴². De gebruiker kan met SSI zelf zijn identiteit bewaren in een soort digitale portefeuille. Het gaat hierbij om gegevens over iemands identiteit, maar ook bijvoorbeeld over een diploma of een registratie bij de Kamer van Koophandel. Dit worden ook wel ‘verklaringen’ genoemd, die zijn gekoppeld aan een specifieke persoon, via een digitale identiteit. Deze verklaringen worden eenmalig digitaal ondertekend door bijvoorbeeld de overheid, banken, werkgevers, verzekeraars. Met SSI beschikt een persoon dus over eigen digitale verklaringen, en over zijn/haar digitale identiteit, in plaats van identiteitsproviders. SSI maakt het ook mogelijk dat een persoon, op een veilige manier, alleen gegevens deelt die voor een bepaalde (rechts)handeling nodig zijn, wat de privacy vergroot. IRMA is een voorbeeld van een SSI-oplossing. Er zijn meer SSI-oplossingen dan IRMA, bijvoorbeeld Sovrin¹⁴³ en Solid¹⁴⁴. De EU ontwikkelt een eIDAS compatibel European Self-Sovereign Identity Framework (ESSIF)¹⁴⁵. ESSIF maakt gebruik van gedecentraliseerde identifiërs (DIDs) en de European Blockchain Services Infrastructure (EBSI).

1.4.2 Sovrin

Sovrin is een private samenwerking in een non-profit organisatie. Sovrin wil identity management regelen via een gedistribueerd grootboek (distributed ledger, oftewel blockchain technologie). Het gedistribueerde grootboek moet het makkelijker maken om PDM-oplossingen aan te bieden op een decentrale manier. Het initiatief zorgt ervoor dat geanonimiseerd delen van attributen mogelijk wordt, met consent van degene over wie de data gaat.



Bij toestemming geeft de eigenaar de dienstverlener toegang tot identiteitsgegevens. 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. In 2018 verscheen een evaluatie van Sovrin¹⁴⁶.

1.4.3 Zero knowledge proof

Een zero knowledge proof¹⁴⁷ is een wiskundige manier om te bewijzen dat je kennis hebt van een zeker gegeven, zonder dat gegeven daadwerkelijk te laten zien. Dit gegeven kan ook een persoonlijk gegeven zijn. Een voorbeeld is het bewijzen dat een persoon ouder is dan 18, door simpelweg ‘ja, de persoon is 18+’ door te geven. In plaats van de specifieke geboortedatum. Dit draagt bij aan

¹⁴¹ Binnen het overheidsdomein speelt het Forum Standaardisatie een belangrijke rol bij het tot stand komen van open standaarden. Dit resulteert in verplichte en aanbevolen standaarden.¹⁴¹ Forum Standaardisatie is een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap. De leden worden op persoonlijke titel benoemd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

¹⁴² Basic building blocks of SSI. <https://livebook.manning.com/book/self-sovereign-identity/chapter-2/v-1/89>

¹⁴³ <https://sovrin.org/>

¹⁴⁴ <https://inrupt.com/vision>

¹⁴⁵ <https://ssimeetup.org/understanding-european-self-sovereign-identity-framework-essif-daniel-du-seuil-carlos-pastor-webinar-32/>

¹⁴⁶ <https://dutchblockchaincoalition.org/uploads/pdf/Blockchain-Sovrin-rapport.pdf>

¹⁴⁷ https://en.wikipedia.org/wiki/Zero-knowledge_proof

dataminimalisatie en voegt waarde toe vanuit privacy perspectief. Zero knowledge proofs worden bijvoorbeeld gebruikt in Idemix, het protocol dat bijvoorbeeld gebruikt wordt in IRMA. 'Zero knowledge proof' is een techniek die in de identity wallet¹⁴⁸ van de Rabobank wordt toegepast om bijvoorbeeld een inkomensstoets van een woningcorporatie te beantwoorden, zonder het inkomen op zich prijs te geven.

Proef inkomensstoets¹⁴⁹

Door het in 2016 geïntroduceerde beleid rondom passend toewijzen zijn woningcorporaties verplicht strikte regels (onder andere inkomenseisen) na te leven bij de toewijzing van sociale huurwoningen. Woningcorporaties voeren bij alle nieuwe huurders een inkomensstoets uit op basis van een maximaal inkomen. Door zowel kandidaat huurders als woningcorporaties worden pijnpunten ervaren bij de uitvoering van de inkomensstoets zoals: complexiteit, fraude en privacy risico's. Uitvoering van de toets kost voor woningcorporaties in Nederland naar schatting jaarlijks €17 miljoen.

Samen met Rabobank heeft Deloitte een ZKP & ID Wallet oplossing ontwikkeld. Deze oplossing geeft de kandidaat huurder meer regie en controle over zijn gegevens. Ook wordt hierdoor de inkomensstoets (sterk) vereenvoudigd en wordt de hoeveelheid data geminimaliseerd.

Uit de gebruikerstoetsen uitgevoerd met kandidaat huurders blijkt dat 95%de ZKP & ID Wallet oplossing als een verbetering ziet ten opzichte van het huidige proces. Uit de gevoerde gesprekken met woningcorporaties blijkt zowel een "problem fit" als een "solution fit".

Zero-knowledge proof

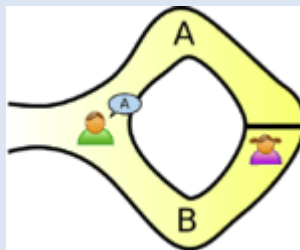
Een bekend voorbeeld van een zero-knowledge proof is de grot van Ali Baba. In deze ronde grot zit een deur. Deze deur gaat alleen open met het geheime wachtwoord. Nu weet Ines dit geheime wachtwoord, maar ze wil deze niet aan Bob vertellen. Toch wil ze aan Bob bewijzen dat ze het wachtwoord weet.

Bob en Ines volgen daarom het volgende zero-knowledge protocol:

Ines gaat, zonder dat Bob het ziet, linksom (A) of rechtsom (B) de ronde grot in.

Bob komt bij het begin van de ronde grot staan en roept naar Ines vanuit welke kant ze de grot uit moet komen (A of B).

Ines komt, met of zonder gebruik van de deur en het geheime wachtwoord, aan de genoemde kant de grot uit lopen.



Ines en Bob herhalen dit protocol een aantal keer, totdat Ines Bob heeft overtuigd dat ze inderdaad het wachtwoord weet. Bob komt nooit het wachtwoord te weten en zelfs niet de kant die Ines kiest om de ronde grot in te gaan. Toch kan hij na X keer het protocol te doen, met een goede kans zeggen dat Ines het wachtwoord weet.

Stel dat Ines het wachtwoord niet wist, dan had ze bij de 1ste ronde van het protocol 50% kans om de goede kant te gokken. Bij de 2de ronde heeft ze weer 50% kans het goed te gokken, enzovoort. Bij de twee rondes heeft ze dus 25% kans om het beide keren goed te hebben. Uiteindelijk zou ze ontzettend veel geluk moeten hebben om het een X-aantal keer goed te gokken.

¹⁴⁸ Rabobank ontwikkelde een Self-Sovereign Identity wallet gericht op HR: <https://tykn.tech/self-sovereign-identity-rabobank/>

¹⁴⁹ Zero Knowledge Proof & ID Wallet Regie Op Gegevens, december 2019

Pilot Digitale Inkomenstoets Woningcorporaties¹⁵⁰

Logius, het Ministerie van BZK, de Belastingdienst en verschillende woningcorporaties starten begin zomer 2021 met de pilot 'Digitale Inkomenstoets Woningcorporaties'. De pilot toetst of woningzoekenden hun inkomensgegevens snel en veilig kunnen delen via MijnOverheid. De woningcorporatie gebruikt de gegevens om te bepalen of de woningzoekende in aanmerking komt voor de woning. De woningzoekende moet vervolgens uit verschillende bronnen informatie ophalen en aanleveren. Dit is vaak een ingewikkeld en foutgevoelig proces. Tijdens de pilot kunnen woningzoekenden de benodigde gegevens eenvoudig, veilig en snel digitaal aan leveren via MijnOverheid.

1.4.4 Idemix

Het Identity Mixer (Idemix) protocol van IBM maakt het mogelijk voor de IRMA-app om attributen die ondertekend zijn door de uitgever te ontvangen en deze vervolgens, deels, te delen met een controleur. Een specifieke privacy-functionaliteit van Idemix is het blinderen van bepaalde attributen in een credential zonder daarbij de digitale handtekening van de uitgever open te breken. Hierdoor kan de gebruiker alleen de attributen delen die de controleur nodig heeft voor de dienstverlening aan de gebruiker. Dergelijke selectieve onthulling functionaliteit is nodig om te voorzien in de AVG-eis van dataminimalisatie.

Het Idemix-protocol is een technologie voor attribuut-gebaseerde identiteitsverklaringen. Binnen het Idemix-protocol worden attributen vanuit een uitgever gecombineerd in een credential. Zo'n credential bevat de naam en publieke sleutel (public key) van de uitgever, het pseudoniem van de gebruiker, een vervaldatum, en een aantal attributen. Het geheel is digitaal ondertekend door de uitgever van het credential en wordt verstuurd naar de gebruiker. Figuur-4 toont een algemeen credential en een voorbeeld DigiD credential.

Credential		DigiD Credential	
Issuer		DigiD	
Issuer public key		DigiD public key	ed9a9fc223f9...
 Pseudonym		 Pseudonym	J97S6K1QIW... 
Attribute1		Voornaam	Mohammed 
Attribute2		Achternaam	Janssen 
Attribute3		Geboorte datum	01-01-2012 
 Experience Date			 
		 Experience Date	04-03-2025 

Figuur-4: Grafische weergave van een credential¹⁵¹ en een voorbeeld van een DigiD credential.

De vervaldatum van het credential wordt gebruikt om te bepalen of de attributen nog actueel zijn. De exacte attributen in een credential zijn afhankelijk van de uitgever.

Het pseudoniem wordt tussen de uitgever en de gebruiker afgesproken en wordt gebruikt om een relatie tussen de uitgever en de gebruiker tot stand te brengen en te bevestigen. De geheime sleutel die bij het pseudoniem hoort is echter alleen bekend bij gebruiker. Met de geheime sleutel kan de gebruiker bewijzen, aan de controleur, dat hij degene is die de attributen rechtmatig verkregen heeft van de uitgever. Dit doet hij met een zero-knowledge proof, zonder dat hij daarvoor zijn sleutel moet laten zien.

Het hele credential wordt ondertekend door de uitgever met zijn geheime sleutel. De controleur kan deze handtekening controleren met de bijbehorende publieke sleutel, die toegevoegd is aan het

¹⁵⁰ <https://www.aedes.nl/artikelen/bedrijfsvoering/digitalisering-en-informatievoorziening/proef-digitale-inkomenstoets-woningcorporaties.html>

¹⁵¹ Specification of the Identity Mixer Cryptographic Library (Revised version 2.3.0)

credential maar ook via de uitgever opgehaald kan worden door iedereen. De handtekening bestaat uit blokken en daardoor heeft elk attribuut zijn eigen blok van de handtekening. Dit maakt het mogelijk om bepaalde attributen uit een credential te delen met een controleur, terwijl andere verborgen blijven voor de controleur. Wederom wordt het bewijs van het bezit van bepaalde attributen, in het Idemix-protocol, met een zero-knowledge proof bewezen aan de controleur.

Met het Idemix-protocol is het mogelijk om simpele zero-knowledge bewijzen te doen, waarmee je de exacte waarde van een attribuut weggeeft, zoals: "Ik heb een DigiD credential waarop staat dat ik inderdaad "Janssen" als achternaam heb". Het is ook mogelijk om een afgeleid attribuut te bewijzen, zonder de exacte waarde weer te geven, zoals: "Ik heb een iDIN credential waarop staat dat ik ouder ben dan 18". Ook complexere afgeleide attributen zijn mogelijk, waarin je bewijst dat je een attribuut binnen een subset valt: "Ik heb een DigiD bewijs waarin mijn burgerlijke staat nooit getrouwd, getrouwd of geregistreerd partnerschap is", zonder dat de controleur erachter komt welke van de 3 genoemde burgerlijke staten de gebruiker heeft.

Voor meer technische en cryptografische details of het Idemix-protocol wordt verwezen naar IBM's Specification of the Identity Mixer Cryptographic Library (Revised version 2.3.0)¹⁵².

1.4.5 X-tee

X-tee¹⁵³ is ontwikkeld in het e-Estonia project. X-tee, de gegevensuitwisselingslaag voor informatiesystemen, is een technologische en organisatorische omgeving die een veilige op internet gebaseerde gegevensuitwisseling tussen informatiesystemen mogelijk maakt.

Door het grote aantal systemen dat zich bij X-tee heeft aangesloten, kunnen alle leden van X-tee de diensten en gegevens van andere leden gebruiken om hun eigen bedrijfsprocessen te verbeteren. Een voorbeeld is een oplossing van de politie voor het controleren van rijbewijzen. Een bestuurder hoeft niet langer een fysiek rijbewijs bij zich te hebben, aangezien een politieagent via X-tee een onderzoek kan doen in de database van de Republiek Estland Road Administration.

In X-tee gaan de gegevens niet via de gebruiker, maar direct van de partij die de gegevens bezit naar de partij die de gegevens nodig heeft. De gebruiker heeft met X-tee wel beter inzicht in wat met persoonsgegevens gebeurt en bij welke partijen deze gebruikt worden, omdat alle gegevensuitwisselingen in X-tee automatisch gelogd worden. Hierdoor kan wetgeving ook beter gehandhaafd worden.

De absolute meerderheid van de X-tee-gebruikers zijn passieve gebruikers. De belangrijkste gebruikers van X-tee zijn datadienstverleners. Ze maken hun gegevens toegankelijk voor andere leden of verzamelen nieuwe gegevens van anderen. Alle staatsregisters zijn datadienstverleners.

Via de X-tee is het mogelijk om gelijktijdig gegevens van anderen te delen en op te vragen. Een organisatie kan bijvoorbeeld gegevens opvragen uit databases A en B, terwijl ze tegelijkertijd gegevens van een burger verzamelt en deze vastlegt in haar eigen database, C. Eenmaal geregistreerd, kan die informatie in Database C worden gedeeld met andere X-tee-leden, inclusief de instellingen die verantwoordelijk zijn voor databases A en B. Last but not least wordt het mogelijk om op basis van de persoonlijke code van die burger een complex gelijktijdig verzoek in te dienen tegen de databases A, B en C en om een gezamenlijke antwoord met gegevens van alle drie.

Gebruikers kunnen tegelijkertijd X-tee-gegevens lezen en bijwerken. De X-tee kan ook complexe zoekopdrachten ondersteunen waarbij bijvoorbeeld 37 gerelateerde databases moeten worden doorzocht.

Een geheel nieuwe klasse van actoren zijn Trust Service Providers (diegenen die diensten verlenen zoals tijdstempels, certificering enz.). Trust Service Providers verstrekken geen gegevens via de X-

¹⁵² <https://www.semanticscholar.org/paper/Specification-of-the-Identity-Mixer-Cryptographic-2-Team-Switzerland/bf6507a279161d15478ec04aab0a3d9c2adb5f7a>

¹⁵³ <https://www.ria.ee/en/state-information-system/x-tee/introduction-x-tee.html>

tee. In plaats daarvan bieden ze een standaard cryptografische service die de betrouwbaarheid van de gegevens die door iemand anders worden verstrekt, verhoogt.

1.4.6 NLX

NLX¹⁵⁴ is een Nederlands overheidsinitiatief en primair bedoeld voor gegevensuitwisseling tussen systemen van organisaties, in het bijzonder de landelijke en lokale gegevensdiensten. De gebruiker krijgt inzicht in wat er met persoonsgegevens gebeurt en welke partijen het gebruiken. Ook maakt NLX geen kopieën van gegevens, wat de kans verkleint dat gegevens bij verkeerde personen of op onjuiste plekken belanden.

NLX maakt deel uit van Common Ground (dat elders in dit rapport wordt besproken), een bredere beweging die voortkomt uit initiatieven van de Vereniging van Nederlandse Gemeenten (VNG). De X-Road van Estland heeft mede als inspiratiebron gediend voor NLX. Deze gemeenschappelijke infrastructuur van de Estse overheid is al zo'n tien jaar succesvol en is inmiddels ook geïmplementeerd in andere landen, waaronder Namibië en Finland.

NLX is een open source systeem om peer-to-peer gegevens uit te wisselen op basis van federatieve authenticatie, beveiligde connectiviteit en protocollen die faciliteren in een grootschalig API-landschap met meerdere organisaties. Iedereen moet in staat zijn om eenvoudig API's van andere organisaties te gebruiken net alsof het eigen API's zijn.

NLX voorziet in een laagdrempelige omgeving voor ontwikkelaars zodat zij gestandaardiseerde gegevensbronnen van andere organisaties kunnen gebruiken. NLX ondersteunt daarbij API's op basis van verschillende technieken zoals REST/JSON en SOAP/XML. Ondersteuning voor HTTP/2 (gRPC) is in ontwikkeling.

NLX richt zich op de 'logistiek' van het bericht, niet op de inhoud. Daardoor kan iedere organisatie die NLX gebruikt, zich beperken tot uitwerking van de inhoud van de bericht uitwisseling.

1.4.7 NUTS

NUTS¹⁵⁵ is een Nederlands initiatief van softwareleveranciers – onder het motto “veilig datadelen, wel zo normaal” - dat zich richt op de zorgsector. De patiënt of de gemachtigde mantelzorger, staat hier centraal en geeft toestemming om data te delen en krijgt inzicht in waar haar data is gedeeld. Patiëntenorganisaties, medische professionals en andere belanghebbende kunnen data makkelijker en direct met elkaar uitwisselen.



NUTS gaat uit van 8 principes die zijn vastgelegd in een manifest¹⁵⁶. NUTS is nog in de concept fase, in hun pilots werken ze toe naar een open source protocol om data uit te wisselen via een peer-to-pee netwerk.

Zowel de patiënt als de zorgmedewerker zal niet direct met NUTS werken. De patiënt krijgt een Persoonlijke gezondheidsomgeving (PGO). Ook de zorgmedewerker blijft gewoon zelf een softwareleverancier kiezen voor de procesondersteuning. Op de achtergrond zullen gegevens tussen deze systemen worden uitgewisseld met behulp van NUTS.

1.4.8 JLINC

JLINC¹⁵⁷ is een Amerikaans initiatief dat een protocol¹⁵⁸ biedt voor het delen van gegevens, beschermd door een overeenkomst over de voorwaarden waaronder de gegevens



¹⁵⁴ <https://nlx.io/>

¹⁵⁵ <https://nuts.nl>

¹⁵⁶ <https://nuts.nl/manifest/>

¹⁵⁷ <https://www.jlinc.com/technology>

¹⁵⁸ <https://protocol.jlinc.org/>

worden gedeeld. Het begint met het bestaan van een of meer standaardovereenkomsten voor het delen van informatie (Standard Information Sharing Agreements = SISA's) voor een bepaalde bedrijfstak of soort activiteit. Het idee is dat deze samen met brancheorganisaties worden uitgewerkt door groepen van burgervertegenwoordigers. JLINC Labs heeft een basis-SISA gemaakt om het proces te starten. De SISA wordt gekozen en cryptografisch ondertekend door de initiërende partij (een Rechtenhouder of Gegevensbewaarder) en aangeboden aan de ontvangende partij. De ontvangende partij, indien zij de SISA herkent en accepteert, ondertekent deze en geeft deze terug aan de initiatief nemende partij. Beide partijen bewaren een kopie van de ondertekende SISA en kunnen deze indienen bij een grootboek¹⁵⁹ naar keuze. Zodra de SISA is voltooid, kunnen de partijen het JLINC-protocol gebruiken om informatie uit te wisselen, vergezeld van een hash van de SISA, wat aangeeft dat de uitwisseling geacht wordt plaats te vinden in de context van de SISA. Loggingen van deze uitwisselingen (SISA-evenementen) worden ook door beide partijen bewaard en kunnen ook aan een grootboek worden voorgelegd.

1.4.9 Open Authorization (OAuth)

Open Authorization 2.0 (OAuth 2.0¹⁶⁰) is een open standaard. Gebruikers kunnen hiermee een programma of website toegang geven tot hun privégegevens, die opgeslagen zijn op een andere website, zonder hun gebruikersnaam en wachtwoord uit handen te geven. OAuth maakt gebruik van tokens, waardoor vertrouwelijke gegevens als een gebruikersnaam of wachtwoord niet afgegeven hoeven te worden. Elk token geeft slechts toegang tot specifieke gegevens van één website voor een bepaalde duur. Zo kan ingesteld worden dat een bepaald programma slechts een jaar toegang heeft tot de gegevens. Hierna kan eventueel opnieuw toegang worden gevraagd. OAuth 2.0 is populair en wordt gebruikt om in te loggen bij Facebook, Netflix, Paypal, Twitter, Microsoft, Instagram, LinkedIn en andere internetreuzen.

1.4.10 User Management Access (UMA)

User Management Access (UMA¹⁶¹) is een standaard waarmee gebruikers toegang tot bepaalde gegevens kunnen geven aan andere gebruikers. UMA is een OAuth gebaseerde standaard die is ontworpen om een webgebruiker een uniform controlepunt te geven om te autoriseren wie en wat toegang kan krijgen tot online persoonlijke gegevens (zoals identiteitskenmerken), inhoud (zoals foto's) en services (zoals het bekijken en maken van statusupdates), ongeacht waar al die zaken op internet te vinden zijn.

1.4.11 OpenID, SAML

Zowel OpenID Connect¹⁶² en SAML¹⁶³ zijn standaarden waarbij gebruikers federatief kunnen inloggen. Wanneer men federatief authenticiseert wordt aan een vertrouwde partij gevraagd om de authenticatie af te handelen. Deze vertrouwde partij geeft vervolgens terug of er juist geauthentiseerd is, en geeft een aantal gevraagde attributen terug zodat eventueel ook geautoriseerd kan worden.

OpenID Connect

OpenID Connect (OIDC) bouwt, net als UMA, verder op de OAuth standaard. OpenID Connect moet volgens de overheid worden toegepast bij het beschikbaar stellen van federatieve authenticatiediensten, waarbij sprake is van mobiele toepassingen¹⁶⁴. OIDC is een open en gedistribueerde manier om authenticatiediensten naar keuze te kunnen hergebruiken bij meerdere ((semi-)overheids) dienstverleners, bij gebruik vanuit onder andere webapplicaties en mobiele toepassingen. OIDC geeft apparaten en programma's de mogelijkheid om de identiteit van een eindgebruiker te controleren gebaseerd op verschillende authenticatieservices (zoals DigiD), waarbij profielinformatie van de eindgebruiker volgens een gestandaardiseerde wijze beschikbaar wordt

¹⁵⁹ een wereldwijd grootboek met alleen aanhangsels dat wordt beheerd door een onafhankelijke leverancier van inloggegevens en transacties.

¹⁶⁰ <https://oauth.net/2/>

¹⁶¹ <https://kantarainitiative.org/confluence/display/uma/UMA+FAQ>

¹⁶² <https://openid.net/connect/>

¹⁶³ <http://saml.xml.org/protocols>

¹⁶⁴ <https://www.forumstandaardisatie.nl/open-standaarden/oidc>

gesteld aan de daarvoor geautoriseerde apparaten en programma's. De gebruiker kan zelf een keuze maken voor een authenticatievoorziening en gebruiker hoeft niet steeds opnieuw in te loggen.

De OpenID foundation¹⁶⁵ is een non-profit internationale standaardisatie-organisatie van individuen en bedrijven die zich inzetten voor het mogelijk maken, promoten en beschermen van OpenID-technologieën.

Security Assertion Markup Language (SAML)

SAML wordt onder andere gebruikt in bijvoorbeeld SURFconext, iDIN, DigiD Machtigen, eHerkenning en Idensys. SAML moet volgens de overheid worden toegepast op de uitwisseling van authenticatie- en autorisatiegegevens om gebruikers na eenmalig inloggen toegang te geven tot meerdere diensten¹⁶⁶.



SAML standaardiseert het berichtenverkeer tussen een Identity Provider (IdP) en een Service Provider (SP). Een IdP is een partij die verantwoordelijk is voor authenticatie van gebruikers en die identiteitsattributen van gebruikers kan verschaffen. Een SP is een dienstverlener die een elektronische dienst aanbiedt aan de gebruikers. Een constellatie van bij elkaar horende IdPs en SPs wordt een (SAML-) federatie genoemd.

De SAML-specificatie schrijft met name voor:

- het XML gebaseerde berichtformaat voor de identiteitsattributen (assertions);
- welke protocollen er gebruikt worden (welke berichten, in welke volgorde, tussen welke partijen worden uitgewisseld);
- en hoe deze berichten getransporteerd worden (de zogenaamde binding).

SAML wordt ingezet bij webgebaseerde diensten. Identiteiten kunnen, dankzij SAML, herbruikbaar gemaakt worden doordat de IdP en de SP niet dezelfde partij hoeven te zijn en zodat meerdere SP's van één en dezelfde IdP gebruik kunnen maken. Daarbij wordt SAML vaak ook ingezet om Single Sign On voor web-diensten te realiseren. Een gebruiker hoeft dan eenmalig in te loggen om van meerdere diensten binnen de federatie gebruik te kunnen maken.

1.4.12 openBadges

NLXOpenbadges¹⁶⁷ is een manier om diploma's, certificaten en andere bekwaamheden gevalideerd te kunnen delen (Discover Open Badges). Een badge is een digitaal bewijsstuk waarmee een student aantoont dat hij of zij bepaalde vaardigheden of kennis beheerst. Openbadges is een open source technologische standaard (Open Badges v2.0 IMS Final Release¹⁶⁸). De technologie kan met verschillende operators gebruikt worden, waaronder Badgr, Badgewell en My Open Badge. Een groot aantal instellingen - waar je Openbadges kunt ophalen - is aangesloten als data aanbieder. Je kunt de badges vervolgens met een open badges operator, delen op social media, op websites en via e-mail. EduBadges¹⁶⁹ is in Nederland een voorbeeld van een implementatie van OpenBadges. Een edubadge helpt studenten om kennis en vaardigheden die zij beheersen, zichtbaar en 'meeneembaar' te maken. Dit kan het overstappen van opleiding naar werk vergemakkelijken en ook het switchen tussen opleidingen.

1.4.13 PKIoverheid

PKIoverheid is de Public Key Infrastructure (PKI) van de Nederlandse overheid. Net als elke andere PKI is het een afsprakenstelsel om digitale certificaten uit te geven en te beheren. Public Key Infrastructure (PKI) voor de overheid, kortweg PKIoverheid of PKIo, maakt betrouwbare digitale communicatie mogelijk met, door en binnen de Nederlandse overheid. PKIoverheid is een infrastructuur, gebaseerd op digitale certificaten. Publieke en private Trust Service Providers (TSP)

¹⁶⁵ <https://openid.net/foundation/>

¹⁶⁶ <https://www.forumstandaardisatie.nl/open-standaarden/saml>

¹⁶⁷ <https://openbadges.org/>

¹⁶⁸ <https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/impl/index.html>

¹⁶⁹ <https://www.surf.nl/edubadges-nationale-aanpak-voor-inzet-van-badges>

binnen het PKI-overheid stelsel realiseren een betrouwbare uitgifte van PKI-certificaten. Deze uitgifte gebeurt onder strikte voorwaarden en toezicht van de Policy Authority PKI-overheid, belegd bij Logius. PKI-certificaten kennen verschillende toepassingen: authenticatie van personen, website beveiliging, veilige versleutelde berichtenuitwisseling tussen servers en digitaal ondertekenen of waarmerken¹⁷⁰. Dit soort digitale certificaten -raken aan ROG omdat ze zorgen dat organisaties zich naar elkaar kunnen authenticeren bij het ophalen van gegevens.¹⁷¹

1.4.14 OpenAPI Specification (OAS)

OAS moet worden toegepast op het beschrijven/specificeren van een REST API. Verplicht in het werkgebied van de Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

1.4.15 REST-API Design Rules

De standaard REST-API Design Rules moet worden toegepast bij het aanbieden van REST API's ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit. De standaard REST-API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt. Dit maakt het voor ontwikkelaars gemakkelijker om betrouwbare applicaties met te ontwikkelen met API's van de overheid.

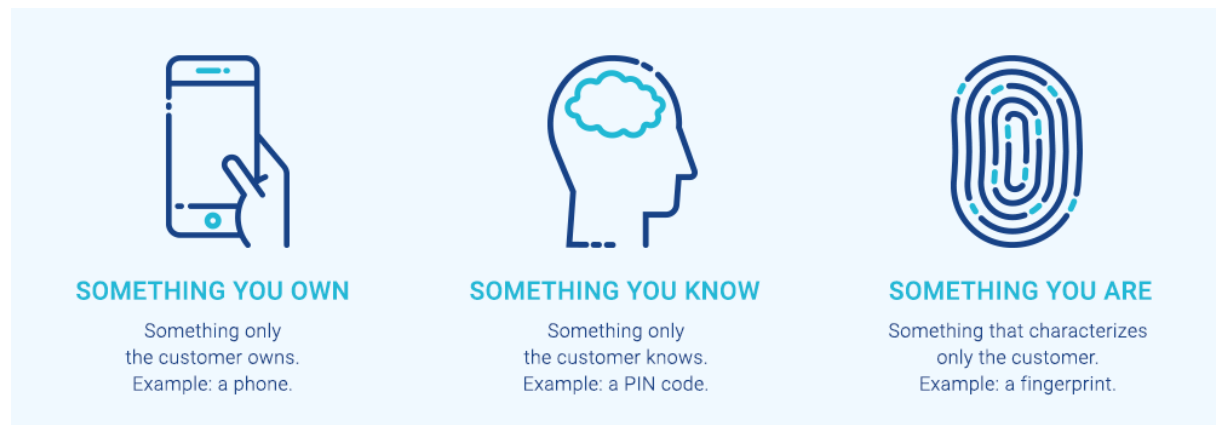
1.5 Authenticatievoorzieningen

Een authenticatievoorziening is een dienst waarmee een PDM gebruiker kan worden geauthentiseerd bij data aanbieders en afnemers. Authenticatievoorzieningen zijn randvoorwaardelijk aan PDM: regie is alleen mogelijk als zekerheid bestaat over de identiteit van de desbetreffende persoon. Een voorbeeld is DigiD, waarmee personen federatief kunnen inloggen bij overheidspartijen en andere organisaties binnen het BSN-domein¹⁷².

Een bijzondere rol spelen daarbij de authenticatiediensten, die soms een onderdeel vormen van een PDM-Dienst en soms zelf een deel van de PDM-Dienstverlening afdekken: ze voorzien primair in gegevensuitwisseling ten behoeve van het online identificeren van de gebruiker en diens autorisaties (machtigingen) voor toegang tot diensten.

Tweestapsverificatie (Strong Customer Authentication = SCA)

Tweestapsverificatie is onder meer nodig om veilig elektronisch te betalen, aan de kassa, in



webwinkels en met mobiel bankieren of internetbankieren.

Tweestapsverificatie wordt ook wel tweefactorauthenticatie of sterke klantauthenticatie genoemd. In het Engels: strong customer authentication of SCA. Het is een veilige manier om een betaling goed te keuren met twee verschillende dingen waar alleen de rechtmatige pashouder of rekeninghouder over beschikt. Aan de kassa is dat meestal een persoonlijke pinpas in combinatie met een geheime

¹⁷⁰ PKI-overheid. InnoValor, Hulsebosch, De Vos, 2019

¹⁷¹ <https://www.logius.nl/diensten/pkioverheid>

¹⁷² Om te bepalen welke informatie ontsloten mag worden na authenticatie met DigiD wordt tevens naar het betrouwbaarheidsniveau gekeken, zie ook <https://www.logius.nl/diensten/digid/hoe-werkt-het>

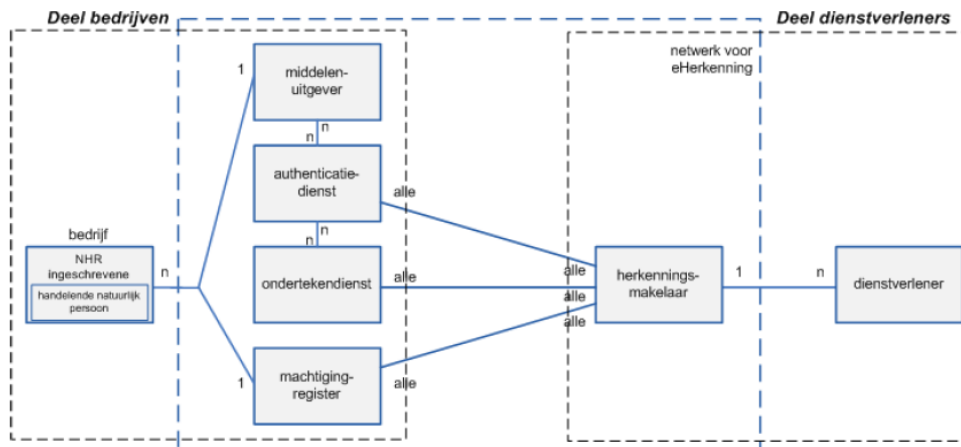
pincode. Met iDEAL en internetbankieren is dat vaak een persoonlijk inlogapparaatje, ook weer in combinatie met een geheime pincode. Bij mobiel bankieren is het een persoonlijke smartphone, bijvoorbeeld in combinatie met gezichtsherkenning.

Issuers, acquirers en betaaldienstverleners (payment service providers of PSP's) moeten voor online betalingen sinds 14 september 2019 voldoen aan de technische standaarden voor sterke klantauthenticatie (SCA) van PSD2. Omdat op 14 september nog veel schakels in de betaalketen voor online kaartbetalingen niet klaar waren met het invoeren van SCA, verlenen toezichthouders overal in de EU onder strikte voorwaarden tot eind 2020. Dit moet eraan bijdragen dat vooral kaarthouders, winkeliers en ondernemers geen onbedoeld negatieve gevolgen ondervinden van de invoering van SCA. Voor een vlotte migratie van de Nederlandse markt naar SCA voor online betalingen coördineert Betaalvereniging Nederland een migratieproject voor issuers, acquirers en PSPS's: het SCA Migratie Project.

1.5.1 Elektronische toegangsdiensten (ETD)

Het ETD-stelsel biedt een uniforme set van standaarden, afspraken en voorzieningen voor de geautoriseerde toegang tot digitale diensten. Hiermee kunnen vertrouwelijke persoonsgebonden gegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld worden. Als de Wet digitale overheid wordt aangenomen vervalt (ten dele) het afsprakenstelsel ETD. In de Wet DO is wel eHerkenning, maar niet Idensys opgenomen. Idensys betreft de digitale identificatie en authenticatie van personen en is stop gezet. De kern van het afsprakenstelsel ETD is dat het een netwerk van meerdere partijen (de zogenaamde deelnemers) betreft die samen toegangsdiensten leveren. In dat netwerk nemen partijen deel die authenticatiemiddelen uitgeven en bijbehorende diensten verlenen. Bestaande en toekomstige authenticatiemiddelen – zoals gebruikersnaam/wachtwoorden, card readers, VPN-tokens, maar ook mobiele telefoons met TANs – kunnen zo worden gebruikt. Ook nemen partijen deel die - op termijn - machtigingen van bedrijven en organisaties registreren en hierover informatie verstrekken.

Onderstaande figuur-5 laat de verschillende rollen in het afsprakenstelsel zien.



Figuur-5: Verschillen rollen in afsprakenstelsel ETD

1.5.2 eHerkenning

In eHerkenning loggen gebruikers (namens een organisatie gemachtigde personen) in via een middel dat is aangeschaft bij een van de makelaars binnen eHerkenning. eHerkenning is – onder de Wet Digitale Overheid verplicht - voor bedrijven die zaken willen doen met de overheid en daarvoor

eHerkenning

moeten inloggen op bepaalde eIDAS betrouwbaarheid niveaus. eHerkenning is daarmee een authenticatie afsprakenstelsel, waar bedrijven zich op kunnen aansluiten. eHerkenning wordt ingezet voor ROG in een zakelijke context. Personen worden gemachtigd door een organisatie of bedrijf om digitaal zaken te doen. Attributen die eHerkenning ontsluit zijn onder andere: naam, leeftijdsindicatie, geboorteplaats, geslacht, e-mailadres, telefoonnummer, organisatie, KvK nummer en identifiers.¹⁷³ Op de website van SIVI staat meer informatie over eHerkenning¹⁷⁴. Dit hangt samen met het gegeven dat de verzekeringssector als eerste private sector migreert naar eHerkenning¹⁷⁵.

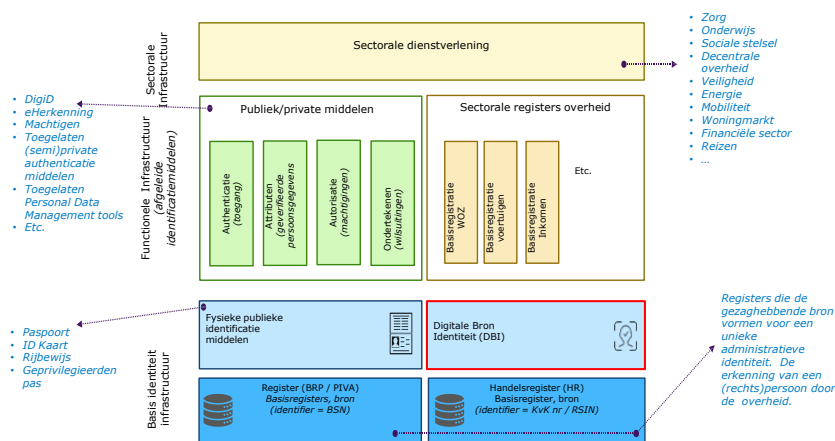
1.5.3 Digitale Bron Identiteit

BZK presenteerde in de Klantenraad Authenticatie en Portalen van 16 juli een voorlopige visie op digitale identiteiten. In een visiebrief aan de Tweede Kamer van 11 februari 2021 bevestigt Knops de uitwerking van deze visie.

De visie is gebaseerd op een aantal uitgangspunten:

- Delen van betrouwbare gegevens: Het fundament van de visie is gebaseerd op een overheid als “gezaghebbende bron”.
- Toegang: Het organiseren van toegang tot cruciale dienstverlening in de Nederlandse maatschappij voor alle burgers en bedrijven op een passend (eIDAS) betrouwbaarheidsniveau, zowel in het publieke als private domein.
- Digitale bron identiteit: Een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector¹⁷⁶.
- Afspraken kader digitaal vertrouwen: De uitgangspunten en afspraken rond het delen van gegevens, toegang en het leveren van vertrouwen in de digitale wereld, inclusief de digitale bron identiteit (DBI), worden vastgelegd in een afspraken stelsel “The Dutch Digital Trust Framework (DDTF)” (werknaam).

Onderstaande figuur-6 geeft een beeld van de beoogde Basis ID Infrastructuur.



Figuur-6: Beoogde Basis ID Infrastructuur – BZK juli 2020

¹⁷³ <https://afsprakenstelsel.etoegang.nl/display/as/Attribuutcatalogus>

¹⁷⁴ <https://www.sivi.org/eherkenning/veel-gestelde-vragen-eherkenning/>

¹⁷⁵ <https://www.sivi.org/eherkenning/>

¹⁷⁶ Zie ook: <https://www.digitaleoverheid.nl/achtergrondartikelen/samenwerken-aan-een-digitale-bronidentiteit/>. DGOO en RvIG ontwikkelen dit samen.

1.5.4 iDIN

Bij iDIN loggen gebruikers in via hun eigen bank, de bank authenticatieert de gebruiker en geeft een identiteitsverklaring af, zie figuur-7. iDIN geeft deze verklaring door aan de dienstverlener. iDIN is ontwikkeld door de banken voor consumenten. Bedrijven kunnen iDIN als inlog methode gebruiken om gebruikers te laten inloggen en deze uniek te identificeren. iDIN is daarmee een authenticatie afsprakenstelsel, waar banken en dienstverleners op kunnen aansluiten. Attributen die middels iDIN ontsloten worden zijn: naam, adres, leeftijdsindicatie, geboortedatum, geslacht, e-mailadres en telefoonnummer¹⁷⁷.

Intersoftware biedt op basis van iDIN een identificatieservice waarmee hypotheekadviseurs hun klanten op een snelle, veilige en betrouwbare manier online kunnen identificeren. Consumenten kunnen onder andere bij Aegon en Achmea online via iDIN inloggen.

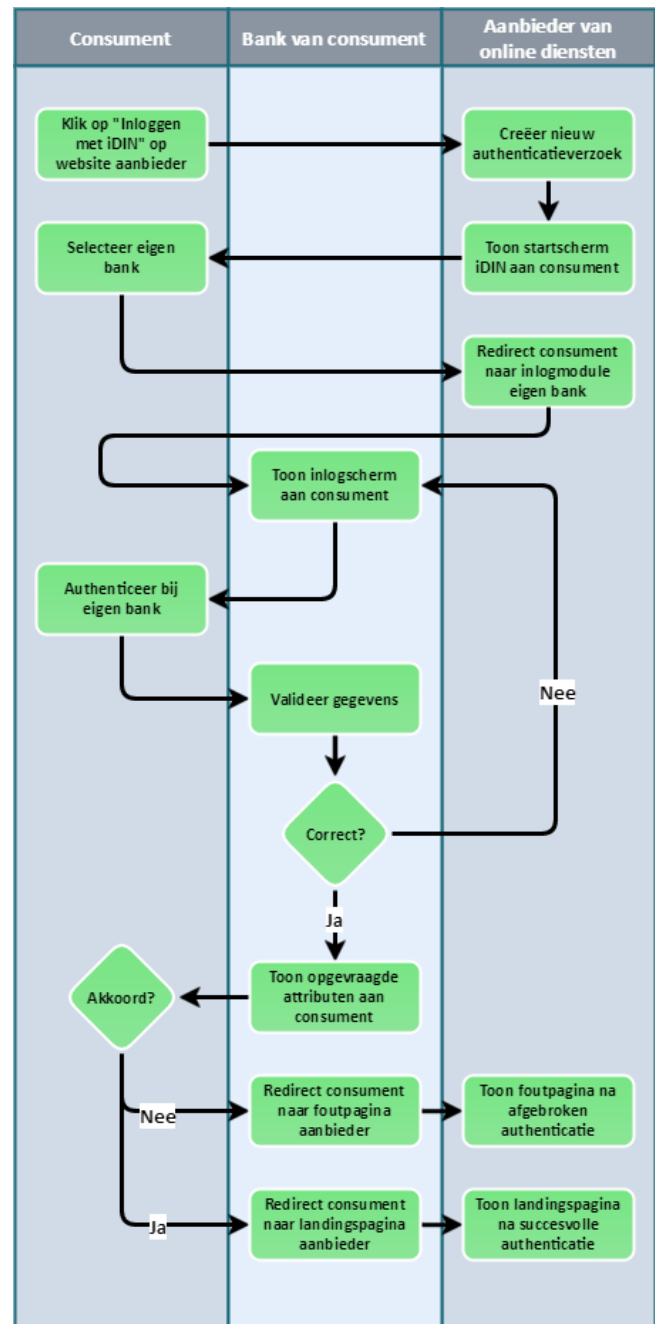
In juni 2020 bereikte werd de mijlpaal van 10 miljoen iDIN-transacties bereikt. Dit is 4 jaar na de introductie¹⁷⁸ door de Betaalvereniging Nederland.

In 2020 is de online identificatie- en inlogmethode iDIN met 7,5 miljoen transacties evenveel gebruikt als in de vier voorafgaande jaren vanaf de invoering in 2016. iDIN wordt niet alleen gebruikt om veilig in te loggen, iemands leeftijd online te controleren en iemand betrouwbaar digitaal te identificeren maar ook bij het rechtsgeldig digitaal ondertekenen van documenten¹⁷⁹.

Ondertekenen

iDIN wordt naast identificeren, inloggen en leeftijd bevestigen ook ingezet om online documenten te ondertekenen. Bij iDIN Ondertekenen wordt een te ondertekenen document gekoppeld aan de iDIN-transactie waarbij de consument bevestigt dat hij op die manier het document digitaal ondertekent met het inlogmiddel van zijn bank. De klant geeft in een herkenbare omgeving expliciet toestemming zijn gegevens te delen in het kader van het ondertekenen van een document. Met de toevoeging van het producttype iDIN Ondertekenen komt er een binding tussen het document en de identiteit, wordt de klantreis verder verbeterd en worden aanbieders specifiek voor deze dienst gecertificeerd. Dit is gebaseerd op de EU-vereisten voor een Advanced Electronic Signature.

Bedrijven die iDIN Ondertekenen willen gebruiken dienen hiervoor iDIN Ondertekenen af te nemen bij een Digital Identity Service Provider (DISP) met een specifiek certificaat voor het leveren van ondertekendienst. Alleen een gecertificeerde DISP kan zijn zakelijke klanten de mogelijkheid aanbieden om iDIN Ondertekenen op hun website te integreren.



Figuur-7: Gesimplificeerde flowchart authenticatieproces in iDIN.

¹⁷⁷ iDIN attributen. <https://www.idin.nl/over-idin/veelgestelde-vragen/>

¹⁷⁸ <https://www.idin.nl/actueel/mijlpaal-10-miljoen-idin-transacties/>

¹⁷⁹ <https://www.currence.nl/nieuws/ideal-idin-opmars-coronajaar-2020/>

1.5.5 EduGAIN

EduGAIN¹⁸⁰ biedt studenten de mogelijkheid om met hun onderwijs account in te loggen bij andere instellingen en diensten. Het focust zich op het internationale onderwijs en omvat onder andere de Nederlandse SURFconext en Zwitserse SWITCH identiteitsfederaties. Het is dus een overkoepelend authenticatie afsprakenstelsel. Voor het uitwisselen van persoonsgegevens over studenten en medewerkers zijn afspraken gemaakt. SAML wordt gebruikt voor de uitwisseling van gegevens, eduPerson en SHAC worden gebruikt voor het gegevensmodel (attribuut definities voor academische identiteiten en gegevens).



1.5.6 SURFconext

SURFconext¹⁸¹ focust zich op middelbaar/hoger onderwijs en onderzoek in Nederland en laat gebruikers met hun universiteit of HBO-account inloggen bij andere instellingen en services. De dienst aanbieder kan zelf kiezen welke teams of personen hij toestaat tot zijn dienst. Attributen die worden ontsloten via SURFconext zijn onder andere: naam, e-mailadres, organisatie, type organisatie, werknemer/student nummer, taal en identifiers¹⁸².



1.5.7 DigiD

DigiD is de Nederlandse oplossing voor het authenticeren van burgers die in willen loggen bij dienstverleners in het BSN-domein. De onderliggende standaarden van DigiD zijn OpenID Connect en SAML. DigiD is toegankelijk voor partijen die direct het BSN-nummer van burgers (wettelijk) mogen verwerken. Dit zijn in de private sector zorgverzekeraars en pensioenuitvoerders.



Op dit moment kan DigiD niet gebruikt worden buiten de overheid; de mogelijkheden hiertoe worden wel onderzocht. “Minister Knops: De heren Van Raak en Middendorp vroegen of DigiD ook gebruikt kan worden buiten de overheid. Zoals ik in mijn inleiding heb aangegeven, kan dat op dit moment niet. De Wet digitale overheid verbiedt dit ook op basis van artikel 8. Ik ga wel onderzoeken of het in de toekomst mogelijk is om dat publieke middel DigiD ook buiten de overheid te gebruiken, vanuit het principe dat de burger bepaalt welk middel hij of zij gebruikt, maar dat moet dan wel aan bepaalde voorwaarden voldoen, ook om de veiligheid te garanderen.”¹⁸³

Het dossier over fraude met DigiD¹⁸⁴ laat zien dat het huidige DigiD (Basis en Midden) niet veilig is. Daarom wordt gestreefd naar DigiD op hogere betrouwbaarheidsniveaus.

Het niveau Substantieel vereist het gebruik van de DigiD-app. In aanvulling op niveau Midden is het hierbij nodig om eenmalig, middels Remote Document Authentication, een identiteitsbewijs te scannen. De te gebruiken identiteitsbewijzen zijn de bestaande middelen en dan met een NFC-chip: het rijbewijs, de identiteitskaart en het paspoort. Voor het lezen van de chip is een NFC-chipkaartlezer of smartphone met NFC nodig. Doordat identiteitsbewijzen in persoon uitgegeven worden is er, in vergelijking tot uitgifte van een koppelcode via de post, meer zekerheid over de identiteit van de aanvrager. De huidige oplossingen voor DigiD substantieel bereiken thans niet de totale gewenste doelgroep. Dit hangt samen met het feit dat een aanzienlijk deel van de doelgroep niet beschikt over een smartphone met een Android besturingssysteem met NFC-lezer. Gevraagd is hoeveel van de ruim 13,5 miljoen actieve DigiD-gebruikers beschikken over een smartphone met een Android besturingssysteem met NFC-lezer. Uit onderzoek in 2019 is gebleken dat ongeveer de helft van het aantal DigiD-gebruikers beschikt over een smartphone met een geschikt Android besturingssysteem met NFC-lezer.

¹⁸⁰ <https://edugain.org/>

¹⁸¹ <https://www.surf.nl/en/SURFconext-global-access-with-1-set-of-credentials>

¹⁸² <https://wiki.surfnet.nl/display/surfconextdev/Attributes+in+SURFconext#AttributesinSURFconext-Attributeoverview>

¹⁸³ <https://zoek.officielebekendmakingen.nl/h-tk-20192020-50-3.html>

¹⁸⁴ <https://opgelicht.avrotros.nl/dossiers/artikel/digid-fraude/#/>

Als no regret-actie, die later de brede uitrol naar het niveau 'Substantieel' en 'Hoog' kan vergemakkelijken en versnellen, is de overheid in 2019 gestart met het stimuleren van het gebruik van de DigiD App. Dit impliceert de verplichting om met 2-factor authenticatie in te loggen. In het zorgdomein is het streven dat burgers vanaf 1 januari 2021 op niveau Substantieel inloggen bij hun zorgverleners.

In de toekomst zal de elektronische identiteitskaart, eID, worden ingevoerd. Hiermee beschikt men over zekerheidsniveau Hoog. Rijbewijzen die na mei 2018 zijn uitgegeven bevatten de eID-applet en hiermee kan men zich aanmelden met DigiD Hoog. Het gebruik van eID, en daarmee DigiD Hoog, vereist ook een pincode als tweede factor. Voor communicatie met de eID-applet op het identiteitsbewijs is het gebruik van de DigiD-app noodzakelijk, net als een NFC-chipkaartlezer of smartphone met NFC. Zoals hiervoor is aangegeven zijn voor DigiD Hoog relatief nieuwe identiteitsbewijzen nodig, die een natuurlijk vervangingsritme kennen van 10 jaar. De uitrol van deze kaarten neemt dus nog flink wat tijd in beslag.

In relaties tot de Europese zekerheidsniveaus, binnen eIDAS, zijn zowel DigiD Basis als Midden vergelijkbaar met eIDAS Laag. DigiD Substantieel en DigiD Hoog zijn vergelijkbaar met respectievelijk eIDAS Substantieel en eIDAS Hoog en zijn ook aangemeld om onderdeel van het eIDAS-stelsel te worden erkent.

1.5.8 *Itsme*

Itsme¹⁸⁵ is een Belgische variant van DigiD, die Belgische burgers een uniek nummer geeft, maar wel publiek en privaat gebruikt kan worden. Dit doet Itsme door gebruikers te identificeren met de Belgische identiteitskaart of via een bank, waarna gebruikers de app kunnen gebruiken om op verschillende plekken desgevraagd hun digitale identiteit te laten zien. In december 2019 is Itsme ook in Nederland geïntroduceerd. Gegevens kunnen in de Itsme app zelf staan, of worden verrijkt door de Belgische overheid via het nationale register voor persoonsgegevens.

Itsme is een centrale oplossing, met alle identiteiten in één database. Hierdoor is centrale monitoring mogelijk. Dit is volgens experts niet wenselijk.



1.5.9 *Cleverbase ID*

Cleverbase is een Qualified Trust Service Provider (QTSP – een begrip uit de eIDAS verordening) en geeft digitale identiteiten en middelen uit voor het zetten van gekwalificeerde elektronische handtekeningen en staat onder toezicht van het Agentschap Telecom.

Cleverbase ID¹⁸⁶ is een authenticatie voorziening in de vorm van een mobiele app. De gebruiker maakt een CleverbaseID aan en kan vervolgens op andere plekken zijn unieke Cleverbase identiteit gebruiken om in te loggen en documenten te ondertekenen. Cleverbase werkt binnen PKI-overheid.

Willeke

Een aantal experts, werkzaam bij Cleverbase, werkten mee aan een artikel over Willeke. Willeke is een slanke infrastructuur voor gekwalificeerde informatie-uitwisseling op basis van vertrouwde identiteiten. Het doel is om een alternatieve architectuur te demonstreren waarin het identificeren van personen, het uitwisselen van informatie, het autoriseren van externe partijen en het ondertekenen van documenten gebruiksvriendelijker en veiliger wordt. Om te beginnen heeft elke persoon zijn of haar persoonlijke gegevensruimte, geleverd door een gekwalificeerde vertrouwensdienstverlener die ook een elektronische ID met hoge mate van zekerheid uitgeeft. Er zijn drie belangrijke bouwstenen nodig: (1) veilige uitwisseling tussen de persoonlijke gegevensruimte van elke persoon, (2) coördinatiefuncties die worden geboden door een op tokens gebaseerde infrastructuur, en (3) governance over deze infrastructuur.

¹⁸⁵ <https://www.itsme.be/>

¹⁸⁶ <https://cleverbase.com/>

1.5.10 EduID

EduID¹⁸⁷ is nog in ontwikkeling. Een eduID is een account voor gebruikers binnen onderwijs en onderzoek in Nederland. Het is persoonsgebonden en bestaat onafhankelijk van een onderwijsinstelling. Het kan gebruikt worden om in te loggen op diverse diensten aangesloten op SURFconext. eduID is vooral bedoeld voor gebruikers die geen account van een instelling hebben of voor diensten waarbij een instellingsonafhankelijk account handig is.



1.5.11 NotarisID

NotarisID is een identificatiemiddel van Koninklijke Notariële Beroepsorganisatie (KNB). NotarisID is nog in ontwikkeling en straks verkrijgbaar via de notaris. Kort door de bocht kunnen gebruikers na een face-to-face-onboarding (bij de notaris) via een app op de telefoon authenticeren. Daarbij kunnen allerlei attributen worden geladen en getoond aan derden. Deze worden niet opgeslagen maar worden per sessie opgehaald en getoond.

Andere kenmerken van NotarisID zijn:

- Betrouwbaarheidsniveau Hoog.
- Biedt gekwalificeerde handtekeningen.
- Burger krijgt middel gratis, de kosten worden verrekend door middel van een tikkenmodel voor de dienstverlener.



1.5.12 Attribuut gebaseerde authenticatie Medmij

PROVES, Stichting MedMij en VZVZ hebben een geslaagde technische proef achter de rug met attribuut-gebaseerde authenticatie. Over de Proof of Concept (PoC) is in juli 2020 een rapport gepubliceerd¹⁸⁸. De oplossing maakt het mogelijk dat een zorggebruiker met hetzelfde authenticatiemiddel kan inloggen bij zijn persoonlijke gezondheidsomgeving (PGO) en bij de eigen zorgaanbieders. Op dit moment is dat nog niet mogelijk binnen MedMij in combinatie met DigiD.

De probleemstelling in het genoemde rapport is:

- DigiD is niet erg gebruiksvriendelijk
- De koppeling van de identiteit van de zorggebruiker in het persoons- en zorgaanbiedersdomein is niet erg sterk
- DigiD op niveau Substantieel is nog niet breed beschikbaar
- Het aansluiten van zorgaanbieders op DigiD gaat gepaard met hoge vaste kosten. Dit alles bemoeilijkt uitrol van MedMij in de praktijk.

Alle opgedane kennis en input is verwerkt in diverse minimale eisen en uitgangspunten voor het Afsprakenstelsel attribuut-gebaseerde authenticatie¹⁸⁹. Vervolgstappen moeten onder meer bepalen hoe authenticatie via attributen (persoonseigenschappen) op een afdoende beveiligingsniveau gerealiseerd kunnen worden.

1.5.13 Verimi

Van de buitenlandse toepassingen wordt Verimi hier kort besproken. Verimi¹⁹⁰ is een brancheoverschrijdend identiteitsplatform. Het Duitse initiatief van Axel Springer, Daimler, Allianz en Deutsche Bank is in april 2018 gelanceerd. Verimi faciliteert Single Sign-on en data consent management voor de gebruiker. Gepersonaliseerde advertenties moeten de voornaamste inkomensstroom worden. Bedrijven koppelen via API's op basis van OpenID Connect & OAuth 2.0.



¹⁸⁷ <https://www.EduID.nl>

¹⁸⁸ Eindrapportage Proves Attribuut-gebaseerde Authenticatie proof of concept, 16 juli 2020

¹⁸⁹ <https://afsprakenstelsel.medmij.nl/display/MACM/RFC0008+Attribuut+gebaseerde+authenticatie>

¹⁹⁰ <https://verimi.de/de/partner>

Verimi is de consortiumleider van PeopleID¹⁹¹, andere consortiumpartners zijn AUTHADA, Deutsche Telekom Security GmbH, Fraunhofer AISEC en ISST, Optica.

Het People ID-showcaseproject richt zich op gebruiksvriendelijkheid, sector overschrijdend en demografisch bereik en naleving van de hoogste beveiligingsnormen. Allereerst ontwikkelt het consortium rond Verimi een concept voor PeopleID, dat vervolgens als voorbeeld in de regio Darmstadt wordt geïmplementeerd. Op deze manier wordt de eerste steen gelegd voor een in Duitsland ontwikkeld systeem dat in heel Europa bruikbaar is voor het gebruik van de elektronische identiteitskaart (eID). De ambitie is het wijdverbreide gebruik van veilige digitale identiteiten aantonen - in een grote verscheidenheid aan publieke en private sectoren.

1.6 Nationale PDM-Diensten

Een PDM-Dienst is een dienst die een individu in staat stelt om zijn/haar persoonlijke informatie duurzaam te beheren en te onderhouden om deze, wanneer de gebruiker dit in zijn belang acht, te kunnen delen met anderen. PDM-Diensten vervullen in ieder geval de rol van operator of data aanbieder, maar in sommige gevallen ook die van data afnemer.

1.6.1 Inleiding

Bieden operators puur de mogelijkheid om toestemmingen te managen? Zijn het kluisen waarin we onze gegevens opslaan of bieden ze slechts een beheerfunctie voor gegevensuitwisseling tussen data afnemer en data aanbieder (ook wel 'sluizen' genoemd)? Of iets daar tussenin?

Voor de analyse hebben we de volgende werkwijze gehanteerd: op basis van een korte deskresearch fase zijn alle relevante operators beknopt beschreven. Daarna is met een deel van de operators contact gezocht voor het invullen van een vragenlijst (zie bijlage F). De uitkomsten van die vragenlijst zijn daarna besproken met de operators en verder aangevuld en ter goedkeuring voorgelegd. Niet alle operators hebben aan de vragenlijst meegewerkt. De feedback van de operators die meewerkten is hierna verwerkt.

1.6.2 Blauwe Knop

De Blauwe Knop is een beeldmerk en werkwijze die ontwikkeld worden door het Blauwe Knop programma. Momenteel is de Blauwe Knop op diverse websites van gemeentes en uitvoerders ingevoerd. Het moet mensen de mogelijkheid bieden hun persoonlijke data te downloaden van overheidswebsites, in een gewaarmerkt document. Mensen kunnen deze data vervolgens zelf gebruiken voor verschillende doeleinden. Schuldhulpverlening is een van de belangrijke thema's waar op dit moment aan gewerkt wordt. In de praktijk krijgen organisaties die de Blauwe Knop willen toepassen een toolkit ter beschikking met het beeldmerk, generieke content, voorbeeldcode en architectuur en een stappenplan voor de implementatie. De Blauwe Knop zorgt daarmee voor standaardisatie van gegevens downloaden bij de overheid. Op termijn moeten naast de downloadfunctionaliteit ook architectuur principes beschikbaar komen voor directe gegevensuitwisseling tussen organisaties onder regie van de persoon. Een definitief besluit over het toepassen van de Blauwe Knop moet nog genomen worden. De juridische basis ontbreekt nog.



1.6.3 MijnOverheid

MijnOverheid¹⁹² is een combinatie van digitale post (Berichtenbox) en diensten voor de burger vanuit de overheid. Het geeft inzicht in persoonlijke gegevens die de overheid van de burger heeft. MijnOverheid ontsluit via een portaal de zaken die bij een veelheid van instanties lopen. Er is onder meer direct inzicht in de data die de basisregistratie personen (BRP) heeft, inkomensgegevens zoals bij de Belastingdienst bekend zijn, woninggegevens

mijnOverheid

¹⁹¹ https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SchaufensterSichereDigIdentProjekte/sdi-projekt_peopleID.html

¹⁹² Mijn Overheid. <https://mijn.overheid.nl/>

van Kadaster en kentekenregistratie van het RDW. Daarnaast wordt ook naar een aantal andere 'mijn omgevingen' doorgelinkt, waaronder Donorregister, DUO en Pensioenregister. MijnOverheid ontsluit primair gegevens richting de burger, het speelt geen rol in het doorgeven van de gegevens aan derden. Gegevensuitwisseling met derden gebeurt door de achterliggende organisaties zelf op basis van wettelijke gronden, niet via de burger. Het is dus nog voornamelijk een data aanbieder, maar puur voor publieke organisaties. Inloggen bij MijnOverheid gaat via DigiD.

1.6.4 IRMA

IRMA is aan de Radboud Universiteit in Nijmegen ontwikkeld. IRMA biedt een privacy vriendelijke manier voor gebruikers om, via een app op de mobiele telefoon, zelf volledige controle te hebben over met wie zij hun gegevens delen zonder dat de verstrekker van die gegevens daar weet van heeft. IRMA staat dan ook voor 'I Reveal My Attributes': de gebruiker heeft zelf de controle over wat gedeeld wordt en met wie.



De gebruiker van IRMA kan over hem of haar door diverse partijen vastgelegde attributen, zoals naam, leeftijd en woonplaats, ophalen bij partijen die IRMA gegevens faciliteren. Dat kan onder andere bij de Basisregistratie Personen (via DigiD), banken (via iDIN). De ontvanger van de gegevens is de partij die de attributen controleert en verwerkt. De beoogde ontvanger geeft aan welke attributen nodig zijn voor optimale dienstverlening aan de gebruiker, die er vervolgens voor kan kiezen om deze attributen wel of niet te delen.

Het betrouwbaarheidsniveau van IRMA is afhankelijk van het betrouwbaarheidsniveau van het middel dat wordt gebruikt om de attributen te verkrijgen. Bij BRP-gegevens is dat nu DigiD Midden, wat in feite betrouwbaarheidsniveau Laag is. Voor veel diensten in de sector is dit voldoende, maar voor diensten die Substantieel of Hoog behoeven is het wachten op een hogere dekingsgraad van DigiD Substantieel of de komst van DigiD Hoog, of zal de dienstverlener zelf alternatieve maatregelen moeten treffen om meer zekerheid over de identiteit van de gebruiker te krijgen.

De echte meerwaarde van IRMA hangt af van de uitgevers die gekoppeld zijn; met BRP heeft IRMA er een aan boord die uniek en strategisch zeer waardevol is. Potentiële toepassingen van IRMA zijn het voorinvullen van gegevens bij het afsluiten van een verzekering, gepersonaliseerde dienstverlening, het verwerken van machtigingen, het doorgeven van schadevrije jaren, een bewijs van in leven zijn en het gebruik als authenticatiemiddel.

Adoptie van IRMA is volgens SIVI nog geen gelopen race. Veel zaken rondom beveiliging, governance, standaardisatie, vertrouwen bij de gebruiker en het businessmodel staan nog in de kinderschoenen en vormen stuk voor stuk een risico voor de continuïteit van de oplossing.

SIDN

De stichting Privacy by Design - de eigenaar van de afspraken rond IRMA – werkt van september 2019 structureel en operationeel samen met SIDN¹⁹³. SIDN is een stabiele, ISO27001 gecertificeerde organisatie met als kernactiviteit het beheren van het .nl-domein. SIDN heeft – net als IRMA – geen winstoogmerk. Met SIDN lijkt IRMA daarmee een goede partner gevonden te hebben om de infrastructuur (zoals de IRMA-server), het beheer en de verdere ontwikkeling ervan blijvend te bekostigen.

Het wetsvoorstel voor Wet Digitale Overheid biedt volgens SIDN de ruimte om private middelen, die worden gebruikt bij toegang tot de overheid, ook in te zetten in het commerciële domein. SIDN¹⁹⁴ stelt dat bij het vaststellen van een toelatingskader voor middelen onder de Wet Digitale Overheid de unieke kans ontstaat om drie dingen te doen:

- De burger beschermen tegen data-driven verdienmodellen en een integere publieke voorziening realiseren;
- Betaalbare en betrouwbare middelen mogelijk maken, wat het gebruik door en vertrouwen van de burger zeker positief beïnvloedt;

¹⁹³ <https://www.sidn.nl/nieuws-en-blogs/sidn-en-privacy-by-design-bundelen-krachten-voor-privacyvriendelijke-elektronische-identiteiten-via-irma>

¹⁹⁴ <https://ibestuur.nl/podium/self-sovereign-identity-kan-het-echte-verschil-maken>

- De scheidslijn tussen publieke en private middelen doorbreken.

Onderzoek SIVI

Zie verder ook het uitgebreide onderzoek van SIVI (in samenwerking met InnoValor) naar IRMA¹⁹⁵

1.6.5 Dappre

Dappre¹⁹⁶ is een mobiele app waarin loyalty- en cadeaukaarten kunnen worden opgeslagen. Het is ook mogelijk in de Dappre App een kaartje aan te maken en daarop persoonsgegevens in te vullen. Gebruikers kiezen daarbij zelf of en welke persoonsgegevens zij voor welk doel met wie willen delen en voor hoelang. Dappre is ontstaan vanuit Digital Me en is ook gebaseerd op de Qiy Trust Principles. Dappre is operationeel en focust zich op de Europese markt van de consumenten sector. Dappre kan bij onder andere HEMA, Decathlon, VVV, Albert Heijn en IKEA gebruikt worden.

1.6.6 Ivido

Ivido¹⁹⁷ is een voorbeeld van een Persoonlijke Gezondheidsomgeving (oftewel, een operator gericht op een medische gegevens). Het is een van de initiatieven die een MedMij-label heeft verkregen. Binnen Ivido kunnen mensen medische gegevens bij elkaar brengen en communiceren met zorgverleners en desgewenst met familieleden. Het is ook mogelijk om gegevens vanuit wearables (zoals fitness horloges) toe te voegen. Ivido koos om personen zich te laten identificeren en inloggen met het eerdergenoemde IRMA. Dit zorgt er daarnaast voor dat Ivido over de BRP-gegevens van de persoon beschikt.



Ivido wordt momenteel kosteloos aangeboden aan gebruikers. Hiervoor wordt gebruik gemaakt van een tijdelijke financieringsregeling van het ministerie van VWS, waardoor Ivido een vaste bijdrage per gebruiker krijgt, maar wel verplicht wordt de PGO gratis aan te bieden.¹⁹⁸

1.6.7 Health Apps

Over Health Apps zegt het Rathenau Instituut¹⁹⁹:

- Het is lastig om de eigen, individuele gegevens in te zien.
- Het is lastig of zelfs onmogelijk om de eigen gegevens te downloaden of onder te brengen in een PGO of medisch dossier voor verdere toepassing. Dat maakt regie nemen over de eigen gezondheid op basis van gegevens uit meerdere bronnen lastig.
- De gebruiker heeft weinig tot geen controle over het verder delen met andere partijen dan de aanbieder van de coachende functie.
- Algoritmen spelen een belangrijke rol bij het tot stand komen van persoonlijk scores van fitheid, of waardering van welzijn en gezondheid. Welke individuele gegevens er wel of niet gebruikt worden, of met welke weging, is voor de gebruiker niet inzichtelijk en in die zin dus oncontroleerbaar.
- De wetenschappelijke onderbouwing van de adviezen én van de gedragstherapie laten bij de vrij beschikbare apps nog veel te wensen over.
- Wanneer de apps worden gekoppeld aan diensten zoals onlineportalen of burgerplatforms, wordt minder inzichtelijk waar gegevens heengaan en voor welke analyses ze worden gebruikt. Ze kunnen weglekken naar commerciële partijen. Voorzichtigheid in het delen van de door de apps gegenereerde gegevens blijft geboden.



¹⁹⁵ <https://www.sivi.org/wp-content/uploads/2019/12/Waarde-IRMA-voor-pensioen-en-verzekeringssector-SIVI-17-december-2019New.pdf>

¹⁹⁶ <https://dappre.com>

¹⁹⁷ <https://ivido.nl/>

¹⁹⁸ <https://www.icthealth.nl/nieuws/ivido-tekent-overeenkomst-met-vws-voor-gratis-pgo/>

¹⁹⁹ <https://www.rathenau.nl/nl/digitale-samenleving/health-apps-data-gebruik>

Rathenau Instituut pleit voor het recht niet gemeten, geanalyseerd of gecoacht te worden en het recht op betekenisvol contact. Het is voor het Rathenau instituut de vraag in hoeverre alle burgers die dat willen ook in staat zijn actie te ondernemen op basis van inzicht in gezondheidsgegevens of feedback van health apps. Het risico bestaat dat de capaciteiten van burgers hierin worden overschat. Naast digitale vaardigheden vraagt dit van burgers namelijk een goede interpretatie van de digitale gezondheidsgegevens en daadkracht om bijvoorbeeld ongezond gedrag aan te passen. Juist diegenen die vaker van zorg gebruik maken – zoals ouderen, mensen met een lage sociaaleconomische status, verstandelijk beperkten, laaggeletterden, mensen met ernstige psychische of complexe aandoeningen, migranten – beschikken vaak in mindere mate over bovenstaande vaardigheden. In de samenleving kan zo een digitale tweedeling in gezondheid ontstaan. Ook kan in de samenleving de solidariteit afnemen ten opzichte van mensen die geen regie willen of kunnen nemen op basis van hun digitale gezondheidsgegevens.

1.6.8 Diabetesdiensten

Diabetes Services²⁰⁰ bouwt een mens-centraal digitaal ecosysteem van data met behulp van diensten voor diabetes- en lifestyle management. Uitgangspunt is dat smartphones, medische apparaten en persoonlijke wearables een grote hoeveelheid gegevens van de persoon verzamelen. Diabetes Services monteert deze data tot een digitaal dagboek.



1.6.9 Emrex

Emrex²⁰¹ is een platform waarop studenten hun gegevens kunnen delen. Het gaat daarbij bijvoorbeeld om het delen van studieresultaten tussen universiteiten (denk aan het doorgeven van resultaat na een semester in het buitenland). Wanneer onderwijsinstellingen zichzelf hebben aangesloten op het systeem kunnen studenten bij hen inloggen en gegevens van andere instellingen ook inladen en delen. Emrex focust zich op het samenbrengen van bestaande oplossingen en niet op het creëren van nieuwe standaarden en operators. Hierdoor raakt Emrex ook aan de functies van een afsprakenstelsels. Emrex is ook onderdeel van ESC (EU student card) afsprakenstelsel. Emrex is een operator, maar kan ook data aanbieder en data afnemer zijn. Emrex is een Europees initiatief, focust zich op de educatieve sector en zit nog in de pilot fase. Er zijn al verschillende instellingen aangesloten, waaronder DUO vanuit Nederland, waardoor Nederlandse diploma's toegevoegd kunnen worden.



1.6.10 Qlik2Share

Qlik2Share²⁰² is een tool om privacy op het internet te waarborgen. De gebruiker krijgt controle over gegevens door deze zelf centraal te beheren en gecontroleerd te delen met partijen die de gegevens nodig hebben. De gebruiker houdt het overzicht over wie welke gegevens van hem/haar heeft.



De gebruiker kan gegevens ook bundelen op een digitaal visitekaartje. Dit resulteert in een link die hij/zij kan uitdelen. De links van anderen kunnen worden opgeslagen in een persoonlijk adresboek. Als extra feature biedt Qlik2Share een digitale kluis waarin de gebruiker wachtwoorden en andere gegevens extra beveiligd in op kan slaan.

Achter Qlik2Share zit ook Qlik2Shop dat samenwerkt met meer dan 1000 webshops. Dit levert de gebruiker bonusvoordeel op.

²⁰⁰ <https://www.diabetes.services>

²⁰¹ <https://emrex.eu/>

²⁰² <https://www.iaddress.nl/qlik2share>

1.6.11 Diplomaregister

In het Diplomaregister²⁰³ staan diplomagegevens van de meeste door het OCW erkende Nederlandse opleidingen. Het Diplomaregister wordt door DUO beheerd. Vanuit het Diplomaregister, binnen de Mijn DUO omgeving, kunnen mensen gewaarmerkte uittreksels van diploma's downloaden. Door de waarmerking van het pdf- bestand kunnen werkgevers en scholen de echtheid controleren van het diploma. Het diplomaregister vervuld hierdoor de rol van data aanbieder. Hiernaast kunnen ook wijzigingen in het geval van fouten doorgegeven worden. Het ophalen van uittreksels en doorgeven van wijzigingen is gratis voor de gebruiker. Het diplomaregister wordt ook binnen EMREX gebruikt voor inschrijvingen bij buitenlandse onderwijsinstellingen.



1.6.12 FeatherFeed

FeatherFeed werkt aan een content recommendation system waarbij de gegevens bij de gebruiker blijven, waardoor deze meer en makkelijker regie kan voeren over zijn gegevens. Momenteel focust FeatherFeed voornamelijk op het aanbevelen van artikelen. Hierbij verzamelt en bewaart FeatherFeed lokaal op het device van de gebruiker de informatie over de gebruiker. Waar deze informatie normaliter naar de dienstverlener gaat, die op deze manier veel informatie over de gebruiker verzamelt, blijft de informatie nu daadwerkelijk bij de gebruiker op het apparaat. Het aanbod wordt vervolgens naar de gebruiker gebracht. Bedrijven kunnen artikelen aanbieden aan de FeatherFeed kluis van de gebruiker, waarna FeatherFeed op basis van de lokaal bewaarde informatie beslist om een artikel daadwerkelijk wel of niet aan de gebruiker aan te bieden. De gebruiker kan vervolgens ook feedback geven aan FeatherFeed, zodat FeatherFeed de volgende keer nog beter passende artikelen kan aanleveren. Ook kan de gebruiker aangeven dat hij bepaalde onderwerpen niet meer wil zien. Zo voorkom je dat je nog maanden achtervolgd wordt met advertenties naar aanleiding van een enkele zoekopdracht: Eén klik op de knop en dergelijke advertenties komen niet meer terug. FeatherFeed wordt ontwikkeld door Katalysis, een Amsterdamse startup. Het is beschikbaar als browser plug-in en zal in 2021 ook als app beschikbaar komen.



1.6.13 JiD

JiD is een PDM-oplossing ontwikkeld door JanusID. Het bestaat in demo vorm sinds 2017. Het biedt mogelijkheden om in te loggen op websites van derden, maar daarnaast ook de mogelijkheid om persoonlijke attributen te delen. Hierbij wordt veel aandacht besteed aan het betrouwbaarheidsniveau van de data die gedeeld kan worden. Belangrijk onderdeel hiervan is CheckedID, een identiteitsverificatieoplossing van JanusID, waar met behulp van een identiteitsdocument en biometrie met hoge betrouwbaarheid de identiteit van iemand kan worden vastgesteld.



Ten opzichte van een normale authenticatiedienst biedt JiD de gebruiker meer controle over welke data gedeeld wordt met de data-afnemer. Er moet consent gegevens worden dat er data gedeeld wordt en deze kan ook ingetrokken of gewijzigd worden. Tevens bestaat de mogelijkheid om op de ene plek een met hoge zekerheid vastgestelde identiteit te delen en op de andere plek, waar zekerheid minder belangrijk is, een nickname. Als potentiële use-cases ziet JanusID vooral situaties waar een hogere zekerheid over iemand identiteit belangrijk is. Denk hierbij aan verhuur van auto's, waar nu nog regelmatig een identiteitsbewijs getoond moet worden of het digitaal ondertekenen van een overeenkomst. JiD ondersteund ook use-cases waar zulke hoge zekerheid van minder groot belang is: Denk hierbij aan een gebruiker die kan bewijzen dat hij oud genoeg bent is alcohol te mogen kopen.

Bij JiD betaalt de data afnemer, maar er wordt ook gekeken naar de mogelijkheid om het individu te laten betalen voor een account waarvan de identiteit met hoge zekerheid is vastgesteld met behulp van CheckedID.

JiD bestaat nog steeds alleen in demo vorm. JanusID is momenteel aan het kijken naar een samenwerking met een aantal andere partijen om JiD opnieuw in te richten en naar een nieuw niveau te tillen.

²⁰³ <https://duo.nl/diplomaregister/>

1.6.14 MijnApp

MijnApp²⁰⁴ is een initiatief vanuit de gemeente Eindhoven en wordt tegenwoordig in samenwerking met meerdere partijen zoals gemeente 's-Hertogenbosch, gemeente Den Haag, VNG, CJIB en de community van het NL Design System verder ontwikkeld. De ambitie van MijnApp is om alle dienstverlening aan de burger aan te bieden op één plek, waarbij de burger of ondernemer ook daadwerkelijk centraal staat. Het wil drie doelstellingen realiseren: Een plek waar de burger terecht kan met zijn of haar vraag, de oplossing voor die vraag en dat onder regie op gegevens voor de burger. Diensten moeten afgenomen kunnen worden onafhankelijk van tijd en locatie.



Een use-case waar MijnApp nu een pilot voor ontwikkeld is de zogenaamde Rode Knop, waarbij een persoon die in betalingsproblemen komt zich kan melden bij het CJIB met het verzoek zijn schuld tijdelijk te laten bevriezen, zodat deze niet verder oploopt. Hierna moet de gebruiker binnen 4 maanden kunnen aantonen dat hij of zij een aanvraag heeft gedaan bij de gemeente voor schuldhulpverlening. Dit bewijs kan via MijnApp makkelijk gedeeld worden met het CJIB.

Een andere use-case, die momenteel al in gebruik is, is het doorgeven van verhuizingen naar of binnen Den Bosch. Dit proces is geheel geïntegreerd in de bestaande flow, waardoor de gebruiker nauwelijks merkt dat hij gebruik maakt van MijnApp. MijnApp is hier geïntegreerd als webapp, waardoor geen separate mobiele app gedownload hoeft te worden.

Zoals MijnApp nu ontwikkeld is, functioneert het als doorgeefsluis. Gegevens worden uit bronnen zoals basisregistraties opgehaald en kunnen gedeeld worden met de organisatie die hiervan gebruik wil maken voor een dienst. Hierbij kan de gebruiker aangeven welke gegevens hij wel of niet wil delen en voor hoe lang hij deze gegevens wil delen. Wel wordt er een waarschuwing gegeven zodra de gebruiker afwijkt van de standaard, dat dit de dienstverlening kan beïnvloeden en gegevens mogelijk nogmaals gedeeld moeten worden.

MijnApp maakt gebruik van het vijflagen model uit Common Ground. Hierbij geeft MijnApp alleen invulling aan de bovenste laag: de UX-laag. Voor deze en onderliggende lagen wordt zoveel mogelijk gebruik gemaakt van bestaande standaarden en best-practices. Zo wordt onder andere gebruik gemaakt van het NL Design System²⁰⁵ voor de UX-laag. MijnApp wordt ontwikkeld als continue bèta-versie. Het is niet de bedoeling dat bij oplevering alle dienstverlening al beschikbaar is, maar dat er in de loop van de tijd steeds meer dienstverlening toegevoegd en in productie genomen wordt. Voorlopig wordt het verdienmodel bepaald met de deelnemende partijen per use-case. Er wordt nog gezocht naar een toekomstbestendig duurzaam verdienmodel.

Ondanks dat MijnApp vanuit het gemeentelijk domein ontwikkeld wordt, is het doel dat ook andere partijen diensten kunnen aanbieden via MijnApp, zowel binnen als buiten het overheidsdomein. Hiervoor wordt onder andere gekeken naar een SSI-oplossing, omdat veel private partijen niet zomaar op het overheidsdomein kunnen en mogen koppelen.

1.6.15 Qii

Qii²⁰⁶ (voorheen bekend als Huurpaspoort) maakt het mogelijk om via digitale weg op woningen te reageren en de benodigde gegevens aan de verhuurder te leveren. Gegevens worden verzameld via een mobiele app van Qii. Gedurende het proces wordt er bij MijnOverheid, Belastingdienst en UWV met DigiD ingelogd om daar de benodigde gegevens via screen scraping op te halen. Naast de opgehaalde gegevens is er de mogelijkheid om extra gegevens aan te leveren of indien de situatie van de huurder veranderd is, gegevens te wijzigen. Alle gegevens worden op moment van verzamelen op het device van de gebruiker opgeslagen, en na toestemming in een persoonlijke digitale kluis op de servers van Qii. Deze gegevens kunnen gedeeld worden met een verhuurder als een gebruiker op een woning wil reageren. De verhuurder kan deze gegevens ophalen bij Qii. Consent om te delen kan weer worden ingetrokken. Dit kan automatisch voor de gegevens die



²⁰⁴ <https://rog.pleio.nl/news/view/57900055/verzekering-vergunning-paspoort-met-mijnapp-regel-je-het-allemaal>

²⁰⁵ <https://designsystem.gebruikercentraal.nl/over-het-nl-design-system/>

²⁰⁶ <https://qii.nl/>

bij Qii staan, maar als gegevens al met de verhuurder gedeeld zijn, zal de gebruiker ook daar een verwijderverzoek moeten doen. Tevens vervalt het consent na maximaal 3 maanden en worden gegevens, indien ze niet tussentijds ververst zijn, na 6 maanden uit Qii verwijderd. Voor data die al zijn gedeeld met een verhuurder moet de gebruiker een verwijderverzoek doen bij de data afnemer. Voor verhuurders zit de meerwaarde in de hogere kwaliteit van data, het versturen van de juiste data en het verlichten van administratieve lasten. Zij betalen per klant die via Qii gegevens aanlevert. Om ook gegevensverkeer te kunnen ontsluiten in use-cases waarbij een hoger authenticatieniveau gewenst of vereist is, onderzoekt Qii momenteel een samenwerking met Cleverbase.

1.7 Internationale PDM-Diensten

1.7.1 Inleiding

PDM is geen Nederlandse ontwikkeling, in tegendeel. Veel ontwikkelingen zijn gestart buiten onze grenzen, zoals OpenPDS (eerder besproken), Mydex en Project VRM²⁰⁷ dat 10 jaar geleden actueel was. Veel initiatieven zijn ook alweer gestopt. In die zin spiegelt de internationale ontwikkeling ook die in Nederland. Hierna wordt een aantal kenmerkende voorbeelden besproken. Voor een uitgebreider overzicht van buitenlandse operators, zie ook de pagina met MyData Operators²⁰⁸.

1.7.2 Geens NPO

Geens NPO²⁰⁹ is een onafhankelijk dataopslag platform voor individuen en bedrijven. De gebruiker heeft zelf volledig zeggenschap over zijn/haar data en de wijze waarop deze gedeeld wordt met derden. Geens NPO biedt een cloud platform waarop rechtstreeks of met behulp van een API-data opgeslagen kan worden door de gebruiker en gedeeld kan worden met derden. De data is end-to-end encrypted en kan ondertekend worden met een blockchain tijdstempel. Dit tijdstempel bewijst dat een document getekend is voor een bepaalde datum die eigenaarschap bevestigt.²¹⁰ Geens NPO is gestart in België en richt zich momenteel primair op de Europese markt. De service is op dit moment operationeel. Individuele gebruikers kunnen een gratis en betaald lidmaatschap afsluiten, bedrijven moeten altijd een betaald lidmaatschap afsluiten.



1.7.3 MyDex

MyDex (UK) bestaat al sinds 2007 en is daarmee een van de langst bestaande operators in het landschap. Het levert diensten aan zowel het individu als organisaties. Het individu kan persoonlijke gegevens verzamelen in een overzicht en toegang krijgen tot diensten die gebruik maken van deze gegevens. Het positioneert zich daarmee als 'kluis'. Voor organisaties zorgt MyDex dat diensten geboden kunnen worden aan personen. Partijen die toegang willen krijgen, moeten wel voldoen aan de regels die MyDex stelt. MyDex focust op dit moment met name op de publieke sector en wordt ook aangeboden via de digitale marktplaats van de Britse overheid²¹¹. In MyDex kunnen diverse datasets bewaard worden, waaronder rijbewijs, paspoort, creditcard gegevens, werkgevergegevens.²¹² Verder maakt MyDex gebruik van meerdere protocollen voor authenticatie waaronder SAML en OpenID Connect. Mydex is onder meer lid van het eerder besproken Personal Data Ecosystem Consortium, dat de ondernemers verbindt die nieuwe bedrijven opbouwen rond gebruikersgerichte persoonlijke gegevens.



²⁰⁷ https://cyber.harvard.edu/projectvrm/VRM_FAQ

²⁰⁸ <https://mydata.org/operators/>

²⁰⁹ <https://geens.com>

²¹⁰ <https://geens.com/timestamp>

²¹¹ <https://www.digitalmarketplace.service.gov.uk/g-cloud/services/457530744783729>

²¹² <https://dev.mydex.org/data-schema/datasets.html>

1.7.4 Meeco

Meeco²¹³ is een operator die in 2012 is opgericht in Australië. In augustus 2019 heeft Meeco ook een locatie in België geopend. De ambitie van Meeco is om te zorgen dat iedereen waarde krijgt uit de data die ze delen. Dit doet Meeco door te zorgen dat gebruikers gegevens veilig kunnen opslaan en uitwisselen onder consent. Op dit moment heeft Meeco met name financiële toepassingen (Personal Finance Management = PFM) en de diensten rond de uitwisseling van onroerend goed gegevens. Meeco wisselt gegevens uit middels API's. Het maakt daarnaast gebruik van onder andere OAuth, OpenID connect voor de integratie met derde partijen. Meeco maakt gebruik van gedistribueerde grootboektechnologie en Zero Knowledge Proofs om mensen in staat te stellen om hun eigen geverifieerde gegevens te verstrekken met gecontroleerde toestemming.



Voor organisaties biedt Meeco modulaire diensten om de organisatie in staat te stellen een persoonsgerichte operator voor persoonsgegevens te worden. Dit omvat een suite van API's, beveiligde data-enclave (kluis), engine voor toestemming en machtigingen, etc. Voor ontwikkelaars is er een sandbox om de mogelijkheden van de API-suite te testen en te verkennen. SDK- en acceleratortools zorgen voor een snelle en gemakkelijke integratie, met een uitgebreide ondersteunende documentatiebibliotheek.

1.7.5 Digi.me

Digi.me (UK)²¹⁴ is een voorbeeld van een operator die zich zeer breed oriënteert en niet werkt vanuit een specifieke sector. Met Digi.me kunnen data-gestuurde apps en services worden gebouwd met privacy en toestemming van de gebruiker. Personen kiezen zelf welke dienst ze willen gebruiken om de gegevens die via de app verkregen worden op te slaan (Google Drive, Dropbox, OneDrive). De gegevens die met Digi.me verzameld kunnen worden zijn divers: financieel, medisch, social, entertainment. Via Digi.me wordt bijvoorbeeld toegang gerealiseerd tot financiële transacties van duizenden banken en financiële instellingen, alle gangbare creditcards (Visa, Mastercard, American Express, Discovery). De gegevens die opgehaald kunnen worden zijn, buiten de socials en entertainment gegevens, met name gericht op het VK en de VS. Digi.me doorstond met succes het proces om MedMij geaccrediteerd te worden.

Praktijktest Verhuizen - Digi.me²¹⁵

In het kader van Programma Regie Op Gegevens van de Nederlandse overheid deed Digi.me mee aan een praktijkproef verhuizen:



- De burger dient online een officiële adreswijziging bij een gemeente in (via een bestaand onlineproces).
- De burger kan regie nemen middels de door de gemeente/BRP verstrekte data van de officiële adreswijziging op een beveiligde manier te downloaden naar de eigen digitale kluis.
- Het gedownloade document dient:
 - Voorzien te zijn van timestamping en sourcing ten behoeve van de audit trail (validated claim);
 - Niet muteerbaar te zijn door de gebruiker;
 - Vrij te zijn van "man-in-the-middle" attacks.
- De burger heeft de vrijheid om eigen data te delen met derden, conform de regelgeving zoals uiteengezet onder de AVG (EU-GDPR). Deze vorm van datadeling is gebaseerd op toestemming die de burger biedt aan de tegenpartij. Hierin is opgenomen met wie, waarom en onder welke condities, de datadeling--overeenkomst wordt aangegaan.

Kantara

Digi.me werkt nauw samen met het Kantara Initiatief in een adviserende rol aan²¹⁶. Kantara is een wereldwijde instantie zonder winstoogmerk, die zich onder andere richt op informatiestandaarden,

²¹³ <https://www.meeco.me/>

²¹⁴ <https://digi.me/>

²¹⁵ Digi.me - Eindrapportage praktijktoets Regie Op Gegevens, 2019

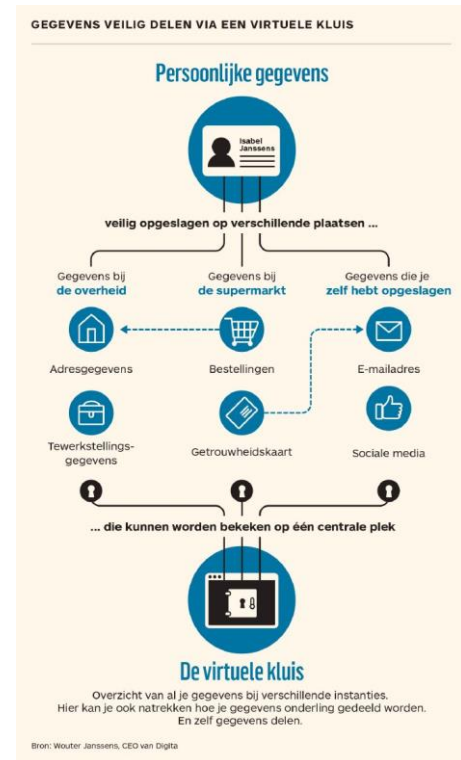
²¹⁶ Eindrapportage praktijktoets Regie op Gegevens, ICTU 2020

privacy en toestemming. Verschillende partijen hebben onlangs gewerkt aan het ontwikkelen en uitgeven van een wereldwijde ISO-norm voor toestemming en toestemmingsbewijzen.

1.7.6 Solid

Solid²¹⁷ is een ontwikkeling vanuit MIT, geleid door Tim Berners-Lee (de bedenker van het World Wide Web). Solid wordt ontwikkeld als open source technologie door het bedrijf Inrupt. Het richt zich op een totaal andere vorm van dataeigenaarschap op het web. Solid staat voor "Social Linked Data" en is een verzameling concepten en standaarden om gedecentraliseerde webapplicaties te ontwikkelen gebaseerd op Linked Data. De fundamentele achterliggende gedachte is dat data losgekoppeld moet worden van toepassingen. Nu bezitten Facebook, LinkedIn en Google persoonsgegevens en kunnen daarmee nieuwe informatie afleiden ten behoeve van bijvoorbeeld adverteerders. Dankzij Solid kan een persoon eenvoudig van de ene dienst op de andere overstappen en wordt de markt toegankelijker voor nieuwe toetreders: zij kijken immers niet tegen een enorme data-achterstand aan maar kunnen direct bouwen op persoonlijke data, onder regie van een bepaalde persoon. Dit betekent dan ook dat er fundamenteel andere bedrijfsmodellen moeten gaan ontstaan. Immers, de data zijn niet meer van de diensteneigenaar en kunnen niet worden gebruikt als inkomstenbron.

Data wordt opgeslagen in persoonlijke datadiensten, data pods, die aan de Solid specificatie voldoen. Deze kunnen door (commerciële) dienstverleners worden geleverd. Applicaties koppelen aan één of meerdere pods. Integratie tussen applicaties loopt ook via de pods; het is een volledig gedistribueerde architectuur²¹⁸.



Figuur-8: virtuele kluis Digita²¹⁹

Eind september 2020 werd duidelijk dat de Belgische overheid in zee gaat met Solid²²⁰. In de Septemберverklaring van de Vlaamse regering haalde minister-president Jan Jambon het concept van een 'datanutsbedrijf' aan. Eind 2020 loopt een testversie van het systeem, waarbij de persoonlijke data van de Vlaming in een Solid-kluis worden bewaard²²¹. In de toekomst is er in de kluis ook plaats voor andere data, zoals e-mailadressen.

Ook telecomoperatoren, banken en media zouden data kunnen deponeren in kluisen die onder beheer en controle staan van de gebruikers zelf. Het Brusselse Digita²²² maakt middleware, software die bestaande informaticasystemen doet praten met een Solid-server. Figuur-8 laat het concept van de virtuele kluis van Digita zien.

Inrupt bouwt oplossingen op basis van Solid. Inrupt zal de infrastructuur zijn waardoor Solid kan floreren, aldus Tim-Berners-Lee die zich persoonlijk voor het bedrijf inzet. Inrupt bracht eind 2020 zijn eerste product op de markt, enterprise-versie van Solid Server (ESS)²²³. Solid heeft al zo'n twintig

²¹⁷ <https://solid.mit.edu/>

²¹⁸ <https://solidproject.org/faqs>

²¹⁹ <https://www.tijd.be/ondernemen/ict/overheden-en-banken-worden-eerste-aanbieders-van-digitale-datakluisen/10255600.html>

²²⁰ <https://www.computable.nl/artikel/nieuws/overheid/7064633/250449/vlaamse-regering-haalt-mosterd-bij-tim-berners-lee.html>

²²¹ Via <https://www.vlaanderen.be/uw-overheid/mijn-burgerprofiel>

²²² <https://www.digita.ai/>

²²³ <https://www.computable.nl/artikel/nieuws/computable-next/7089321/250449/bedrijf-van-tim-berners-lee-stelt-eerste-product-voor.html>

miljoen dollar aan investeringen ontvangen, onder meer van de BBC, de Britse National Health Service, maar ook van de Vlaamse regering. De laatste is van plan om op termijn de technologie naar alle burgers uit te rollen om er documenten als rijbewijzen en huwelijksakten in op te slaan.

1.7.7 Personium

Personium is een open source 'Personal Data Store Server' en is bedoeld als basis voor organisaties om een operator mee te bouwen²²⁴. Personium is opgestart in 2008 en wordt ondersteund door Fujitsu. OpenID connect en SAML worden in Personium toegepast. Onder andere financiële gegevens, energieverbruik en social data worden verwerkt in toepassingen van Personium. Personium levert zelf geen diensten direct aan de eindgebruiker, maar kan door andere partijen gebruikt worden om een operator te bouwen. Personium is onder meer de basis van Japanse vertrouwensbanken voor persoonlijke gegevens, organisaties die het vertrouwd delen van persoonlijke gegevens met toestemming van mensen kunnen vergemakkelijken²²⁵



1.7.8 MyFairData

MyFairData (voorheen Fair&Smart) is een Frans initiatief dat sinds 2016 actief is²²⁶. MyFairData richt zich niet op een specifieke sector. Het is een dienst die opslag, veilige gegevensuitwisseling en consentmanagement biedt aan personen en organisaties. Op dit moment is MyFairData in operationele fase, het wordt met name gebruikt door publieke en organisaties in de zorg. Voor authenticatie maakt het gebruik van OpenID Connect. Gegevensuitwisseling verloopt voornamelijk middels REST API's, alleen onder consent van de persoon.



1.7.9 MyDataShare

MyDataShare²²⁷ is ontwikkeld en wordt beheerd door de Finse Vastuu Group. Dit is een data- en ICT-servicebedrijf dat publiek-private ecosystemen ontwikkelt die zijn geïnitieerd vanuit de vastgoed- en bouwsector en zijn uitgegroeid tot andere zakelijke gebieden die veel vertrouwen vragen. MyDataShare is een software-as-a-service-pakket voor het beheren van digitale identiteiten, het delen van persoonlijke gegevens en het verwerken van gerelateerde machtigingen tussen individuen en digitale diensten.



²²⁴ <https://personium.io/en/index.html>

²²⁵ Zie, bijvoorbeeld, <https://mydata2019.org/programme-page/japanese-data-banks/> voor een korte introductie over de Japanse Data Banken.

²²⁶ <http://myfairdata.com/>

²²⁷ <https://www.mydatashare.com/>

1.7.10 MyLife Digital

Consentric is een cloudgebaseerd platform²²⁸ dat zorgt voor het beheer van de verwerking van persoonsgegevens. Het levert transparantie aan de individuele deelnemers over welke gegevens zijn verzameld en voor welk doel. Het stelt het individu in staat om beslissingen te nemen over het gebruik van persoonsgegevens.

MyLife Digital werd in april 2021 overgenomen door DataGuard.²²⁹



1.7.11 Cozy

Cozy is een Frans open-source platform²³⁰. Het is gericht op het geven van regie op persoonlijke gegevens en doet dat door middel van data-connectoren en apps.



1.7.12 iGrant.io

Deze organisatie²³¹ biedt pay-per-user SaaS-oplossing met diensten om transacties met persoonlijke gegevens tussen een bedrijf en haar klanten te vergemakkelijken. De RESTful API's en SDK's kunnen eenvoudig worden geïntegreerd in een bestaande IT-infrastructuur, portals en mobiele app. Als alternatief biedt de iGrant.io-app een handig hulpmiddel voor uw klanten om al hun persoonlijke gegevens in meerdere organisaties te beheren.



1.7.13 Comuny

Comuny²³² organiseert een open, gedecentraliseerd ecosysteem voor vertrouwensdiensten voor processen zoals gegevensverificatie, multifactor-authenticatie, kredietcontroles, fraudebescherming, digitale handtekening, beveiligde apparaat status, enz.



Toepassingen zijn onder ontwikkeld voor de gezondheidssector. Centraal staat het concept van de Trust Data Operator.

1.7.14 Doccle

Missie

Doccle²³³ streeft er naar met haar nutsvoorziening digitale processen en administratie voor iedereen toegankelijk, eenvoudig en overzichtelijk te maken. Doccle wil daarbij de veiligste persoonlijke digitale document- en datakluis worden die archiveren, filteren en consulteren van documenten combineert met het uitvoeren van nieuwe vormen van betalingen, betaalhistorie bekijken etc. Om dit mogelijk te maken wordt het platform doorontwikkeld voor uitwisseling van data over sectoren heen en hieraan gekoppeld aan een netwerk van organisaties. De gemeenschappelijke klant van de organisaties staat hierbij centraal met zijn/ haar administratieve processen.

De consument wordt ontzorgd in belangrijke administratieve processen op een manier dat hij:

- Controle heeft over zijn data;
- Bestaande, relevante, informatie wordt zoveel geautomatiseerd krijgt aangeleverd;
- Dezelfde data niet telkens opnieuw aan iedere actor in een proces dient te bezorgen;
- Proactief door de belanghebbenden wordt ondersteund om noodzakelijke acties niet te vergeten en voor hem te ondersteunen door samenwerking;
- Veilige en privacy gebaseerde informatie uitwisseling heeft op basis van toestemming (consent) gedreven akkoord.

²²⁸ <https://mylifedigital.co.uk>

²²⁹ <https://www.dataguard.co.uk/consent-preference-management-platform?mld=true>

²³⁰ <https://cozy.io/en/>

²³¹ <https://www.igrant.io>

²³² <https://www.comuny.de/>

²³³ <https://doccle.be/nl/>

Doccle België

Doccle²³⁴ is in België het grootste digitale platform voor een innovatieve administratie tussen bedrijven en hun klanten en medewerkers.



Doccle heeft in België ongeveer 2,2 miljoen gebruikers en bijna alle grote bedrijven maken gebruik van het platform voor veilige digitale verzending van persoonlijke documenten. Naast bedrijven zijn ook de overheden aangesloten op deze kluis van de burger. De gebruiker kan in Doccle gratis kluizen voor zijn documenten en data afkomstig van zijn leveranciers samenbrengen en heeft mogelijkheden om contracten te ondertekenen, facturen die hij krijgt te betalen, automatische incasso te activeren, elektronische aangetekende zendingen te ontvangen. Doccle is in 6 jaar tijd marktleider geworden in België, heeft een gezond businessmodel en zet nu de stappen om voor een internationale lancering. De voornaamste redenen van het succes van Doccle is dat het samen met haar eindgebruikers en deelnemende organisaties continue wordt doorontwikkeld.

Doccle Nederland

Nederland is het eerste land om naar uit te bereiden. Naast het uitwisselen van documenten wordt het in Nederland ook mogelijk om vanuit de gratis data kluis persoonlijke data uit te wisselen. De gebruiker is baas van eigen data en blijft dit door toestemming te geven voor het doel en het gebruik van deze data. Op dit moment vindt de activatie plaats naar de verzekeringen, notariaat, makelaardij en hypotheek adviseurs. Doccle heeft de ambitie een generieke, sectoroverstijgende oplossing te bieden, daarom worden nu ook stappen gezet naar de Zorg, Telecom en Energie sector.

Nieuwe investeerder

Op 15 juni 2021 is een nieuwe aandeelhouder bij het Doccle in België toegetreden. Met de komst van deze aandeelhouder is ook het besluit genomen de komende jaren € 5 mln. In het platform te investeren²³⁵.

1.7.15 Kivra

Kivra²³⁶ is een gratis service voor interactie tussen bedrijven en consumenten. De consument kan Kivra gebruiken om naast het opslaan van documenten ook facturen te ontvangen en direct van de bankrekening te betalen. Verder kan een consument documenten digitaal ondertekenen, papieren post scannen, de boekhouding stroomlijnen, digitale ontvangstbewijzen verzenden en ontvangen.



Voor bedrijven biedt Kivra een eenvoudige manier om de bedrijfsvoering te digitaliseren en de klantervaring te verbeteren.

Het verhaal van Kivra begon in Zweden in 2011. Tegenwoordig heeft Kivra 4 miljoen gebruikers in Zweden, met meer dan 37.000 bedrijven en openbare organisaties die digitale post via de dienst verzenden. Kivra is in februari 2020 in Finland gelanceerd.

1.7.16 BitsaboutMe

BitsaboutMe²³⁷ is een Zwitsers online platform waar gebruikers hun digitale leven veilig kunnen beheren en data-deals kunnen sluiten met bedrijven en organisaties. De kern



van BitsaboutMe is de privacy van elke individuele gebruiker. De marktplaatsfunctie stelt gebruikers in staat om selecties van persoonlijke gegevens veilig te delen met bedrijven en organisaties tegen een beloning of anoniem voor onderzoeksdoeleinden.

²³⁴ <https://doccle.be/nl/business/>

²³⁵ https://doccle.be/nl/blog/Telenet_en_Isabel_Group_investeren_samen_in_Doccle

²³⁶ <https://kivra.se/en/private>

²³⁷ <https://bitsabout.me/en/>

1.7.17 Faidrop

Faidrop²³⁸ is een Sloveense open source opslagoplossing voor persoonlijke gegevens die is gericht op het bereiken van gebruikerssoevereiniteit. Door het peer-to-peer karakter is het opzetten van infrastructuur niet nodig. Er is geen centrale autoriteit. De hoeveelheid gebruikte opslagruimte kan naar behoefte worden geschaald. Een voorbeeld van een use case is de opslag van Kantara-conforme toestemmingsbewijzen in een speciale "map". Faidrop maakt gebruik van open source javascript- bibliotheken van Fair Data Society.



1.7.18 Numbers

Numbers²³⁹ uit Taiwan biedt gegevens-integriteits-garantie voor gegevensverzameling en -uitwisselingsservices. Om de gegevens-privacy beter te beschermen, kiezen veel diensten tegenwoordig voor gedistribueerde gegevensverzameling en -opslag, zoals het bewaren van de informatie op persoonlijke mobiele telefoons. Numbers helpt serviceproviders de gegevensintegriteit te beschermen met behulp van blockchain- en cryptografische technologieën.



1.7.19 Onecub

Het Franse Onecub²⁴⁰ biedt een service voor het delen van persoonlijke gegevens. De consumenten profiteren van een toestemmingsdashboard voor meer controle. Ze passen het "Separation of Powers Principle (SPP)" toe: ze slaan gegevens alleen op met het oog op toestemmingsbeheer, ze slaan overgedragen gegevens niet op.



1.7.20 OwnYourData

OwnYourData²⁴¹ uit Oostenrijk is een vereniging zonder winstoogmerk. Zij biedt verschillende diensten en producten aan – allemaal gelicentieerd als Open Source en volgens de MyData-principes.



1.7.21 Polypoly

Ontworpen en ontwikkeld door de Polypoly Cooperative uit Duitsland, kunnen gebruikers polyPod²⁴² installeren op conventionele apparaten zoals laptops en smartphones, maar ook op alle IoT-apparaten zoals slimme horloges, auto's en in de toekomst zelfs koelkasten. De polyPod slaat persoonlijke informatie op, maar het is meer dan dat: inbegrepen is een Feature Depot waarmee gebruikers verdere apps en extra functies kunnen downloaden.



1.7.22 Streamr

Streamr²⁴³ (streamr.network) is een marktplaats en gedecentraliseerd netwerk voor realtime gegevens. Streamr is in 2017 in Finland opgericht om data meer beschikbaar, eerlijk en waardevol te maken voor iedereen.



²³⁸ <https://datafund.io/>

²³⁹ <https://numberspr.tocol.io/>

²⁴⁰ <https://www.onecub.com/>

²⁴¹ <https://www.ownyourdata.eu/en/>

²⁴² <https://polypoly.org/en-gb/>

²⁴³ <https://streamr.network/>

1.7.23 VisionsTrust

Het Franse Visions biedt een tool waarmee mensen hun gegevens kunnen delen tussen verschillende diensten. Organisaties kunnen VisionsTrust²⁴⁴ API gebruiken om data te delen op een mensgerichte manier en om mensgerichte data-ecosystemen te creëren. Gebruikers hebben een onafhankelijk dashboard om hun toestemmingen voor gegevens te beheren. Visions creëert over de hele wereld mensgerichte data-ecosystemen.



²⁴⁴ <https://visionspol.eu/>

2. BIJLAGE B - PDM IN DE FINANCIËLE SECTOR

Dit hoofdstuk richt zich op de PDM-initiatieven gericht op de financiële sector:

1. Speelveld;
2. Wetgeving;
3. Technologie en standaarden;
4. Authenticatievoorzieningen;
5. Afsprakenstelsels;
6. Operators.

Speelveld	Wetgeving	Afsprakenstelsels
Autoriteiten - Autoriteit Financiële Markten - De Nederlandse Bank	- PSD2 - Wet op het financieel toezicht - Wet ter voorkoming van witwassen en financieren van terrorisme	
Belangenorganisaties - Stichting Pensioenregister - Verbond van Verzekeraars - Adfiz - NVGA - HDN - Nederlandse Vereniging van Banken - Currence - Nibud - Wijzer in Geldzaken - SchuldenLabNL - Social Fintech Alliantie - Plinkr - Stichting Financieel Paspoort - Contactgroep Automatisering - Financial Services Consumer Panel	- Hypothekenrichtlijn MCD - Pensioenwet - Wet gemeentelijke Schuldhulpverlening	
Communities en programma's - Nederlandse Schuldhulproute - Social FinTech Alliantie - Overheid - Sociale Verzekeringsbank - Stichting Bureau Kredietregistratie - Europese Commissie		
Wetenschap - Sustainable Finance Lab - Netspar - Digicampus		

Technologie/Standaarden	Authenticatie voorzieningen	PDM-Diensten
- Gegevensstandaard Persoonlijke Financiën - SIVI All Finance Standaard - Consumentendata standaard HDN - Ockto Brondata Service - Standaarden Betalingsverkeer - NextGenPSD2 Framework	- Propriëtaire voorzieningen	PDM-Diensten - Financieel Paspoort - Invers - Ockto - MijnPensioenOverzicht - iWize - Bittiq - TM-pro - IDA Planningstools - ToekomstVerkenner - APG Helder Overzicht en Inzicht - AZL pensioenplanner - TKP Planningstool - Independer Pensioenplanner - Financiële Planningstools verzekeraars: KNAB, Zwitserleven, ING Pensioenwijzer, ASR Mijn Pensioenplein app, NN Mijn Inkomen later app. - Omniplan Personal Finance Platform - Figlo - Finrust - Pensioenpod - ACTU-IT - AdviesBox Huishoudboekjes - Bank Trans - Flow Your Money - Dyme - Grip - MijnGeldzaken - Virtueel Inkomstenloket Tools schuldhulpverlening en voorkomen schulden - Buddy Payment - FiKks - Schuldwisser - Seev - MoneyFit - Krap.nl - Roos - Budlr Klantmappen/Apps financiële dienstverleners Internationale PDM-Diensten - Yolt - DataYogi - N26 Online Bankieren

Technologie/Standaarden	Authenticatie voorzieningen	PDM-Diensten
		- Swish - Satispay - Mint - Finanda - Plaid - Saltedge - Eurobits - Envestment Yodlee - MX - Finicity - Cashedge (Fiserv) - Kontamatik - Tink

2.1 Speelveld

Het speelveld rond PDM bestaat uit drijvende krachten achter de (door)ontwikkeling van technologie, standaarden, juridische kaders, oplossingen en governance rondom PDM.

Dit betreft op alfabetische volgorde:

- Autoriteiten
- Belangenorganisaties
- Communities en programma's
- Overheid
- Wetenschappelijke instituten

2.1.1 Autoriteiten

Autoriteiten zijn gezaghebbende organisaties met een formele rol in de definitie en/of naleving van gegevensverwerking.

2.1.1.1 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.



In het 2015 verscheen het rapport "Neem drempels weg opdat Nederlanders in actie komen voor hun pensioen". Een grote groep Nederlanders stevent, veelal zonder dat zij dit weten, op een pensioentekort af, aldus de AFM. De AFM doet aanbevelingen om hierop te anticiperen:

- Consumenten actief stimuleren om in actie te komen door ze periodiek een oproep te (laten) sturen om hun financiële totaalplaatje bij pensionering in kaart te krijgen.
- Het onderwerp te vergemakkelijken door de ontwikkeling van een online tool te stimuleren waar alle relevante financiële producten op één plek in kaart gebracht worden.

Uit het jaarverslag AFM 2019 blijkt dat de AFM zich richt op het identificeren en verkleinen van de belangrijkste risico's die zich voordoen op het gebied van het centraal stellen van het klantbelang (p.108). De AFM ziet erop toe dat ondernemingen hun bedrijfsvoering zodanig inrichten dat technologische ontwikkelingen in het belang van de klant zijn en geen negatief effect hebben op de beheersing van de bedrijfsvoering. (p. 117).

De laatste jaren is de richting van AFM duidelijk:

- als evident is dat het klantbelang wordt geschaad dan treedt de AFM op;
- van dienstverleners wordt vooral verwacht dat ze voorkomen dat de klant verkeerde financiële keuzes maakt;

- focus ligt op kunstmatige intelligentie en informatiebeveiliging.

2.1.1.2 De 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.

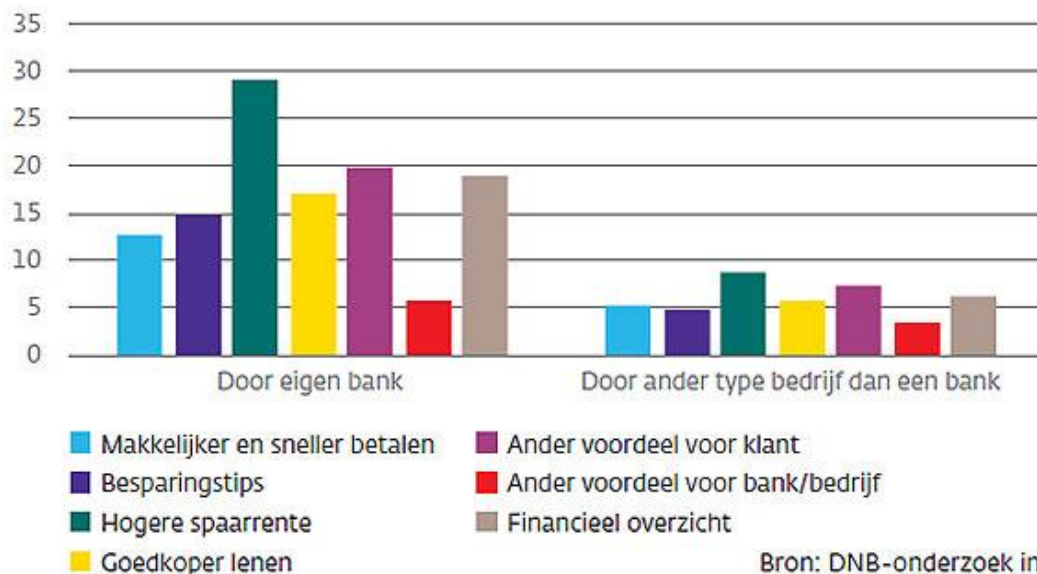
DeNederlandscheBank

EUROSYSTEEM

DNB-rapport 'Visie op de toekomst van de verzekeringssector' van december 2016, pleit de DNB voor een actieve houding van de sector rond het borgen van klantbelang: 'DNB streeft naar een duurzame, stabiele, efficiënte en maatschappelijk dienstbare verzekeringssector. De verzekeringsdienstverlening voorziet in een belangrijke maatschappelijke behoefte. Hierbij is het van belang dat de verzekeringssector duurzaam en stabiel is. Tegelijkertijd moet de sector efficiënt en maatschappelijk dienstbaar zijn. Dit betekent onder meer dat verzekeraars producten bieden die begrijpelijk zijn en voldoen aan de wensen van de klanten. Het centraal stellen van het klantbelang, passende oplossingen aanbieden en transparantie geven, vergroot het klantvertrouwen in de verzekeringsbranche'.

Volgens onderzoek²⁴⁵ van de DNB in 2019 onder 2600 consumenten is weinig animo voor delen betaalgegevens. In het onderzoek zegt gemiddeld 11% van de ondervraagden toestemming te zullen geven voor uiteenlopende vormen van datagebruik (zie Figuur-9), 72% is niet bereid dit te doen en 15% weet het nog niet, als er verschillende situaties worden voorgelegd. Zo geeft 1 op de 5 respondenten aan dat ze in zouden stemmen met het gebruik van de data om de eigen bank een overzicht te laten maken van alle rekeningen en de inkomsten en uitgaven. Voor niet-bancaire bedrijven ligt het percentage respondenten dat toegang wil geven tot de betaalrekening voor het maken van zo'n overzicht met 6% nog lager.

Procenten



Bron: DNB-onderzoek in samenwerking met CentERdata.

Figuur-9: Aandeel respondenten dat toestemming wil geven per situatie

²⁴⁵ <https://www.dnb.nl/>

De bereidheid tot het verlenen van toestemming voor het gebruik van betaalgegevens hangt af van wat daar tegenover staat. De bereidheid is het hoogst indien de eigen bank de data gebruikt en er een echt financieel voordeel voor de klant tegenover staat.

DNB²⁴⁶ geeft voorts aan dat als bigtechs, gebruik makend van PSD2, nieuwe diensten aanbieden en consumenten ervan overtuigen om hen toegang te geven tot de gegevens op hun betaalrekening, zij de data over personen en bedrijven die zij hebben combineren met betaalgegevens voor zover de Algemene verordening gegevensbescherming (AVG) dat toestaat. Dat is aantrekkelijk omdat deze gecombineerde data bijvoorbeeld inzicht kunnen geven in aankoopgedrag of kredietwaardigheid van consumenten. Banken en betaalinstanties kunnen deze data uiteraard ook gebruiken, maar beschikken niet over de informatie waar dergelijke online platformen als Google, Facebook en Apple nu al over beschikken. De betaaldata hebben daarmee nog meer waarde voor bigtechs dan voor banken en andere betaalinstanties.

Onderzoek ING

Volgens ING is gemak en vertrouwen essentieel bij adoptie Open Banking²⁴⁷. Uit onderzoek van ING blijkt dat significante groepen mensen al wel de voordelen zien van innovaties, maar terughoudend zijn in het gebruik. Zij wegen de risico's nog vaak af tegen de voordelen.

Inwoners uit het Verenigd Koninkrijk zijn het meest geneigd om iets met Open Banking te doen. Het Verenigd Koninkrijk huisvest 178 bedrijven die gelicentieerd zijn om te opereren onder Open Banking of PSD2. Nummer twee Duitsland telt er slechts 36, meer dan Frankrijk, Italië en Spanje tezamen.

2.1.2 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.

Verscheidene belangenorganisaties zijn actief op het terrein van privacy en bescherming van persoonsgegevens.

2.1.2.1 Stichting Pensioenregister

De Stichting is een initiatief uit 2008 van de Sociale Verzekeringsbank, Pensioenfederatie en Verbond van Verzekeraars.²⁴⁸ Via de website kan een persoon (vanaf 2011) zien hoeveel pensioen is opgebouwd bij Nederlandse werkgevers en wat de opgebouwde AOW-rechten zijn. Via webservices worden de gegevens opgehaald bij de pensioenuitvoerders. Kern van het systeem is Verwijsindex met Burgerservicenummers en verwijzingen naar de webservices van pensioenuitvoerders. Door inloggen met DigiD (dat is gekoppeld is aan het Burgerservicenummer van de inloggende persoon) kunnen de juiste gegevens opgehaald worden. In 2018 waren er 5,1 miljoen bezoekers, in 2019 7 miljoen bezoekers en in 2020 7,1 miljoen bezoekers. Gegevens kunnen in PDF of XML gedownload worden.



De Stichting erkent dat alleen het presenteren van gegevens op mijnpensioenoverzicht.nl niet meer voldoet aan de behoeften en verwachtingen in de huidige maatschappij. Daarom wil Stichting Pensioenregister de gegevens de komende jaren, onder de regie van de burger, ontsluiten. In 2019 is daarvoor de techniek gerealiseerd. Parallel daaraan is gewerkt aan de juridische context om deze toepassing te kunnen leveren. Op basis van de huidige taakomschrijving, mag SPR deze techniek helaas nog niet inzetten. SZW werkt aan de voorbereiding om dit met wetgeving mogelijk te maken.

²⁴⁶ BigTech bedrijven in toenemende mate actief op Europese betaalmarkten, 4 juni 2019 (DNB)

²⁴⁷ <https://www.banken.nl/nieuws/22664/ing-gemak-en-vertrouwen-essentieel-bij-adoptie-open-banking>

²⁴⁸ Stichting Pensioenregister. <https://www.pensioenregister.nl/>

Voorbeeld: API-ontsluiting gegevens uit MijnPensioenoverzicht

Stichting Pensioenregister heeft onderzocht wat de mogelijkheden zijn om een API-koppeling te maken op MijnPensioenoverzicht. Zodat burgers, wanneer ze daar expliciet toestemming voor geven, persoonlijke informatie uit het pensioenregister kunnen delen met derden. In de Pensioenwet (artikel 51) staat beschreven dat deze informatie alleen mag worden gebruikt voor het omschreven doel (gegevens over pensioen raadplegen).

Vanuit SZW is aangegeven dat er geen belemmeringen zijn wanneer een gebruiker een Xml-bestand met de gegevens downloadt. Maar wel wanneer een API-koppeling gemaakt wordt. 'Deze wettelijke taak sluit ander gebruik van de gegevens uit. Toestemming van betrokkenen gebruiken om een andere wijze van verwerking mogelijk te maken, zou neerkomen op omzeiling van de wettelijke grondslag.' Hiermee ontstaat een grijs gebied: de gebruiker mag wel handmatig de gegevens downloaden en doorsturen, echter wanneer de informatie via een API-koppeling doorgegeven wordt is dit niet toegestaan. Ook al geeft de gebruiker toestemming.

2.1.2.2 Verbond van Verzekeraars

Brancheorganisatie van schade- en levensverzekeraars.²⁴⁹ Een van de speerpunten in het middellange termijnplan (2019-2021) van het Verbond van Verzekeraars is: 'Betrouwbaar met data - voor klant en samenleving.

"Het Verbond zet zich in om te zorgen dat de privacyregels uitvoerbaar zijn en de eisen die gesteld worden niet bovenmatig en helder zijn. Ook biedt het Verbond ondersteuning aan leden bij de vertaling van de privacyregels in het eigen bedrijf."

In 2019 werd Mijnverzekeringenopeenrij uit de lucht gehaald. Uit een evaluatie na een testfase bleek dat op dat moment onvoldoende mogelijkheden bij verzekeraars aanwezig waren om de website verder door te ontwikkelen tot een volwaardige dienst en een ruime dekking aan beschikbare verzekeringen te garanderen. Mijnverzekeringenopeenrij.nl was een niet-concurrerend online platform dat de particuliere verzekeringnemer een integraal overzicht zou bieden van al zijn verzekeringen. Via Mijnverzekeringenopeenrij zou de consument een gestandaardiseerde set gegevens (op basis van het AFD) over al zijn polissen kunnen downloaden. In potentie was Mijnverzekeringenopeenrij een ideaal platform voor ROG. Via het platform zouden bijvoorbeeld mutaties in adresgegevens, telefoonnummers doorgegeven kunnen worden.



2.1.2.3 Adfiz en NVGA

Adfiz en NVGA vertegenwoordigen respectievelijk adviseurs/bemiddelaars en gevolmachtigde assurantiebedrijven. Hier zijn privacycommissies actief die ontwikkelingen voor hun leden duiden.

In 2016 kondigde Adfiz een Financiële APK te ontwikkelen, met onbekend resultaat.



Modeldocument misinterpretatie AVG²⁵⁰

Adfiz stelde dit in 2018 op.

De AVG biedt grondslagen om als aanbieder en bemiddelaar klantinformatie te delen wanneer dit:

- noodzakelijk is voor het uitvoeren van een overeenkomst,
- noodzakelijk is om te voldoen aan een wettelijke verplichting.

²⁴⁹ Verbond van Verzekeraars. <https://www.verzekeraars.nl/home>

²⁵⁰ <https://www.adfiz.nl/dossiers/privacy/>

Het vragen van toestemming van de klant om noodzakelijke en belangrijke klantinformatie met elkaar te delen is volgens Adfiz overbodig en onnodig belastend. Weliswaar is het geven van toestemming een belangrijke grondslag van de AVG, maar het is slechts een van de grondslagen, aldus Adfiz.

Advies in Cijfers (Adfiz)

Uit Advies in Cijfers 2020, een uitgave van Adfiz, blijkt financieel advies steeds vaker buiten bereik te geraken van kwetsbare groepen zoals financieel laag geletterden en huishoudens met een laag inkomen. Zo geeft meer dan 60% van huishoudens met een laag inkomen aan advieskosten niet te kunnen betalen. En kiezen 2,5 keer zoveel huishoudens met weinig financiële kennis voor financieel doe-het-zelven doordat ze opzien tegen de advieskosten.



Financiële laag geletterdheid is volgens Adfiz bovendien een omvangrijk probleem. Uit verschillende (internationale) onderzoeken blijkt dat 40% van de consumenten niet weet wat bepaalde financiële basisbegrippen betekenen.

Dit alles draagt eraan bij dat volgens Adfiz 70% van de Nederlandse huishoudens enige financiële zorgen heeft en 20% met betalingsproblemen kampt. Die problemen beperken zich niet tot lage inkomens, want ook bij werknemers met een salaris boven de 65.000 euro geeft één op de vijf aan van loonstrook naar loonstrook te leven. Die financiële zorgen zijn niet alleen op persoonlijk vlak een probleem, maar ook maatschappelijk en voor werkgevers. Een werknemer met financiële problemen die voltijds werkt en een modaal salaris verdient, kost een werkgever gemiddeld 13.000 euro per jaar. Kosten die veroorzaakt worden door de gevolgen van stress: verminderde concentratie, lagere productiviteit en een hoger verzuim. Op jaarbasis hebben we het dan, omgerekend naar de hele beroepsbevolking, over een kostenpost van ruim 8 miljard euro voor werkgevers. Er is dus volgens Adfiz kortom een groot maatschappelijk belang om toegangsdrempels tot financieel advies weg te nemen.

Data delen

Adfiz en Tulp Hypotheken namen eind 2019 het initiatief genomen voor het Convenant Data Delen hypotheken²⁵¹. Hierin staan duidelijke en heldere afspraken over het delen van klantinformatie. Adfiz ontwikkelde een standaardmachtiging om namens de klant (persoons)gegevens op te vragen of te wijzigen bij een aanbieder. Rabobank accepteerde deze in augustus 2020²⁵².

Actief Klantbeheer²⁵³

Het 'Manifest Actief Klantbeheer' is op 1 juli 2021 tijdens een bijeenkomst in Diemen getekend doormarktpartijen: ABN Amro Intermediaire Distributie, Adfiz, Dukers & Baelemans, FlexFront, Helder Beheerd, Nationale Hypotheekbond, Obvion, Vereniging EigenHuis en VVP. Actief klantbeheer is in dit verband het totaal aan activiteiten dat bijdraagt aan de financiële gezondheid van klanten.

2.1.2.4 Pensioenfederatie

Overkoepelende belangenbehartiger van bijna alle Nederlandse Pensioenfondsen. Oriënteert zich momenteel onder meer op het vraagstuk rond zorgplicht en zorgambitie. Vanaf 2018 heeft SIVI een samenwerkingsovereenkomst met de Pensioenfederatie. De projecten en het beheer van Uniforme Pensioenaangifte worden aangestuurd vanuit een stuurgroep met pensioenuitvoeringsorganisaties (Achmea, APG, AZL, MN, PGB Pensioendiensten, PGGM, TKP). Voorts worden projecten uitgevoerd samen met pensioenverzekeraars.



In 2019 werd onderzoek uitgevoerd naar financiële planningstools. In de markt zijn meerdere tools ontwikkeld die pensioendeelnemers inzicht geven in hun financiële situatie zowel voor als na pensionering. De tools voorzien tevens in de mogelijkheid waarmee de deelnemers een beeld krijgen van de effecten van keuzes die zij kunnen maken. De vraag is of, en op welke wijze, de

²⁵¹ <https://www.adfiz.nl/nieuws/adfiz-berichten/adfiz-en-tulp-hypotheek-ondertekenen-convenant-data-delen-hypotheek/>

²⁵² <https://www.vvponline.nl/nieuws/rabobank-accepteert-modelmachtiging-adfiz>

²⁵³ <https://www.actiefklantbeheer.nl/assets/files/manifest.pdf>

Pensioenfederatie hierin moet/kan interveniëren. Interventies kunnen variëren. Bijvoorbeeld van niets doen (marktwerking), het ontwikkelen van standaarden (bijvoorbeeld voor berekeningen en het presenteren van de gegevens), tot het gezamenlijk ontwikkelen van de “achterkant” van een tool. Het onderzoek keek naar de interventiemogelijkheden, vooral naar de voor- en nadelen en de impact ervan voor de stakeholders (pensioenfondsen, deelnemers, toezichhouders etc.).

Het onderzoek kreeg vorm door deskresearch om het landschap en de ontwikkelingen in kaart te brengen en diepte-interviews.

De deelnemers aan het onderzoek geven duidelijk aan van de Pensioenfederatie te verwachten dat zij een regierol gaan spelen om de ontwikkelingen rond financiële planningtools positief te beïnvloeden. Er zijn zes opties bij het standaardiseren van de achterkant onder regie van de stuurgroep:

1. Het door pensioenuitvoerders en/of -fondsen gezamenlijk (laten) ontwikkelen van een eigen data-aggregator. Het gezamenlijk ontwikkelen van een data-aggregator brengt voordelen met zich mee, in potentie ook met kostenvoordelen voor de sector. Dit stelt echter dermate hoge eisen aan het draagvlak en de governance, dat verder onderzoek vereist is. Investerings over meerdere jaren zijn nodig en het vereist het oprichten/bemannen van een aparte organisatie die losstaat van de bestaande organisaties.
2. Het uitwerken van scenario's die van invloed zijn op het inkomen op pensioenleeftijd en het opstellen van gestandaardiseerde rekenregels.
3. Opstellen van een catalogus voor databronnen.
4. Realiseren van randvoorwaarden om databronnen via standaarden te ontsluiten.
5. Afdwingen van gemak en veiligheid bij inloggen (authenticatie).
6. Opstellen van een gestandaardiseerd begrippenkader.

Er is behoefte aan meer guidance over de zorgplicht waar pensioenfondsen en –uitvoerders mee te maken hebben. Enerzijds is er onduidelijkheid over de huidige reikwijdte van de zorgplicht (wat moet je minimaal doen?) en anderzijds is er discussie over de mogelijkheden die er zijn om deelnemers te activeren (hoever mag je gaan?).

2.1.2.5 HDN

Hypotheek Data Netwerk is een coöperatieve vereniging zonder winstoogmerk. De organisatie is gericht op het leveren van informatie-uitwisseling voor financiële dienstverlening via een goed beveiligd netwerk.



Dit doet HDN door beheer, onderhoud en doorontwikkeling het HDN-platform en berichtstandaarden. HDN werkte onder meer samen met iWize en Ockto om de Consumentendata standaard te ontwikkelen²⁵⁴. Het ontsluiten van data uit verschillende bronnen, versnelt het hypotheek-aanvraagproces.

Opdracht tot datauitwisseling

Diverse adviesketens werken begin 2020 met een door de klant ondertekende ‘opdracht tot datauitwisseling’. Hierin verzoekt de klant de geldverstrekker om in zijn belang de data actief aan te dragen bij de adviseur. Met de opdracht voeren de ketens de druk op geldverstrekkers op om data uit te wisselen in het kader van de zorgplicht van de adviseur. De ketens in kwestie zijn CMIS Franchise (De Hypotheekshop, Huis & Hypotheek, Hypokeur), Financieel Fit Groep, Finzie, Geld & Woning, Hypotheek Visie en Van Bruggen Adviesgroep. (<https://www.vvponline.nl/nieuws/data-uitwisseling-adviesketens-zetten-geldverstrekkers-onder-druk>)

2.1.2.6 Nederlandse Vereniging van Banken

Inleiding

Behartigt belangen van Nederlandse²⁵⁵ en buitenlandse banken die in Nederland actief zijn. ‘Bank en Data’ is een prominent thema van de NVB. Een van de speerpunten in de middellange termijn agenda is ‘de gegevens van onze klanten en partijen verbinden in een nieuw financieel ecosysteem.’

²⁵⁴ <https://www.hdn.nl/nieuwe-toepassing-van-de-consumentendata-standaard-live/>

²⁵⁵ <https://www.nvb.nl/>

Visie

Highlights uit de visiedocumenten van de NVB²⁵⁶:

- Data – de toegang tot en het delen ervan – zijn van toenemend economisch belang voor de economie.
- Verantwoord datagebruik is belangrijk. De toegang tot data en het delen van data – op initiatief van de consument – moet veilig, gestandaardiseerd en transparant gebeuren. Zodat mensen zelf bepalen wat er gebeurt met hun gegevens²⁵⁷.
- Banken ontwikkelen handige tools waarmee klanten meer grip krijgen op hun geldzaken. Bijvoorbeeld apps voor een beter inzicht in inkomsten en uitgaven.
- Banken zorgen dat digitale diensten toegankelijk zijn voor mensen met een visuele of auditieve beperking.
- De markt voor digitale financiële diensten is veel breder geworden. Niet alleen banken, maar ook partijen zonder bankvergunning, zoals fintechs en bigtechs, bieden financiële diensten aan of willen dat doen. Bijvoorbeeld op het gebied van betalen, sparen en beleggen.
- De financiële sector kent dankzij de digitalisering veel nieuwe toetreders. Bijvoorbeeld nieuwe banken die uitsluitend digitaal werken. Maar ook niet-bancaire spelers - zoals bigtechs, Third Party Providers en nieuwe leenplatforms - bieden concurrerende financiële diensten in de EU aan, steeds vaker grensoverschrijdend. Dit is de ambitie van de Europese digital single market. Nieuwe partijen met de juiste vergunning uit een EU-land, mogen via een Europees 'paspoort' ook in Nederland financiële producten en diensten aanbieden. Zulke aanbieders moeten zich houden aan de wet- en regelgeving van het EU-land dat het 'paspoort' heeft verstrekt. Die regels kunnen verschillend en soms minder strikt zijn dan in Nederland. Dat leidt volgens de NVB tot oneerlijke concurrentie. Daarom pleiten banken voor meer Europese harmonisatie van het toezicht²⁵⁸.
- De nieuwe spelers die volledig digitaal werken en zich richten op technisch onderlegde (tech-savvy) klanten, hoeven zich geen zorgen te maken over toegankelijkheid voor kwetsbare klantgroepen. Daardoor bestaat het risico dat traditionele banken onevenredig worden belast met de maatschappelijke zorg voor Nederlanders die moeite hebben met digitale financiële dienstverlening²⁵⁹.



Data governance organisatie

De praktische invulling van een 'data governance organisatie', en daarmee de vereisten en standaarden, kan volgens de NVB in principe tussen marktpartijen worden vastgesteld. Hierin moeten zowel data-gebruikers als data-eigenaren zijn vertegenwoordigd. Bestaande afsprakenstelsels in het betalingsverkeer kunnen hiervoor als voorbeeld dienen.

Binnen een afsprakenstelsel worden afspraken vastgelegd over technische standaarden. Maar ook over rechten en plichten van de verschillende partijen over en weer. Naast de belangen van de data-gebruikers, kunnen ook de rechten van de data-eigenaren eenduidig worden vastgelegd. Dit leidt tot een versterking van de positie van consumenten, omdat zij collectieve afspraken kunnen maken met data-gebruikers.

Aangewezen toezichthouders moeten toezicht op deze entiteit houden op het gebied van gegevensbescherming, consumentenbescherming en eerlijke concurrentie. Daarnaast is het voor de ontwikkeling van de Digital Single Market vooral van belang dat toezichthouders dezelfde regels en voorwaarden hanteren in de diverse Europese landen.

De Nederlandse Vereniging van Banken vindt dat de meest efficiënte wijze in de markt tot stand kan komen, middels een afsprakenstelsel – een zogenaamd scheme – zoals ook bekend in het betalingsverkeer. In een scheme maken marktpartijen afspraken over contractuele verhoudingen/business model, de governance en het gebruik van standaarden voor efficiënte en

²⁵⁶ <https://www.nvb.nl/themas/digitalisering/>

²⁵⁷ <https://www.nvb.nl/themas/digitalisering/banken-in-de-data-economie/>

²⁵⁸ <https://www.nvb.nl/themas/digitalisering/toezicht-in-de-digitale-wereld/>

²⁵⁹ Digitaal met de mens centraal - Banken in de 21ste eeuw, NVB 2020

veilige implementaties. Voorstellen uit de Euro Retail Payments Board (ERPB) binnen de Working Group on SEPA API Access Scheme²⁶⁰ vormen een verkenning voor een dergelijk scheme.

Bij cross-sectorale data-deling zullen vergunnings- of accreditatie-eisen per sector kunnen verschillen. Vergunningsverplichting van partijen voor data-deling zoals in PSD2 is niet per sé noodzakelijk voor data-deling; de AVG is van toepassing op alle spelers in alle sectoren. Data-deling moet uitgaan van allen-op-allen (sectoren) principe en zou van toepassing moeten zijn op zowel de private als publieke sector. In principe zouden er geen uitzonderingen moeten zijn voor data-gebruikers onder de reikwijdte van de AVG. Wel kan proportionaliteit van belang zijn om kleine marktpartijen vrij te stellen van aansluiting op een scheme: een vorm van 'comply or explain' voor kleine bedrijven is te overwegen.

De bouwblokken van een scheme voor data-deling zijn:

- een afsprakenstelsel voor aangesloten derde partijen;
- eisen aan interoperabiliteit en standaardisatie, zoals een API-framework;
- opzetten van scheme owner organisatie, voor governance, naleveringscriteria, standaarden, business rules, documentatie, stakeholder-communicatie, promotie, fraudepreventie, klachtafhandeling;
- ruimte voor een businessmodel met (wederzijdse) vergoedingen;
- consent (authenticatie/autorisatie/verificatie) mechanismen die de gebruiker controle geven over zijn data en overzicht geven van afgegeven consents – met mogelijkheid tot wijzigen en intrekken;
- eisen aan beschikbaarheid (near real-time, uptime) en veiligheid van de online toegang.

Ook in "De overheid als partner bij datadelen, een verkenning naar de rol van de overheid bij datadeelsystemen"²⁶¹ (2020) wordt gepleit voor een publiek/privaat afsprakenstelsel.

2.1.2.7 Betaalvereniging Nederland

De Betaalvereniging²⁶² coördineert de gemeenschappelijke taken van haar leden op het gebied van infrastructuur, standaarden en gezamenlijke productkenmerken in het betalingsverkeer.



Roadmap 2020-2022

In de "Roadmap 2020-2022" stelt de Betaalvereniging de vraag of consumenten in de regel voldoende beseffen waarvoor zij precies toestemming geven als zij derde partijen toegang geven tot persoonsgegevens, waaronder betaalrekeninginformatie. Verschillende partijen zullen de consument hiertoe proberen over te halen door hem (gratis) online diensten, kortingen of andere voordelen in het vooruitzicht te stellen. Veel consumenten realiseren zich daarbij niet dat zij in die gevallen, in plaats van met geld, met hun persoonlijke data betalen. Hoe meer privacy de consument prijsgeeft, des te vaker hij gebruik kan (blijven) maken van gratis onlinediensten. Veel online platforms baseren hun verdienmodel in meer of mindere mate op handel in persoonsgegevens.

Dashboards voor betaalrekeninghouder

Verschillende banken hebben, mede op verzoek van het Maatschappelijk Overleg Betalingsverkeer en de Tweede Kamer, 'dashboards' ingericht waarmee zij de betaalrekeninghouder via de online bankomgeving overzicht biedt aan welke derde partijen hij of zij toestemming heeft gegeven om betaalrekeninggegevens te ontvangen.

DNB gaf, via Open Boek Toezicht op haar website aan een bank haar klanten een overzicht mag bieden van de door de klant gegeven toestemmingen aan betaalinitiatie- en rekeninginformatiedienstverleners. Ook mag een bank de klant binnen dit overzicht op neutrale wijze de mogelijkheid bieden de gegeven toestemming in te trekken. Bij het intrekken van een gegeven toestemming moet de bank de betaalinitiatie- of rekeninginformatiedienstverlener hierover informeren via een gestandaardiseerde notificatie op de gebruikte interface.

²⁶⁰ Report from the ERPB WG on a SEPA API Access Scheme

²⁶¹ <https://ibestuur.nl/podium/de-overheid-als-partner-bij-datadelen>

²⁶² <https://www.betalvereniging.nl/over-ons/>

Overstapservice

De Overstapservice²⁶³ maakt veranderen van betaalrekening naar een andere bank eenvoudiger en zorgt ervoor dat het betalingsverkeer soepel doorloopt. De dienst leidt 13 maanden lang bij- en afschrijvingen van de oude betaalrekening door naar de nieuwe of bestaande betaalrekening bij een andere bank. Ook worden bedrijven die incasso's zenden automatisch geïnformeerd. Jaarlijks maken er in totaal ca. 80.000 consumenten en bedrijven gebruik van de Overstapservice. In het interbancaire Convenant Overstapservice, dat wordt beheerd door de Betaalvereniging, staan de afspraken die in dit kader zijn gemaakt.

2.1.2.8 Currence

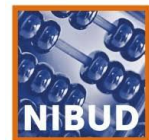
De missie van Currence is het faciliteren van marktwerking en het creëren van transparantie in het collectieve betalingsverkeer in Nederland en het behouden en verder ontwikkelen van de kwaliteit, veiligheid en efficiency van de collectieve betaalproducten. Currence doet dat door een helder en gelijk speelveld te bieden voor iedere partij die met de door Currence gevoerde betaalproducten Acceptgiro, iDEAL en Incassomachtigen wil werken.



2.1.2.9 Nibud

Het Nibud²⁶⁴ is een onafhankelijk voorlichtingsinstituut over de huishoudportemonnee. Doel is dat consumenten meer grip op geld krijgen. Hiertoe zijn onder andere rekentools ontwikkeld.

Het Nibud is tevens onderzoeksbureau op het gebied van huishoud-financiën en biedt onder andere referentiecijfers die inzicht geven in geldzaken van Nederlanders.



2.1.2.10 Wijzer in geldzaken

Wijzer in geldzaken²⁶⁵ is een initiatief van het ministerie van Financiën, waarin partners uit de financiële sector, de wetenschap, de overheid en onderwijs-, voorlichtings- en consumentenorganisaties hun krachten bundelen om samen de financiële fitheid van Nederlanders te verbeteren. Onderzoek van Wijzer in geldzaken naar verantwoord financieel gedrag, vormt de grondslag voor de (toekomstige) activiteiten van het platform.



2.1.2.11 SchuldenLabNL

De stichting SchuldenLabNL²⁶⁶ werkt samen met publieke en private partners om samen te werken aan minder schuldzorgen in Nederland. SchuldenLabNL werkt aan een landelijk netwerk van lokale Schuldenlabs. In zulke lokale Schuldenlabs ontstaan projecten die ook in andere gemeenten te gebruiken zijn. Tegelijkertijd helpt



SchuldenLabNL gemeenten ook om een eigen project op te schalen. Als dat succesvol is, kan het vervolgens landelijk uitgerold worden. SchuldenlabNL ondersteunt met:

- Financiële expertise - kennis op het gebied van subsidies, commerciële investeringen, leningen tegen lage rentes, constructies met borgstellingen en allerlei vormen van impactinvesteringen;
- Data-analyse - Dit is nodig om bijvoorbeeld effectmeting te organiseren en de impact vast te kunnen stellen;
- Implementatie-expertise;
- Juridische expertise;
- Inhoudelijke expertise - SchuldenLabNL heeft inzicht in het mogelijk combineren van projecten. Door 'matchmaking' kunnen zo lokale initiatieven elkaar versterken en aanvullen;
- Inzet bij projectmanagement en communicatie;
- Inzet van netwerk/contacten.

²⁶³ Zie voor meer informatie: <https://www.overstapservice.nl/>

²⁶⁴ <https://www.nibud.nl/>

²⁶⁵ <https://www.wijzeringeldzaken.nl/platform-wijzeringeldzaken/platform-wijzer-in-geldzaken/>

²⁶⁶ <https://www.schuldenlab.nl/>

De Nederlandse Schuldhulproute wordt gemonitord en geaccrediteerd door het onafhankelijke SchuldenLabNL.

2.1.2.12 Social Fintech Alliantie²⁶⁷ (SFA)

Een social fintech is een organisatie die financiële technologie ontwikkelt met een maatschappelijke doelstelling. Leden die zijn aangesloten bij de SFA zetten zich specifiek in om met fintech schulden en geldzorgen tegen te gaan.

Leden van de Social Fintech Alliantie ontwikkelden ieder een eigen oplossing. Onderstaand overzicht laat zien met welk doel deze oplossingen worden ingezet.

- Het Plinkr Platform helpt hulpverleners en inwoners om samen de thuisadministratie te verbeteren. De Plinkr Hub helpt gemeenten om de uitstroom uit bewind te vergroten.
- De app fiKks helpt mensen met betalingsachterstanden door ze te koppelen aan digitale buddy's.
- De Buddy-app is een mobiel platform dat internetbankieren en budget coaching combineert voor het financieel stabiliseren van kwetsbare Nederlanders.
- Inforing levert aan circa 120 gemeenten ICT-oplossingen voor de vroegsignalering van schulden
- Met Mijn Intake levert de hulpvrager m.b.v DigiD en PSD2 veilig de informatie aan voor schuldhulp, waarna MijnIntake de informatie ordent voor de hulpverlener.
- Buyproxy biedt organisaties de ondersteunende technologie om nieuwe diensten aan te bieden gebaseerd op geoormerkt geld. Deze techniek kan in de gehele keten worden ingezet.
- Seev is een digitale oplossing die organisaties helpt om schulden bij jongeren te voorkomen
- Initiatiefnemer Purpose heeft een faciliterende rol om werk te maken van de doelstellingen van de alliantie.

Oplossing	Preventie	Vroeg signalering	Aanmelding	Hulp verlening	Nazorg
Plinkr					
fiKks					
Buddy					
Inforing					
Mijn Intake					
Buyproxy					
Seev					

2.1.2.13 Plinkr

Plinkr²⁶⁸ noemt zich een sociale onderneming, is aangesloten bij Social Enterprise NL, en richt zich op mensen met schulden. Plinkr ontwikkelt digitale hulpmiddelen – waaronder een hub - voor de financiële hulpverlening. Financiële hulpverleners kunnen ook gebruik maken van vergelijkers om mensen met schulden bij te staan.



2.1.2.14 Stichting Financieel Paspoort

De Stichting Financieel Paspoort is ontstaan vanuit de denktank 2015 van het PensioenLab en is een initiatief van burgers voor burgers en wil positief bijdragen aan maatschappelijk welzijn. Daarbij is financiële zelfredzaamheid essentieel. Door nauw samen te werken met diverse organisaties streeft de Stichting Financieel Paspoort voor verbinding en passende oplossingen voor alle partijen na. Hierbij brengt de Stichting Financieel Paspoort niet alleen de belangen van de burger in, maar vooral ook de rechten van de burger.



De Stichting Financieel Paspoort streeft vanaf 2016 een digitaal financieel ecosysteem na waarin de burger – gedurende opeenvolgende levensfasen - op een vertrouwde manier regie voert over zijn persoonlijke gegevens in het algemeen en zijn financiële gegevens in het bijzonder. Deze gegevens kunnen door deze burger ter beschikking gesteld worden aan diensten die in zijn/haar voordeel zijn.

²⁶⁷ <https://www.socialfintech.nl/>

²⁶⁸ <https://plinkr.nl/over-plinkr/>

2.1.2.15 Contactgroep Automatisering

De Stichting Contactgroep Automatisering (CGA), is opgericht in 2016. Deelnemers aan de CGA zijn ondernemingen die zich richten op het verzorgen van advies-, administratie-, communicatie-, en ondersteunende applicaties voor financiële dienstverleners. Op dit moment maken 24 partijen deel uit van de Stichting. De CGA heeft twee primaire doelstellingen:



Bij meer dan 95% van de financieel dienstverleners in Nederland wordt momenteel gebruik gemaakt van één of meer applicaties van deelnemers aan de CGA²⁶⁹.

De exacte doelstellingen van de CGA staan op <https://www.contactgroepautomatisering.nl/>
De doelstellingen kunnen als volgt worden samengevat:

- Centraal platform
Fungeren als centraal platform voor partijen die in overleg willen treden met leveranciers van software, zoals die bij financieel dienstverleners wordt gebruikt. Het gaat hierbij om partijen zoals AFM, Adfiz, HDN, Ministerie van Financiën, SIVI, Verbond van Verzekeraars, etc.
- Inspiratie
Het vergroten van de bewustwording bij financieel adviseurs van de gevolgen die de digitalisering van de financiële sector voor de bedrijfsvoering van deze adviseurs gaat hebben en inspiratie geven aan adviseurs om digitalisering te omarmen. Tevens zullen waar mogelijk initiatieven worden ondernomen om financieel adviseurs te stimuleren tijdig en op de juiste wijze hun bedrijfsvoering aan te passen.

De CGA heeft data uitwisseling (Data Exchange) aangemerkt als kernonderwerp en heeft een werkgroep data exchange²⁷⁰. Vanuit deze werkgroep is het idee voor een generieke 'datacontainer' ontstaan waarmee databestanden van elk formaat in welke branche dan ook uitgewisseld kunnen worden. Om dit te realiseren geeft CGA voorlichting over het belang van branche overstijgende 'data exchange' en hoe dit te realiseren.

Delen van klantdata tussen aanbieder en adviseur²⁷¹

De CGA-voorzitter pleitte in het voorjaar van 2021 voor een uniforme overeenkomst van opdracht met gestandaardiseerde uitsluitingen en disclaimers.

2.1.2.16 Financial Services Consumer Panel²⁷²

Dit panel adviseert de Financial Conduct Authority (FCA) vanaf de vroegste stadia van haar beleidsontwikkeling om ervoor te zorgen dat zij rekening houdt met de belangen van de consument. In 2018 publiceerde het Panel bijvoorbeeld een rapport "Report on a study of how consumers currently consent to share their financial data with a third party"

2.1.3 Communities en programma's

De ontwikkeling van technologie, standaarden en juridische kaders worden veelal gedreven door communities en programma's in het speelveld van regie op persoonlijke gegevens. Deze groepen zijn een drijvende kracht achter veel initiatieven, maar zijn zelf niet als bijvoorbeeld 'PDM-Dienst' of technologie te beschrijven. Denk hierbij aan een community als MyData Global of het overheidsprogramma ROG (dat eerder is besproken). Dit soort netwerken en programma's worden door betrokkenen van groot belang geacht om regie op persoonlijke gegevens te realiseren.

²⁶⁹ <https://solera.nl/nieuws-1/persbericht-stichting-contactgroep-automatisering>, 16 juni 2020

²⁷⁰ <https://www.contactgroepautomatisering.nl/assets/files/persbericht-stichting-contactgroep-automatisering-data-exchange-cruciaal-doel-voor-de-financi.pdf>

²⁷¹ <https://www.vvponline.nl/nieuws/cga-voorzitter-schetst-oplossing-problematiek-delen-klantdata>

²⁷² <https://www.fs-cp.org.uk/consumer-panel/what-panel>

2.1.3.1 De Nederlandse Schuldhulproute

In de Nederlandse Schuldhulproute²⁷³ werken gemeenten, partners uit het schuldendomein en bedrijven krachtig samen om schuldzorgen te voorkomen.

Pilot Samen schuldzorgen voorkomen

In de pilot vroegsignalering schulden werken vier banken (ABN AMRO, ING, Rabobank en De Volksbank) samen met partners uit het schuldendomein in vijf gemeenten. Banken kunnen (beginnende) financiële problemen identificeren op basis van rekeningdata. Op basis daarvan worden mensen gewezen op passende hulp. Het doel hiervan is het aanpakken van financiële problemen, wanneer deze nog klein zijn.

Aegon, Nationale-Nederlanden en a.s.r. starten samen met de Nederlandse schuldhulproute een pilot om klanten met geldproblemen sneller de juiste weg te wijzen. Vanaf 1 september 2020 verwijzen de drie verzekeraars klanten waarvan ze vermoeden dat deze in de financiële problemen zitten, actief door naar Geldfit.nl²⁷⁴. De organisatie Geldfit²⁷⁵ helpt mensen om hun geldzaken fit te krijgen of fit te houden. Op de gelijknamige site (geldfit.nl) kan de bezoeker een gratis test doen die maar vijf minuten van je tijd kost en nog een persoonlijk advies oplevert ook, waarbij zoveel mogelijk wordt doorverwezen naar lokale hulp.

Het grootste pensioenfonds van het land ABP ging in de zomer van 2021 een samenwerking aan met de Nederlandse Schuldhulproute. Dit initiatief heeft als doel om Nederlanders preventief uit de schulden te houden²⁷⁶.



2.1.3.2 Social FinTech Alliantie (SFA)

De Social FinTech Alliantie²⁷⁷ (SFA) is begin oktober 2020 opgericht. Het brengt een aantal 'sociale' technologiepartijen bij elkaar die nauwer willen samenwerken om betere hulpverlening in het schuldendomein te kunnen bieden. De alliantie wil versnippering van digitale oplossingen voorkomen en de samenhang in de oplossingen versterken. Dit met als doel om de juiste digitale hulp voor eenieder met geldzorgen mogelijk te maken. Hierbij zijn drie speerpunten geformuleerd:

1. Een duidelijk overzicht voor gemeenten, hulporganisaties en bedrijven met zorgplicht over het aanbod van de verschillende sociale technologiepartijen.
 2. Drempelloze, digitale hulp: meer samenwerking en samenhang tussen digitale oplossingen van de partijen aangesloten bij de SFA.
 3. Digitale inclusiviteit: iedereen moet toegang kunnen krijgen tot digitale hulp bij geldzorgen.
- Aangesloten partijen zijn onder andere Buddy Payment en FiKks.



2.1.4 Overheid

2.1.4.1 Sociale Verzekeringsbank (SVB)

De SVB²⁷⁸ voert de volksverzekeringen uit in Nederland. Waaronder de AOW en de Algemene nabestaandewet, Wet langdurige zorg en Kinderbijslag. SVB levert gegevens over opgebouwde AOW-rechten aan het Pensioenregister.



²⁷³ <https://nederlandseschuldhulproute.nl/>

²⁷⁴ https://www.verzekeraars.nl/publicaties/actueel/verzekeraars-starten-pilot-schuldhelp?utm_medium=email

²⁷⁵ Vanaf de zomer 2020 gaat Geldfit Nederland verder als Nederlandse Schuldhulproute (NSR).

²⁷⁶ https://www.amweb.nl/pensioen/nieuws/2021/07/abp-schiet-mensen-met-financiele-problemen-te-hulp-101130935?utm_source=Vakmedianet_red&utm_medium=email&utm_campaign=20210803-am-signalen-pensioen&tid=TIDP5166338X29A3BFB5C21F4C289B3613F30A54ACB4YI4&utm_content=Email

²⁷⁷ <https://www.socialfintech.nl/sfa-doelstellingen>

²⁷⁸ <https://www.svb.nl/>

2.1.4.2 Stichting Bureau Krediet Registratie (BKR)

Kredietverstrekkers zijn wettelijk verplicht om elke lening aan te melden bij Stichting BKR, waarna zij deze opnemen in het Centraal Krediet Informatiesysteem (CKI).

Zo'n 11 miljoen mensen staan bij Stichting BKR geregistreerd. Alleen leningen met een waarde van € 250,- of hoger staan geregistreerd²⁷⁹. Studieleningen en hypotheekleningen worden niet bij BKR vastgelegd.

BKR is al met al een belangrijke databron voor schuldgegevens, met name om kredietverstrekkers inzicht te geven in de financiële situatie van een persoon. Een persoon kan na een inlog met iDIN zijn/haar gegevens opvragen.



2.1.4.3 Europese Commissie

In maart 2018 heeft de Europese Commissie²⁸⁰ een actieplan voor Fintech aangenomen om een meer concurrerende en innovatieve Europese financiële sector te stimuleren. Het actieplan maakt deel uit van de inspanningen van de Europese Commissie om een interne markt voor financiële diensten aan consumenten tot stand te brengen.



2.1.5 Wetenschappelijke instituten

De wetenschap stimuleert de publieke en politieke meningsvorming over privacy en bescherming van persoonsgegevens.

2.1.5.1 Sustainable Finance Lab (SFL)

Het Sustainable Finance Lab (SFL) is een informeel netwerk van merendeels academici van verschillende disciplines en universiteiten in Nederland die lid zijn op persoonlijke titel. Het SFL is in 2011 opgericht op initiatief van de hoogleraren Herman Wijffels en Klaas van Egmond van de Universiteit Utrecht en Peter Blom van de Triodos Bank. Een van de doelstellingen is individuele controle en soevereiniteit over persoonlijke financiële gegevens.



2.1.5.2 Netspar

Vanaf 2005 wijdt Netspar zich aan het bevorderen van een beter begrip van de economische en sociale gevolgen van pensioenen, vergrijzing en 'de oude dag' in Nederland. Dat doet Netspar via kennisontwikkeling en kennisdeling. Netspar zorgt voor onafhankelijk wetenschappelijk onderzoek en deelt dat in publicaties en met evenementen, Webinars en onderwijs.

Towards integrated personal financial planning, Netspar Design paper 117²⁸¹

Het doel van dit paper is om de informatie gerelateerde barrières voor persoonlijke financiële planning (inzicht, overzicht en handelingsperspectief) in kaart te brengen en ontwerprichtlijnen te introduceren die bij toepassing ervan mensen beter in staat stellen om op eenvoudige en veilige wijze gegevens op te halen en te delen ten behoeve van de eigen financiële planning.

Op basis van de 'design science' onderzoeksmethode is een spectrum van barrières geïdentificeerd voor het verzamelen en gebruiken (zelf financieel plannen) van persoonlijke gegevens of die te delen met dienstverleners.

De barrières voor burgers/klanten zijn:

- met name het niet weten waar te beginnen,
- meerdere informatiebronnen (meestal achter mijn-portalen),
- het moeten beheren van meerdere digitale identiteiten (voor toegang via mijn-portalen),
- de tijdrovende zoektocht naar gegevens (papier en digitaal),
- het handmatig gegevens overtypen in verschillende portalen (of apps),
- de noodzaak van handtekeningen op papier,



²⁷⁹ <https://www.bkr.nl/veelgestelde-vragen/registratie-bij-stichting-bkr/>

²⁸⁰ https://ec.europa.eu/info/business-economy-euro/banking-and-finance/digital-finance_en

²⁸¹ <https://www.netspar.nl/publicatie/towards-integrated-personal-financial-planning/>

- verschillende gegevensdefinities
- en het gebrek aan regie over gegevens en de verwerking daarvan.

Het wegnemen van de barrières vereist domeinoverstijgende samenwerking waarbij partijen gezamenlijk een open en vertrouwde infrastructuur neerzetten voor informatie-uitwisseling. De paper identificeert de volgende componenten voor een domein overstijgende infrastructuur:

1. persoonlijke datakluizen voor ROG,
2. eenvoudig te gebruiken digitale identiteiten met het hoogste zekerheidsniveau, waarmee ook gekwalificeerde elektronische handtekeningen geplaatst kunnen worden,
3. dataspecificaties (standaardisatie van syntax, semantiek en structuur) als katalysator voor de geautomatiseerde verwerking van gegevens,
4. online functionaliteiten/services die door burgers kunnen worden gebruikt voor het samenvoegen van gegevens, analyse en financiële planning,
5. gestandaardiseerde processen voor het geautomatiseerd verzamelen, uitwisselen en verwerken van gegevens voor persoonlijke financiële planning en dienstverlening,
6. beveiligde technische interfaces (API's) voor informatie-uitwisseling die door alle organisaties kunnen worden gebruikt,
7. ondersteuning voor organisaties die gebruik willen maken van de eerdergenoemde componenten en
8. een domein overstijgende publiek-private governance die stuurt op het ontwikkelen en toepassen van componenten.

Hoe nu verder? Deze paper introduceert drie voortbrengingsscenario's voor een domein overstijgende infrastructuur:

- bedrijven gaan samenwerken en ontwikkelen,
- de overheid gaat voorschrijven en ontwikkelen,
- publiek-private samenwerking geflankeerd door wetenschappers (onderzoeksvragen, theorieën en methodieken faciliteren de specificatie en realisatie van de domeinoverstijgende infrastructuur en de governance hiervan).

2.1.6 Digicampus

In 2019 werd Digicampus opgericht²⁸². De founding partners zijn de TU Delft, Logius, ICTU en Nederland ICT. Het doel is het creëren van de optimale omstandigheden om te innoveren door partijen bij elkaar te brengen die eigen ervaring en kennis meebrengen. Binnen de missie "Burger meer regie geven" verkent Digicampus het concept SSI, consent in een inclusieve samenleving en hoe een persoon toch regie kan hebben door zelf te kiezen om anderen te laten handelen. Via toestemming, vertegenwoordiging of machtiging.

DIGICAMPUS

2.2 Wetgeving

2.2.1 PSD2

2.2.1.1 Inleiding

De Payment Service Directive 2 (PSD2)²⁸³ is een relatief nieuwe Europese richtlijn voor betalingsverkeer van consumenten en bedrijven. Onderdeel van PSD2 is dat het voor derde partijen mogelijk wordt om transactiegegevens te verwerken, met toestemming van de rekeninghouder. Dit betekent dat het makkelijker wordt voor organisaties buiten de banken om financiële diensten aan te bieden, zoals een huishoudboekje of het realiseren van één financieel overzicht over meerdere bankrekeningen. Niet 'zomaar' alle derde partijen mogen hier gebruik van maken. Hier is een vergunning voor noodzakelijk die in Nederland bij de DNB moet worden aangevraagd.



²⁸² <https://digicampus.tech/over-digicampus/>

²⁸³ <https://www.dnb.nl/>

PSD2 is net als de AVG een drijfveer voor de ontwikkeling van PDM-initiatieven, echter primair op de financiële sector gericht. Dit leidt tot veranderingen²⁸⁴:

- Rekeninginformatiediensten (rekeningen van banken tonen in andere applicaties)
- Betalingen uitvoeren met andere applicaties dan die van de bank (betaalinitiatiediensten)
- Sterke authenticatie werd verplicht (met name verbetering voor creditcard gebruik)
- Meer aandacht voor procedures en beveiligingseisen om een vergunning te krijgen

Het delen van rekeninginformatie zien we terug in applicaties als Grip en Dyme. Ook het uitvoeren van betalingen wordt mee geëxperimenteerd, bijvoorbeeld door Yolt Pay.

2.2.1.2 Rekeninginformatiediensten en betaalinitiatiediensten²⁸⁵

Partijen met een PSD2-vergunning (ook banken) kunnen twee soorten diensten aanbieden. Ten eerste rekeninginformatiediensten. Dat zijn diensten waarbij partijen gebruik maken van informatie van de rekening, zoals het saldo en de transacties. Daarmee kunnen zij klanten bijvoorbeeld inzicht geven in hun financiën. Ten tweede de betaalinitiatiediensten: diensten waarbij klanten een partij toestemming geven om een betaling te doen. Bijvoorbeeld voor een bestelling in een webwinkel. Het is een alternatief voor iDEAL, creditcard en Paypal.

2.2.1.3 Primaire spelers

Binnen de PSD2 spelen primair vijf spelers een rol²⁸⁶.

1. Traditionele betaaldienstverleners, ook wel Account Servicing Payment Service Providers (ASPSP) genoemd. Dit zijn de banken. Klanten houden hier rekeningen aan en initiëren betalingen via een ASPSP. Deze partijen worden onder de PSD2 verplicht om Third Party Payment Providers (TPP's) met een vergunning, na toestemming van de rekeninghouder, toegang tot de online toegankelijke rekeningen te geven. Dat doen de banken door Open Application Programming Interfaces (API's) beschikbaar te stellen, waarmee TPP's toegang kunnen krijgen tot de bancaire systemen. Via deze API's delen banken en de TPP's data op een veilige en betrouwbare manier.
2. De Payment Service Users (PSU). Dit zijn klanten die een bankrekening aanhouden. Dat kan zowel een bedrijf als een consument zijn, maar ook de overheid.
3. De Payment Service Providers (PSP). Dit zijn banken en andere serviceproviders van elektronische betaaldiensten aan klanten.
4. De rekeninginformatiedienstverlener, ook wel een Account Information Service Provider (AISP) genoemd. Dat is een TPP die geregistreerd is en voldoet aan de eisen van de PSD2 en die met toestemming van de betaaldienstgebruiker rekening informatie bij de bank ophaalt en beschikbaar stelt.
5. Betaalinitiatiedienstverlener, of wel de Payment Initiation Service Provider (PISP). Dat is een TPP die met toestemming van een betaaldienstgebruiker betalingen namens hen (on-behalf-of) mag initiëren. PISP's hebben een vergunning van de nationale toezichthouder nodig om betalingen namens rekeninghouders te initiëren.

De spelers genoemd onder 4 en 5 zijn relatief nieuw.

Begin 2021²⁸⁷ zijn in Nederland PSD2-vergunningen toegekend aan:

Bedrijf	Vergunningen		Activiteiten
	Betalings initiatie	Rekening informatie	
Bizcuit Payments B.V. bizcuit.nl	✓	✓	financiële toolkit voor ondernemers
Buddy Payment B.V. buddypayment.nl		✓	wordt in dit rapport besproken
Ceron IT Solutions B.V. gatesoftware.nl		✓	eigendom bheer

²⁸⁴ <https://www.emerce.nl/opinie/jaar-psd2-nederland-stilte-storm>

²⁸⁵ nvb.nl/bank-wereld-online/psd2

²⁸⁶ <https://www.enigmaconsulting.nl/psd2-stimuleert-innovatie/>

²⁸⁷ <https://psd2sig.nl/> Cobase en Online Payment Platform worden hier niet vermeld.

Bedrijf	Vergunningen		Activiteiten
	Betalings initiatie	Rekening informatie	
Cobase www.cobase.com	✓	✓	multibank platform
Dyme B.V. dyme.app		✓	wordt in dit rapport besproken
Floryn B.V. floryn.com		✓	zakelijke kredietverlening
Flow Money Automation B.V. flowyour.money	✓	✓	huishoudboekje
Invers B.V. invers.nl		✓	wordt in dit rapport besproken
Jortt B.V. jortt.nl		✓	boekhoudsoftware
MoneyMonk B.V. moneymonk.nl		✓	online boekhouden voor zzp'ers
Ockto B.V. ockto.nl		✓	wordt in dit rapport besproken
Online Payment Platform https://onlinepaymentplatform.com/	✓	✓	online betaalplatform
Peaks B.V. peaks.com	✓	✓	beleggingsplatform
Plaid plaid.com	✓	✓	wordt in dit rapport besproken
SkillSource B.V. e-boekhouden.nl		✓	online boekhouden
Tellow B.V. tellow.nl		✓	boekhouden voor zzp'ers
Tink AB tink.com	✓	✓	open bank platform
Twinfield International N.V. taxnl.woltersklower.com		✓	online boekhouden

2.2.1.4 Toezicht

Het toezicht op PSD2 is verdeeld over verschillende toezichthouders. Naast de AP zijn dit de DNB, ACM en AFM. Het toezicht op de privacyaspecten van PSD2 ligt vooral bij de AP. Omdat er raakvlakken zijn in het toezicht, ondertekenden DNB en de AP op 21 februari 2019 een samenwerkingsprotocol om effectief en efficiënt toezicht te houden en waar nodig onderling informatie uit te wisselen. Daarnaast is ook afgestemd met de andere toezichthouders.

2.2.1.5 PSD2 en AVG

PSD2 kan volgens de NVB²⁸⁸ als voorbeeld dienen voor toekomstige data-toegang en data-delings, maar kent ook belangrijke verschillen waarmee rekening moet worden gehouden bij de inrichting van een toekomstig systeem:

- Dataportabiliteit onder de AVG is slechts beperkt tot individuen, waar PSD2 ook zakelijke klanten betreft.
- De AVG kent geen gestandaardiseerde toegang tot data, waar de PSD2 specifieke afspraken kent over datavelden en technische standaarden (API's).
- Onder de AVG is de portabiliteit van data niet online realtime verplicht, wat vaak essentieel is voor innovatieve toepassingen en het vergroten van concurrentie.
- Specifieke privacy- en datarechten zijn in sectorale wetgeving opgenomen, aanvullend op brede sector-overschrijdende wetgeving, waardoor fragmentatie en inconsistentie ontstaat.
- Ten opzichte van de andere sectoren kent de bankensector intensief toezicht, en is (mede om die reden) data-management relatief professioneel ingericht.

Volgens de NVB is met de introductie van PSD2 een ongelijk speelveld ontstaan, waarbij klanten (data-eigenaren) eenzijdig bancaire data kunnen delen met gelicenseerde data-gebruikers. Maar omgekeerd kunnen banken geen data van niet-bancaire partijen ontvangen.

De AVG (GDPR art. 20) legt het recht op dataportabiliteit duidelijk vast. Maar wat mist, is een deugdelijk systeem dat zorgt voor gestandaardiseerde en digitale datauitwisseling. Het ontbreekt

²⁸⁸ Digitaal met de mens centraal - Banken in de 21ste eeuw, NVB 2020

individueel aan voldoende grip op hun data; controle op toegang, delen, intrekking en vergetelheid. Mensen hebben geen eenduidige mogelijkheden om te weten welke derde partijen hun persoonlijke data bezitten, de data gebruiken en toestemming hebben voor toegang tot specifieke data.

Om veilige data-toegang en data-deling mogelijk te maken, zou artikel 20 van de AVG nader moeten worden uitgewerkt in Europese regelgeving. Daarmee zou een Data Services Regulation tot stand moeten komen. Deze moet de consument ook de praktische mogelijkheden geven voor toegang en delen van data.

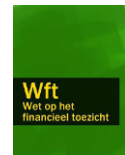
Het mag volgens de NVB niet zo zijn dat de data-eigenaren buitenspel worden gezet als het gaat om verrijkte data; zij moeten regie kunnen blijven voeren op hun data en deze op verzoek kunnen inzien en laten verwijderen. Dit geldt ook voor verrijkte data.

2.2.1.6 Delen betaalgegevens – status volgens DNB

Een kwart van de Nederlanders heeft het afgelopen jaar toestemming gegeven voor het gebruik van hun betaalgegevens in ruil voor de levering van nieuwe diensten op basis van deze data, zo blijkt uit een enquête van DNB onder het Nederlandse publiek²⁸⁹. Het is vooral de eigen bank die hiervoor toestemming kreeg; andere bedrijven kregen slechts mondjesmaat toestemming. Deze uitkomst past bij het hoge publieke vertrouwen in banken, aldus de DNB. Betaalgegevens worden als zeer privacygevoelig ervaren, ook in vergelijking met andere soorten data.

2.2.2 Wet op het financieel toezicht (Wft)

De Rijksoverheid houdt toezicht op financiële instellingen (zoals banken en verzekeraars) en het hele financiële systeem. Dit beschermt consumenten en bedrijven die hun geld toevertrouwen aan deze instellingen. De Wft²⁹⁰ beschrijft de regels met betrekking tot de financiële markten en het toezicht daarop. De Nederlandsche bank (DNB) en de Autoriteit Financiële Markten (AFM) voeren het toezicht uit. De AFM houdt toezicht op het gedrag van ondernemingen, DNB houdt prudentieel toezicht. Dit houdt in dat DNB erop toeziet of partijen op de financiële markten aan hun financiële verplichtingen kunnen voldoen.



2.2.3 Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)

De Wwft²⁹¹ dwingt af dat financiële organisaties²⁹² hun klanten goed kennen. Hiervoor stellen ze onder andere een risicoprofiel op. Deze wetgeving²⁹³ is de Nederlandse implementatie van het AMLD (Anti-Money Laundering Directive) en wordt ook wel verwoord als 'KYC' of Know Your Customer principe²⁹⁴.



Om te voorkomen dat in strijd wordt gehandeld met sanctieregelgeving moeten instellingen bij aanvang en periodiek relaties screenen aan de hand van de sanctielijsten²⁹⁵. Dit zijn lijsten met organisaties en personen waarvoor financiële beperkingen gelden.

De wet verplicht *dat* financiële instellingen de identiteit van hun klanten moeten controleren, maar de wet schrijft niet voor *hoe* dat moet gebeuren. DNB en de AFM geven in hun Leidraden Wwft diverse voorbeelden, zoals video-identificatie, het uitlezen van de chip op een ID, een liveness-check en een eID-middel²⁹⁶. Een Kifid-uitspraak maakt duidelijk dat dat de consument niet kan volstaan met het per aangetekende post verzenden van een gewaarmerkte kopie van een ID.

²⁸⁹ <https://www.dnb.nl/>

²⁹⁰ <https://www.rijksoverheid.nl/onderwerpen/financiele-sector/wet-op-het-financieel-toezicht-wft>

²⁹¹ <https://www.afm.nl/nl-nl/professionals/onderwerpen/wwft-wet>

²⁹² <https://www.fintool.nl/20472/voor-wie-geldt-wwft.htm>

²⁹³ <https://wetten.overheid.nl/BWBR0024282/2020-07-10>

²⁹⁴ <https://www.betalvereniging.nl/actueel/achtergrondinformatie/in-het-kort/ken-uw-klant-in-het-kort/>

²⁹⁵ <https://wetten.overheid.nl/BWBR0003296/2015-01-01>

²⁹⁶ <https://www.vvponline.nl/nieuws/financiele-instellingen-mogen-online-identificatie-eisen?mid=iZyTqXFjmGSYkQ==>

2.2.4 Hypothekenrichtlijn MCD

De Mortgage Credit Directive²⁹⁷ (MCD) – de hypothekenrichtlijn - verplicht aanbieders vanaf 2016 om de consument een bindende offerte aan te bieden die op een eenvoudige wijze te vergelijken is met die van andere aanbieders. Het European Standardised Information Sheet (ESIS) is een precontractueel gepersonaliseerd informatiedocument dat door de (hypothek)aanbieder of bemiddelaar aan de consument moet worden verstrekt. De vorm en inhoud van het document zijn voorgeschreven. Belangrijk is dat ruim voordat de consument gebonden is aan de overeenkomst, hij het document in zijn bezit moet hebben. Ook moet hij de mogelijkheid hebben gehad om verschillende producten te vergelijken en te beoordelen²⁹⁸.

MORTGAGE CREDIT
DIRECTIVE

Het gegeven dat een bindende offerte moet worden aangeboden geeft aanbieders van hypothecaire leningen de verplichting om het proces van het inwinnen van informatie over de betreffende consument naar voren te halen. Toegang tot brondata is hiervoor van groot belang.

Naast het beschikbaar stellen van brondata in de oriëntatie- en aanvraagfase is het van belang dat de adviseur zich aan zijn zorgplicht kan houden in de beheerfase van een financieel product. Bijvoorbeeld door het periodiek ontvangen van data (vanuit de consument of aanbieder)”²⁹⁹

2.2.5 Pensioenwet

In artikel 51.1 van de Pensioenwet³⁰⁰ staat: “ Er is een pensioenregister, ingericht en in stand gehouden door de pensioenuitvoerders, dat tot doel heeft op duidelijke en begrijpelijke wijze de aanspraakgerechtigde of de pensioengerechtigde in de gelegenheid te stellen gegevens over zijn pensioenaanspraken en pensioenrechten te raadplegen, waarbij deze gegevens, voor zover het ouderdomspensioen betreft, tevens weergegeven worden op basis van een pessimistisch scenario, een verwacht scenario en een optimistisch scenario. Het pensioenregister heeft verder tot doel inzicht te geven in de hoogte van het te bereiken pensioen, de keuzes ten aanzien van het pensioen, waaronder de mogelijkheid tot omzetting in een variabele uitkering, en de gevolgen van deze keuzes en van belangrijke gebeurtenissen en op het pensioen van de aanspraakgerechtigde of de pensioengerechtigde. Onder pensioenaanspraken en pensioenrechten in de zin van dit artikel worden tevens verstaan aanspraken op ouderdomspensioen en recht op ouderdomspensioen op grond van de Algemene Ouderdomswet.”

De Pensioenwet

en de bijbehorende documenten



2.2.6 Wet gemeentelijke Schuldhulpverlening (Wgs)

Op 1 januari 2021 treden de wijzigingen van de Wgs in. Het doel van de wijziging van de Wgs is dat schuldenaren sneller in beeld komen. Gemeenten krijgen een wettelijke zorgplicht met betrekking tot het vroegtijdig signaleren van schuldenproblematiek.

2.3 Afsprakenstelsels

2.3.1 Zorgeloos Vastgoed

Zorgeloos Vastgoed³⁰¹ biedt eigenaren van woningen duidelijkheid en zekerheid, doordat ze met betrouwbare en gevalideerde gegevens eerder, beter en complete informatie kunnen bieden voor de koper, verkoper, woning en financiering. In het initiatief ‘Zorgeloos Vastgoed’ werken NVM, KNB, HDN en Kadaster samen aan betrouwbare informatievoorziening in de vastgoedketen. Zorgeloos Vastgoed biedt de consument en branchegenoten informatie tijdens alle



²⁹⁷ <https://www.afm.nl/nl-nl/professionals/onderwerpen/hypothekenrichtlijn>

²⁹⁸ <https://www.afm.nl/nl-nl/professionals/onderwerpen/hypothekenrichtlijn>

²⁹⁹ <https://www.hdn.nl/wp-content/uploads/2016/10/Handboek-HDN-Bronservice-v.2.1.pdf>

³⁰⁰ <https://wetten.overheid.nl/BWBR0020809/2020-01-01>

³⁰¹ <https://zorgeloosvastgoed.nl/>

fases van het wonen: zoeken, kopen, wonen en verkopen. De consument bepaalt met wie hij zijn gegevens deelt, op een veilige en betrouwbare manier en de ontvangende partij kan vertrouwen op eenduidige en begrijpelijke informatie, die direct van de bron afkomstig is.

Een struikelpunt dat Zorgeloos Vastgoed aanpakt is dat bij kopen woning veel (persoonlijke) gegevens moeten worden aangeleverd bij veel verschillende partijen (zie:

<https://zorgeloosvastgoed.nl/2020/03/20/het-kopen-van-een-huis-perspectief-van-de-doorstromer/>).

De taxonomie van Zorgeloos Vastgoed is gepubliceerd op <http://taxonomie.zorgeloosvastgoed.nl> en zojuist is een consultatie uitgezet voor het informatiemodel. Zie daarvoor <https://zorgeloosvastgoed.nl/consultatie-informatiemodel-koopovereenkomst/>

Momenteel (zomer 2021) worden de bouwblokken (architectuur, juridisch kader et cetera) eerst nog afgestemd met Binnenlandse Zaken en daarna voor openbare consultatie aangeboden, aldus de programmamanager Leon Roseleur.

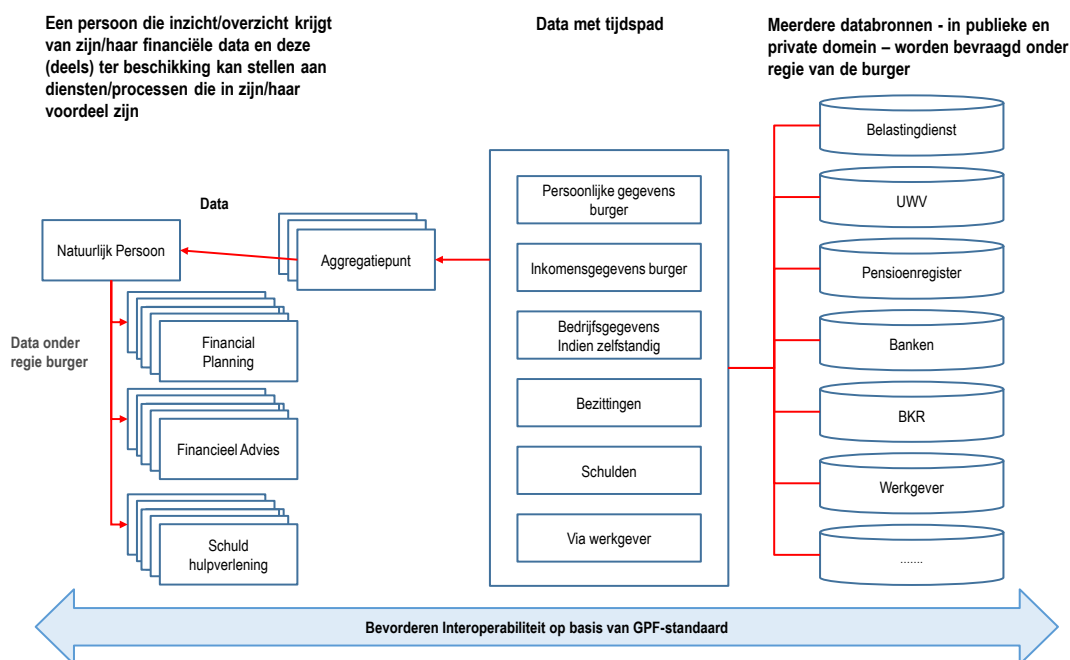
2.4 Technologie en standaarden

2.4.1 *Gegevensstandaard Persoonlijke Financiën (GPF)*

De Stichting Financieel Paspoort ontwikkelde met een aantal partners de Gegevensstandaard Persoonlijke Financiën (GPF). Dit is primair een processtandaard om de uitwisseling van persoonlijke financiële gegevens te bevorderen onder regie van de burger.

Onderstaande figuur-10 laat rechts de databronnen in het publieke en private domein zien. Uit deze databronnen worden data opgehaald onder regie van een (natuurlijk persoon). Dit kan via een app op de Smartphone maar ook vanuit een online platform bijvoorbeeld. In de figuur-10 is deze toepassing of applicatie “aggregatiepunt” genoemd. Om de datauitwisseling goed te laten verlopen zijn afspraken nodig.

In de standaard staan mensen centraal. De standaard vormt een hulpmiddel voor partijen die financiële gegevens vragen aan een persoon en daarbij duidelijk willen maken welk antwoord uit welke bron zij bij welke vraag verwachten. De GPF zorgt voor herkenning van uitgewisselde gegevens en maakt de geautomatiseerde verwerking hiervan mogelijk. De GPF verbindt en helpt structuur aan te brengen bij persoonlijke financiën. De GPF is een horizontale standaard (over sectoren heen) met waar mogelijk verwijzingen naar bestaande standaarden uit het werkveld. Tevens is het ambitie om - in overleg met domeinen zoals hypotheek, schuldhulpverlening en financiële planning - om rond de GPF datasubsets per domein te definiëren waarmee zowel recht wordt gedaan aan de behoefte aan voldoende gegevens in dat domein (wat is minimaal nodig) als het principe van data-minimalisatie (alleen gegevens die echt nodig zijn). Dit laatste is een belangrijke vereiste vanuit de AVG.



2

Figuur-10: Context waarin GPF toegevoegde waarde biedt

Het doel is dus om personen in staat te stellen op eenvoudige wijze inzage te geven in hun financiële situatie. Dit wordt mogelijk door met behulp van een applicatie (in de afbeelding aggregatiepunt genoemd) deze financiële gegevens op te halen bij organisaties die beschikken over deze gegevens.

De GPF schrijft voor:

- hoe de applicatie weet welke gegevens waar opgehaald moeten worden;
- hoe de desbetreffende persoon de mogelijkheid krijgt de gegevens aan te passen en te fiatteren en
- hoe deze gegevens aan derden ter beschikking gesteld kunnen worden,

zodat de desbetreffende persoon ondersteuning kan krijgen van gegevensvragers die gespecialiseerde kennis en software hebben om mensen terzijde te staan in het verkrijgen van helderheid over hun huidige en toekomstige financiële situatie.

De GPF is bedoeld voor softwareontwikkelaars die in de beschreven context een data-aggregatie applicatie willen bouwen en voor (softwareontwikkelaars van) gegevensvragers die bekend willen maken welke gegevens nodig zijn om hun diensten te verlenen zodat zij de juiste, en niet te veel, gegevens ter beschikking kunnen krijgen van een bepaalde persoon. De gegevens kunnen, na fiat, geautomatiseerd aangeboden worden aan de BackOffice applicatie van de gegevensvragers of bijvoorbeeld lokaal opgeslagen worden op het device van de betrokken persoon.

De GPF is beschreven in Word en werkt diverse realtime processtappen uit. De kern is dat een persoon aangeeft van welke dienst/dienstverlener gebruik wordt gemaakt. De dienstverlener maakt daarna duidelijk welke data uit welke bronnen gevraagd wordt. De data worden vervolgens uit de diverse bronnen in het private/publieke domein opgehaald en in begrijpelijke taal aan de burger gepresenteerd. De burger geeft de data daarna al dan niet gefilterd door aan de dienstverlener.

De standaard draagt bij aan het efficiënt/effectief uitwisselen van gegevens onder regie van een bepaalde persoon, op basis van principes van dataminimalisatie. De dienstverlener (bijvoorbeeld een financieel adviseur) beschikt hierdoor laagdrempelig en snel over de benodigde gegevens die uit verschillende bronnen afkomstig zijn.

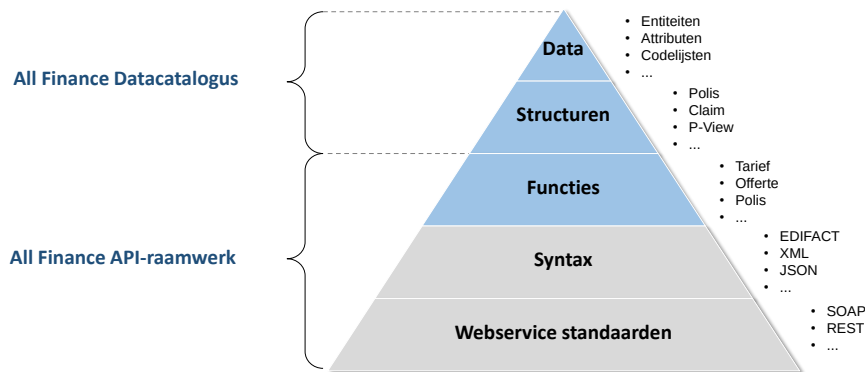
2.4.2 SIVI All Finance Standaard (AFS)

De 'SIVI All Finance Standaard' is ontwikkeld voor moderne, efficiënte en effectieve gegevensuitwisseling én -opslag. Het doel van de SIVI All Finance Standaard is dat ze binnen de financiële dienstverlening in de breedte het digitaal zakendoen ondersteunt met betrekking tot het:

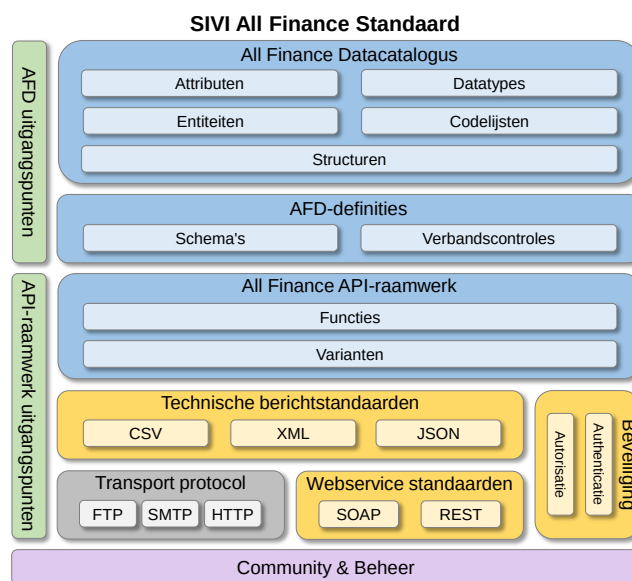
- Uitwisselen van gegevens

- Registreren van gegevens
- Ontwikkelen van webservices

In het blauw (figuur-11) de onderdelen specifiek gericht op het domein financiële dienstverlening. Alle gegevens gerelateerde afspraken zijn gedocumenteerd in de All Finance Datacatalogus. Alle afspraken rond functies en processen zijn gedocumenteerd binnen het All Finance API-raamwerk.



Figuur-11: SIVI AFS is de basis voor digitaal ecosysteem



Figuur-12: Bouwstenen SIVI All Finance Standaard

In figuur-12 is een overzicht opgenomen van de bouwstenen van de SIVI All Finance Standaard. De blauwe blokken zijn specifiek voor de financiële dienstverlening. De gele blokken staan, gerelateerd aan het gebruik van de SIVI AFS, voor richtlijnen rond generieke standaarden. De groene blokken staan voor de uitgangspunten voor de All Finance Datacatalogus en het All Finance API-raamwerk. Het paarse blok omvat alle afspraken rond het beheer en onderhoud van SIVI AFS.

De reikwijdte van de SIVI All Finance Standaard is zeer breed. Binnen het domein financiële dienstverlening omvat de standaard bijna alle branches (zoals schadeverzekeringen, levensverzekeringen, pensioen, hypotheek, lening, etc.) en vele processen (als advies, offerte, aanvraag, wijziging, schadeafwikkeling, etc.). Bij processen gaat het om alle relevante processen tussen partijen die actief zijn in de distributieketen voor financiële dienstverlening: primaire

ketenpartijen (verzekeraars, banken, intermediairs, serviceproviders etc.), derden (herstellers, experts, etc.) en de leveranciers die deze processen met hun software of services ondersteunen.

Op basis van de All Finance Datacatalogus kunnen berichten gespecificeerd worden. Deze berichten kunnen ook toegepast worden in het domein van PDM. SIVI heeft een afbeelding gemaakt van het Ockto Datamodel naar de modernste versie van de All Finance Datacatalogus.

2.4.3 Consumentendata standaard HDN

De consumentendata standaard – ook wel CA/CX standaard genoemd – is ontwikkeld door HDN³⁰². De standaard maakt het mogelijk dat brondata automatisch verwerkt kan worden bij een hypotheek aanvraag. Consumentendata leveranciers in dit kader zijn bijvoorbeeld Ockto en iWize. De CA/CX berichten bevatten data uit IBL³⁰³ en MijnPensioenoverzicht.

De processtappen staan beschreven³⁰⁴. Hier wordt ook het gebruik toegelicht. Medio augustus 2020 is een zestal geldverstrekkers in staat om hypotheekaanvragen te verwerken die gebruik maken van data van consumentendata-leveranciers: Aegon, Allianz, Argenta, bijBouwe, Florius en Rabobank.

Inkomensbepaling pensioen

ING, ABN AMRO, Aegon, Florius, Rabobank, De Hypotheker, NHG en HDN startten in juli 2020 een pilot met de Inkomensbepaling Pensioen (IBP). De IBP berekent direct een pensioeninkomen uit met de gegevens uit MijnPensioenOverzicht (MPO) op basis van gestandaardiseerde rekenregels. Met de Inkomensbepaling Pensioen wordt het bestendige pensioeninkomen bij AOW-leeftijd en, indien van toepassing, ook vóór AOW-leeftijd geautomatiseerd berekend op basis van de gegevens van het MPO³⁰⁵.

Incident IBL-rekentool³⁰⁶

De IBL-rekentool vervangt de traditionele werkgeversverklaring. De tool werd in 2018 na een pilot in gebruik genomen en is ontwikkeld in opdracht van Hypotheken Data Netwerk (HDN) in samenwerking met ING, NHG, Florius, ABN AMRO, Rabobank, De Hypotheker, Vereniging Eigen Huis, UWV, IG&H en zo'n 150 intermediairs. Het was het eerst project van het samenwerkingsverband, genaamd Handig! Met de IBL-rekentool wordt de werkgever niet meer bij het hypotheekproces betrokken. Het (digitale) UWV-verzekeringsbericht bevat de loonhistorie van alle werkenden in loondienst. Op basis van deze gegevens wordt het toetsinkomen van de klant bepaald.

Begin 2021 berichtte HDN twee keer over incidenten met de rekentool waarbij verkeerde uitkomsten werden gegenereerd. Gebrek aan goede afspraken met de broneigenaren werd door meerdere betrokkenen aangedragen als oorzaak van de incidenten. Dit incident bewijst het belang van adequaat beheer van koppelvlakken en wijzigingen daarin.

2.4.4 Ockto Brondata Service

Via de Ockto Brondata Service (OBS) kan de consument zijn data veilig delen met verschillende partijen binnen de hypotheekketen. In het aanvraagtraject van een hypotheek zorgt OBS ervoor dat geldverstrekkers zelf bepaalde brondata en documenten kunnen ophalen, zonder dat deze door de adviseur aangeleverd hoeven te worden.

Op https://www.ockto.nl/hypotheekverstrekkers_brondata_service/ staat welke documenten bij welke aanbieder komen te vervallen:

³⁰² Consumentendata standaard. <https://www.hdn.nl/consumentendata-standaard/>

³⁰³ UWV, inkomsten bepaling loonbelasting = IBL <https://www.hdn.nl/inkomensbepalingloondienst/>

³⁰⁴ <https://www.hdn.nl/consumentendata-standaard/>

³⁰⁵ <https://www.hdn.nl/altijd-het-juiste-pensioeninkomen-bij-de-hand-met-de-inkomensbepaling-pensioen/>³⁰⁵

³⁰⁶ <https://www.findinet.nl/artikel/rekentool-voor-hypotheekaanvragen-faalde-door-ontbreken-afspraken-over-brondata/>

Bedrijf	Bewijs inschrijving beëindiging geregistreerd partnerschap	Bewijsstukk en uitkering	Kopie identiteits bewijs	Pensioen overzicht	Saldobiljet schuldrest woningen	Werkgevers verklaring	WOZ-aanslag/ bewijs waarde onderpand
Aegon			✓	✓		✓	
Allianz				✓		✓	
bijBouwe				✓		✓	
Lot	✓			✓	✓	✓	✓
Rabobank				✓		✓	
ING	✓	✓		✓	✓	✓	✓
Lloyds				✓		✓	
Obvion				✓		✓	
Centraal Beheer				✓		✓	
Woonnu				✓		✓	

2.4.5 Standaarden Betalingsverkeer

Inleiding

De Betaalvereniging is beleidsmatig nauw betrokken bij de ontwikkeling van verschillende betaalstandaarden, via de Werkgroep Coördinatie Bancaire Standaardisatie (WCBS) die in 2016 is opgericht. Samen met haar leden verkent de Betaalvereniging de wenselijkheid en haalbaarheid van het aanpassen van bestaande internationale standaarden en het invoeren van nieuwe standaarden. Voorbeelden van standaarden in het betalingsverkeer:

- De IBAN-standaard. IBAN geldt als identificatienummer van een (internationale) betaalrekening.
- De SEPA-afsprakenstelsels voor bijvoorbeeld Europese overboekingen en Instant Payments.
- De PCI-beveiligingsstandaarden voor o.a. bankpassen, creditkaarten, smartphones, wearables en betaalautomaten.
- De ISO 20022 financiële berichtenstandaard waarmee straks vrijwel alle transacties met en tussen banken worden uitgewisseld.

QR-codes

De European Payments Council (EPC) ontwikkelde een standaard³⁰⁷ om alle betaalgegevens die nodig zijn voor een gewone Europese overboeking in een QR-code te zetten: het bedrag, het IBAN van de ontvanger, de naam van de ontvanger en een omschrijving of betaalreferentie. Dankzij EPC QR-codes kunnen betalers met een mobiele telefoon makkelijker overboeken, zonder vergissingen of tikfouten te maken. De begunstigde kan de juiste betaalgegevens in een QR-code zetten en de betaler moet die QR-code alleen maar met een bankapp scannen om over te boeken. Hij hoeft daarbij zelf geen betaalgegevens in te tikken.

Instant Payments

Instant Payments worden in Nederland conform de SEPA-standaard geïmplementeerd. Voor de Nederlandse markt worden enkele specifieke verbeteringen gerealiseerd:

- De instant betaling doet er maximaal 5 seconden over, en kent een harde time-out van 7 seconden.
- Elk bedrag is mogelijk.

Deze extra functionaliteiten zijn vastgelegd in NL Standaarden.

³⁰⁷ <https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/quick-response-code-guidelines-enable-data-capture-initiation>

2.4.6 NextGenPSD2 Framework

De meest besproken en impactvolle delen van PSD2 hebben betrekking op de bepalingen over sterke klantauthenticatie (SCA) voor online betalingen en op de introductie van nieuwe 'betalingsinitiatie- en rekeninginformatiediensten', beheerd door Third Party Providers (TPP's). De PSD2-beveiligingsmaatregelen met betrekking tot TPP-accounttoegang en SCA worden meer gedetailleerd in de EBA RTS (European Banking Authority Regulatory Technical Standards) en traden in werking op 14 september 2019.



Op basis van de PSD2- en EBA RTS-vereisten heeft Berlin Group NextGenPSD2 gewerkt aan een gedetailleerd 'Access to Account (XS2A) Framework' met datamodel (op conceptueel, logisch en fysiek dataniveau) en bijbehorende berichtgeving³⁰⁸.

Het NextGenPSD2 Framework biedt een open, geharmoniseerde en interoperabele set Application Programming Interfaces (API's) als de veiligste en meest efficiënte manier om gegevens veilig te verstrekken.

Kenmerken zijn onder meer:

- Moderne "RESTful" API-set die HTTP/1.1 gebruikt met TLS 1.2 (of hoger) als transportprotocol
- TPP-identificatie door ETSI-gedefinieerde eIDAS-certificaten: QWACS verplicht gesteld (eenvoudige maatregel ter bescherming, bijv. Tegen DDOS-aanvallen), QSEALS optioneel voor banken (TPP volgt instructies van bank).
- Volledige ondersteuning voor meerdere valuta's van accounts.
- Vier architectuurmodellen voor Strong Customer Authentication (SCA): omleiding, OAuth2, ontkoppeld en ingebed, met invloed van de TPP op omleidingsvoorkeur.
- Multilevel SCA-benadering voor bedrijven, bijv. ter ondersteuning van een 4-ogen-principe
- Toegewijde toestemmings-API die toestemmingsafhandeling scheidt van accounttoegang, in overeenstemming met zowel PSD2- als AVG-vereisten.
- Optionele sessieondersteuning (reeks opeenvolgend uitgevoerde transacties), onder voorbehoud van de juiste toestemming van de klant.
- Datastructuren ofwel als JSON met datamodel gebaseerd op ISO 20022, of XML met pain.001 voor PISP's en camt.05x voor AISP's.

2.5 Authenticatievoorzieningen

De financiële sector lift mee op generieke sector onafhankelijke voorzieningen als DigiD (waar wettelijk toegestaan) en iDIN. Deze zijn in het vorige hoofdstuk besproken. Verder wordt veel gebruik gemaakt van propriëtaire oplossingen. De meeste financiële diensten op het internet zijn niet open toegankelijk, om toegang te krijgen heeft de gebruiker gebruikspersmissie via een account nodig. Tijdens het eerste gebruik van een dergelijke dienst maakt men zo'n account aan. Een account bestaat uit een gebruikersnaam en een wachtwoord. Daarnaast worden vaak nog extra gegevens ingevuld om een soort profiel te maken. Voor gebruik moet telkens de gebruikersnaam en het bijbehorende wachtwoord worden ingevoerd. Het is mogelijk gebruikersnaam/wachtwoord uit te breiden met een tweede factor.

2.6 PDM-Diensten

Hierna volgt een overzicht van PDM-Diensten. Aparte aandacht gaat uit naar planningstools, huishoudboekjes, tools in het kader van schuldhulpverlening, klantmappen en apps.

2.6.1 PDM-Diensten

2.6.1.1 Financieel Paspoort (FP)

De Stichting Financieel Paspoort biedt een mobiele app waarmee gebruikers gemakkelijk een overzicht van hun financiën krijgen, zonder dat andere mensen deze gegevens kunnen inzien of opslaan. Hiermee focussen ze zich op de financiële zelfredzaamheid van de Nederlandse burgers. De gebruiker kan zelf

Financieel Paspoort

³⁰⁸ <https://www.berlin-group.org/psd2-access-to-bank-accounts>

Pilot Regie op financiële gegevens t.b.v. schuldhulpverlening

- Burger heeft behoefte aan inzicht**
 - Overzicht en inzicht in financiële situatie
 - Regie op mijn eigen gegevens
- Burger heeft keuze uit verschillende online hulpmiddelen, zoals:**
 - Kk
- Gegevens worden beschikbaar gesteld aan de burger**

Bronnen:

 - Uitvoeringsorganisaties
 - Gemeenten
 - Verzekeringsmij
 - Pensioenoverzicht
 - Hypotheek
 - Bank
 - ...

Methode:

 - Scraping
 - Blauwe knop
 - Afsprakenstelsel
- Burger gebruikt de opgehaalde gegevens**
 - Eigen inzicht
 - Schuldhulpverlening
 - Budgetcoach
 - Woningcorporatie
 - Hypotheekverstrekker
 - ...

The infographic also includes logos at the bottom: KLOOSTERHOF, Samenwerking Ondernemers, Central Institute voor maatschappelijke ondersteuning, Breda, and various partner logos like UWV, S y v B, C/AK, and VNG.

In 2019 verscheen een rapport³⁰⁹ over een pilot met fikKs en Financieel Paspoort, zie figuur-13. In de pilot draaide het om het verzamelen van financiële gegevens in het kader van schuldhulpverlening. In het rapport worden meerdere conclusies getrokken, onder andere:

- De auteurs van rapport stellen voorts dat voor een goed financieel inzicht vaak gegevens nodig zijn van het gehele huishouden en niet alleen van een individu. Gegevens moeten dan voor verschillende personen worden opgehaald, een goede machtigingenoplossing is hiervoor een cruciale

101 » 149

randvoorwaarde. "Het is dan ook van belang dat hiervoor een generiek te gebruiken oplossing wordt gevonden binnen het Programma Machtigen van het ministerie van BZK." Financieel Paspoort heeft ambities zich door te ontwikkelen tot open source.

Use case Schadevrij jaren

Iedere autorijder bouwt automatisch schadevrije jaren op als er geen schade wordt gemeld aan de verzekeraar. Als de autorijder overstapt naar een nieuwe verzekeraar dient het aantal schadevrije jaren doorgegeven te worden. Dit proces is op dit moment fraudegevoelig en kan door een operator applicatie in te zetten worden verbeterd. Bijvoorbeeld door de oude verzekeraar het aantal jaren door te laten geven aan de app, en de nieuwe verzekeraar ze vervolgens te laten opvragen bij de app.

2.6.1.2 Invers

Invers³¹⁰ is een voorbeeld van een organisatie die analyses biedt op basis van financiële data. Banktransacties worden opgehaald onder expliciete toestemming van de gebruiker. In 2019 kreeg Invers een PSD2 vergunning. Deze gegevens worden verrijkt en verwerkt tot financiële analyses (in JSON formaat). De gebruikte tool het LinX³¹¹. Denk aan categoriseren van transacties en verwerking tot uitgave overzichten. Deze diensten worden geleverd aan B2B en B2C klanten. Klanten met een PSD2 vergunning hebben de mogelijkheid zelf voort te bouwen op de white-label technologie van Invers. Recentelijk is Invers een samenwerking aangegaan met Ockto om een financieel overzicht te kunnen bieden, waarbij Invers gecategoriseerde banktransacties aanlevert³¹². Nationale-Nederlanden nam eind 2020 een belang in Invers³¹³. Recent lanceerde Nationale-Nederlanden ook het digitale huishoudboekje Nova³¹⁴ in samenwerking met Invers.



NOVA

Breng balans
in je geldzaken



Experian, mondiale speler op het gebied van data en analyse, en Invers, gaan samenwerken. Dit werd november 2020 bekend³¹⁵. Ze bieden bedrijven nieuwe oplossingen waarmee beslissingen voor het verstrekken van krediet geoptimaliseerd kunnen worden. Met de onderliggende overeenkomst hebben Experian en Invers een technologieplatform voor Open Banking ontwikkeld.

2.6.1.3 Ockto

Ockto³¹⁶ is een platform waarmee consumenten data kunnen verzamelen vanuit verschillende databronnen en deze data kunnen doorgeven aan een datadienst. Ockto zorgt ervoor dat consumenten snel en simpel informatie kunnen verzamelen en deze met adviseurs, banken, hypotheekverstrekkers of andere dienstverleners kunnen delen. De gebruiker en data aanbieder kunnen Ockto gratis gebruiken, data afnemers betalen een transactie vergoeding als zij data vanuit Ockto willen gebruiken. Ockto is een Nederlands initiatief en focust zich op de Nederlandse financiële markt. Ockto is operationeel: op dit moment kan een gebruiker met de Ockto app onder andere gegevens ophalen bij de Belastingdienst, UWV, MijnPensioenoverzicht, DUO en MijnOverheid middels een QR-code. Het ophalen van studieschuld was daarin niet onomstreden: het voornemen om studieschuld toegankelijk te maken voor



³¹⁰ <https://www.invers.nl/services>

³¹¹ <https://www.invers.nl/linx>

³¹² <https://www.amweb.nl/financiele-planning/nieuws/2020/05/ockto-en-invers-gaan-samenwerking-aan-101122940>

³¹³ <https://www.hypotheek-vinden.be/nieuws/nationale-nederlanden-investeert-in-psd2-partner-invers-6694>

³¹⁴ <https://www.vvponline.nl/nieuws/nn-komt-met-digitaal-huishoudboekje-met-verzekeringenoverzicht?mid=k6Kaq3FnI2SYkQ==>

³¹⁵ <https://www.creditexpo.nl/experian-en-invers-werken-samen-voor-lancering-van-open-banking-oplossing/>

³¹⁶ <https://www.ockto.nl>

hypotheekverstekkers leidde tot Kamervragen³¹⁷, maar werd toegestaan op basis van de AVG (dus mits het gegeven onder toestemming van de burger wordt opgevraagd).

Ockto is geïmplementeerd bij onder meer: Rabobank, ABN AMRO, AEGON, Allianz en recentelijk ING^{318,319}. Daarnaast wordt Ockto ook toegepast in verschillende applicatie het bieden van financieel overzicht, zoals FinanceBook van Achmea en MyLife van Yellowtail³²⁰. Specifiek voor de hypotheekketen heeft Ockto, samen met onder andere HDN, de Ockto Brondata Service ontwikkeld. Dit zorgt ervoor dat de consument minder documenten hoeft op te leveren bij de aanvraag van een hypotheek³²¹.

Via 'Opvragen Digitale Klantgegevens' in FAN, de adviseursomgeving van Florius³²², kunnen klanten via Ockto voor het adviesgesprek hun digitale klantgegevens aanleveren.

Met behulp van het Ockto platform is het voor een prospect mogelijk om kredietverleners op een eenvoudige en veilige manier inzage te geven in de informatie die zij nodig hebben voor de kredietbeoordeling³²³.

De gegevensuitwisseling tussen Ockto en data aanbieders en gelicenseerde data-afnemers verloopt via API of screen scraping (bij screen scraping is geen sprake van waarmerking vanuit de data aanbieder). De data worden opgeslagen op het apparaat van de gebruiker en verwerkt op de server van Ockto. Een data-afnemer kan de gebruiker daarnaast vragen om de gegevens maximaal 90 dagen bij Ockto beschikbaar te houden. Daardoor kan een geldverstrekker de persoonsgegevens gebruiken voor het uitbrengen van een aanbod. Ockto is recentelijk een samenwerking gestart met Invers om een financieel overzicht te kunnen aanbieden waarbij ook gecategoriseerde banktransactiegegevens ontsloten kunnen worden.³²⁴

Use case hypotheek afsluiten

Als een consument een lening wil voor een nieuwe of bestaande woning en een hypotheekvraag heeft dan richt hij/zij zich tot een hypotheekadviseur. Deze onderzoekt de persoonlijke situatie (klantbeeld) en geeft hier een passend advies bij. Nu is de doorlooptijd 4 tot 8 weken. Door koppeling met databronnen en regie van de consument moet versnelling tot een paar dagen mogelijk zijn. In het volgende wordt uitgegaan van regie van de consument die via een operator met DigiD inlogt bij databronnen en data ophaalt.

Op dit moment (mei 2020) zijn de volgende adviesapplicaties in staat om de gegevens van de consumentendata-leverancier in te lezen in het pakket zodat adviseurs direct een reeds ver ingevuld klantdossier hebben van hun aanvraag: Findesk, Faster Forward Elements, Accelerate, Figlo, Adviesbox, Private Wealth Support, DIAS Advies, FinDash, FinRust, Scope

- Aanbieders die werken met de consumentendata van leveranciers: Argenta, Allianz, Florius, Rabobank, bijBouwe.
- De bronnen die ontsloten worden zijn onder meer Inkomsten Bepaling Loonbelasting (UWV), Mijnpensioenoverzicht.nl en BRP.
- De operators die hierbij genoemd worden zijn Ockto en iWize.

³¹⁷ <https://zoek.officielebekendmakingen.nl/ah-tk-20192020-821.html>

³¹⁸ <https://www.ockto.nl/2020/05/12/ing-gaat-data-via-ockto-gebruiken/>

³¹⁹ <https://www.aegon.nl/particulier/klantenservice/veelgestelde-vragen/wat-finsnap>

³²⁰ <https://www.wijzeringeldzaken.nl/pensioen3daagse/PensioenWegwijzer/achmea-financebook/>
<https://yellowtail.nl/oplossingen/mylife/>

³²¹ <https://www.ockto.nl/ockto-brondata-service/>

³²² https://www.vvponline.nl/nieuws/florius-stelt-brondata-beschikbaar-voor-adviesgesprek?mid=k5*YrGikmWSYkQ==

³²³ <https://www.ockto.nl/consumptief-krediet/>

³²⁴ <https://www.amweb.nl/financiele-planning/nieuws/2020/05/ockto-en-invers-gaan-samenwerking-aan-101122940>

2.6.1.4 MijnPensioenoverzicht (MPO)

MijnPensioenoverzicht³²⁵ is een online platform waarop iedere Nederlandse burger een overzicht van zijn pensioenrechten kan opvragen. Daarbij biedt het de mogelijkheid, op verzoek van de burger, aan pensioenuitvoerders om te informeren bij welke andere pensioenuitvoerder een gewezen deelnemer pensioenaanspraken opbouwt ten behoeve van waardeoverdracht van pensioen. Gebruikers kunnen inloggen via DigiD of eIDAS.



Experts kwalificeren het versiebeheer van MPO als zwak. Iedere keer weer is sprake van verrassingen. Een API-koppeling is technisch operationeel, maar het gebruik is nog niet mogelijk. SZW moet de juridisch basis nog leggen.

2.6.1.5 iWize

iWize³²⁶ haalt gegevens op die vervolgens verder verwerkt kunnen worden, onder toestemming van de gebruiker. De bronnen waar het om gaat zijn onder andere inkomen, gezinssamenstelling, uitkering, arbeidsverleden, studieschuld, en pensioenen. Hiervoor worden gegevens opgehaald bij Belastingdienst, UWV, MijnPensioenoverzicht, MijnOverheid, DUO, Funda en LinkedIn. De consument kiest welke gegevens ontsloten worden. De opzet van iWize is B2B; het biedt de tooling white-label aan om consent en gegevensuitwisseling te regelen binnen de processen van de afnemende organisatie.



2.6.1.6 Bittiq

Bittiq³²⁷ biedt aggregatie van financiële data, data-analyse en tools voor financieel welzijn.

Bronnen die Bittiq ontsluit: MijnOverheid, MijnPensioenoverzicht, MijnBelastingdienst, DUO en UWV.

In maart 2021 kondigde Achmea bank samenwerking met Bittiq aan.³²⁸



2.6.1.7 TM-pro

TM-pro³²⁹ biedt tooling die er met name gericht is op personen meer inzicht in financiën te geven. Onder meer door diverse dashboards op basis van transactiegegevens. Dit wordt echter niet direct aan consumenten aangeboden, maar als white-label platform voor organisaties. Via TM-pro kunnen ook betalingen verwerkt worden voor organisaties met PSD2 vergunning, en voor organisaties die hier niet over beschikken middels het Swift protocol.



De oplossingen van TM-pro worden gebruikt door banken, verzekeraars, family offices en financiële startups in heel Europa. De software wordt aangeboden in de vorm van white label-componenten, vaak geïntegreerd in en ter ondersteuning van bestaande omgevingen.

Recent nam TM-Pro het technologieplatform Moneyou Go over van ABN AMRO³³⁰.

2.6.1.8 IDA

Rabobank zet met IDA³³¹ (25 FTE in het voorjaar van 2021) groot in op een rol nemen in het "data custodian" landschap. Daarin faciliteert Rabobank een oplossing om persoonlijke gegevens veilig te delen zonder daarin ook maar iets van de gegevens of transacties te zien.



³²⁵ <https://www.mijnpensioenoverzicht.nl/>

³²⁶ <https://www.iwize.nl/>

³²⁷ <https://www.bittiq.com/>

³²⁸ <https://www.achmeabank.nl/nieuws/achmea-bank-gaat-samenwerken-met-bittiq-voor-psd2-diensten>

³²⁹ <https://tm-pro.eu/#/>

³³⁰ <https://www.banken.nl/nieuws/22648/fintech-tm-pro-verwerft-platform-moneyou-van-abn-amro>

³³¹ <https://mijnida.nl/ida/>

Hoe het werkt:

- Op de website van de aanbieder bestel je een dienst of product en zie je het IDA logo en QR code.
- Met de IDA app scan je de QR code. Het “data delen” verzoek verschijnt in de IDA app.
- In de IDA app voeg je al je benodigde persoonlijke gegevens toe, tekent eventueel een overeenkomst, en klikt op verzenden.

IDA gaat uit van geverifieerde credentials³³². Een digitale credential representeert zelfde als fysieke credential of document, en biedt onder meer fraudebestendigheid, focus op privacy, juiste bron garantie.

2.6.2 Planningstools

Er zijn veel verschillende programma's of tools in de markt waarmee consumenten inzicht wordt gegeven in hun financiële situatie, zowel voor als na pensionering. Meestal bevatten deze programma's ook scenario's waarmee de deelnemers de effecten van bepaalde keuzes op hun financiële situatie kunnen zien. De opkomst van de pensioenplanners en financiële planningstools is mede te verklaren vanuit maatschappelijke ontwikkelingen. De digitalisering van de samenleving heeft ervoor gezorgd dat vrijwel alle Nederlanders beschikken over een computer, laptop en/of smartphone. Daarmee hebben consumenten steeds meer toegang gekregen tot online omgevingen om informatie in te zien en zelf bepaalde handelingen uit te voeren. Daarnaast is financiële informatie uitgebreider en complexer geworden.

Inmiddels is duidelijk dat een grote groep Nederlanders in financiële problemen is geraakt en dat er een reëel risico is dat die groep gaat stijgen. Vanuit de overheid wordt daarom actie ondernomen om burgers meer financieel zelfredzaam³³³ te maken. Ook relevant is dat het thema pensioen volop in het nieuws is. Berichten over onder meer mogelijke pensioenkortingen, een nieuw pensioenakkoord en het verhogen van de pensioengerechtigde leeftijd zorgen voor veel discussie binnen (en buiten) het pensioendomein. Grote groepen burgers maken zich zorgen over hun financiën, nu en in de toekomst. Pensioen weegt daarin nog steeds zwaar, maar wordt tegenwoordig meer beschouwd als belangrijk onderdeel van de oudedagvoorziening.

De planningstool stellen adviseurs van consumenten in staat regie over hun financiële situatie te voeren. Om snel inzicht op te bouwen is het van belang dat gebruik wordt gemaakt van digitale koppelingen met brongegevens. Hierbij wordt al dan niet gebruik gemaakt van een externe en/of geïntegreerde data-aggregator.

2.6.2.1 ToekomstVerkenner

ToekomstVerkenner is ontwikkeld door Yellowtail en Ortec³³⁴, in opdracht van PGGM voor pensioenfondsen PFZW. De ToekomstVerkenner maakt gebruik van Ockto om data op te halen. Gegevens die worden verzameld door de deelnemer via de Ockto app zijn van MijnOverheid, Belastingdienst, UWV en MijnPensioenOverzicht. Daarnaast wordt voor referentiebedragen (uitgavenpatroon) gebruik gemaakt van gegevens van het Nibud. De ToekomstVerkenner baseert zich op pensioenaanspraken 1e, 2e en 3e pijler en salarissen en bezittingen (woning, sparen en beleggen), biedt inzicht in netto besteedbaar inkomen van deelnemer of het huishouden, en geeft de mogelijkheid zelf te spelen met verschillende scenario's.

De ToekomstVerkenner wordt ook gebruikt door pensioenfondsen PME, PMT en Koopvaardij (via uitvoerder MN Services). Volgens PGGM wordt nu hard gewerkt om het platform zo open mogelijk te maken, zodat naast pensioenfondsen bijvoorbeeld ook financieel adviseurs er gebruik van kunnen gaan maken. Bannink: “Daarnaast willen we graag samen met andere fondsen de ToekomstVerkenner doorontwikkelen met nog meer specifieke microservices die concrete vragen van deelnemers beantwoorden. Denk daarbij aan andere life events zoals scheiden of het kopen van een

³³² <https://www.w3.org/TR/vc-data-model/>

³³³ Iemand is financieel redzaam wanneer hij weloverwogen keuzes maakt, zodanig dat zijn financiën in balans zijn op zowel korte als op lange termijn'. Dat is niet alleen op het moment dat iemand zelf al zijn geldzaken kan regelen, maar ook dat iemand weet wanneer hij hulp zou moeten invoeren. (www.nibud.nl)

³³⁴ Ortec levert de rekenengine Opal

nieuwe woning. Wederom niet alleen op het individu gericht, maar op de impact voor het gezin als geheel.”³³⁵

2.6.2.2 APG Helder Overzicht en Inzicht³³⁶

APG heeft een vermogensplanner laten ontwikkelen door Finbase, de partij achter MijnGeldzaken.nl. Voor de berekeningen wordt gebruik gemaakt van Ortec Finance. De planner heet Helder Overzicht en Inzicht. De tool is beschikbaar voor alle fondsen die door APG bediend worden, maar wordt nu gebruikt door een paar (ABP, SPW, Personeelspensioenfonds APG). De tool bevat scenario's (eerder stoppen met werken, sabbatical, langer doorwerken) en de informatie kan op gezinsniveau worden bekeken, in netto bedragen. Deelnemers kunnen zelf handmatig andere regelingen, buiten APG, toevoegen.

2.6.2.3 AZL-pensioenplanner

Pensioenuitvoerder AZL verzorgt de administratie van zo'n veertig pensioenfondsen. Voor elk pensioenfonds is een deelnemersportaal ingericht. Daarnaast biedt AZL een eigen pensioenplanner aan en een pensioenschets.

- Pensioenplanner: Circa dertien fondsen maken gebruik van de pensioenplanner van AZL. De tool is ontwikkeld door Actu-IT. AZL levert alle data aan en verwerkt daarin ook de specifieke reglementen en gebruikte factoren van het individuele pensioenfonds. De look and view is per pensioenfonds verschillend.
- Pensioenschets. Dit wordt door 14 fondsen (niet allemaal dezelfde als de gebruikers van de planningtool) afgenomen. Hiermee kunnen deelnemers zelf spelen met getallen op basis van voorbeeldbedragen om een beeld te krijgen van de financiële situatie na pensioendatum. Het is een generieke tool die AZL zelf heeft ontwikkeld.

De tools die AZL aanbiedt gaan over het domein pensioen en oude dag voorziening. AZL verwacht in de toekomst ook een planner te kunnen bieden die de totale financiële situatie van een deelnemer in oogschouw neemt.

2.6.2.4 TKP-planningstool

Pensioenuitvoerder TKP had al een dashboard voor de deelnemers ontwikkeld waarin de inkomsten bij pensioen worden getoond, maar waar ook andere inkomsten (3^e pijler) in kunnen worden opgenomen. Inmiddels is men bezig met de ontwikkeling van een nieuwe tool met meer gebruiksgemak en meer inzage richting financiële planning. De oude pensioenplanner werd matig bezocht omdat de gebruiksvriendelijkheid laag was. Met de nieuwe tool, die voor de aangesloten fondsen beschikbaar komt, staat de deelnemer meer centraal.



2.6.2.5 Independer Pensioenplanner

Via de Independer Pensioenplanner kunnen klanten van Independer zelf inkomsten en uitgaven toevoegen en wat je al hebt geregeld. Via DigiD kun je het pensioenoverzicht toevoegen van jezelf en van een eventuele partner. De berekeningen op basis van aannames.

2.6.2.6 Financiële planningstools verzekeraars

Verschillende verzekeraars en banken bieden hun klanten vormen van financiële planningtools. Naast Zwitserleven en Knab, zijn dat onder meer:

- ING Pensioenwijzer;
- ASR Mijn Pensioenplein app;
- NN Mijn Inkomen later app.

³³⁵ <https://www.wijzeringeldzaken.nl/pensioen3daagse/PensioenWegwijzer/Interview-winnaar-2018-pensioenwegwijzer/>

³³⁶ <https://www.ppf-apg.nl/plan-jouw-pensioen/inzicht-in-jouw-financiele-toekomst/>

2.6.2.7 Omniplan Personal Finance Platform

Het Personal Finance Platform stelt adviseurs in staat consumenten financieel inzicht te bieden. Hiertoe worden onder meer verschillende externe databronnen ontsloten (MijnOverheid, MijnPensioenoverzicht, kadaster, UWV etc.)³³⁷.

2.6.2.8 Figlo

Figlo is al jaren marktleider op het gebied van API gedreven rekenservices en applicaties in de institutionele markt. Als 'onzichtbare kracht' is het de motor achter tal van online initiatieven binnen onder meer het financial planning en hypotheekdomein. Figlo levert software die financieel inzicht en begrip op een consumentenniveau toegankelijk maken. En biedt tegelijkertijd tools voor de professional ten aanzien van complexe financiële dienstverlening. Figlo's oplossingen worden geleverd aan financieel adviseurs in allerlei markten, waaronder banken, verzekeringsmaatschappijen, accountants en pensioenfondsen. Ontworpen om financiële zaken inzichtelijk te maken en laagdrempelige toegang te bieden tot deze belangrijke informatie.



Yellowtail is de belangrijkste implementatiepartner van Figlo in Nederland. Figlo heeft diverse koppelingen zoals de Vooraf Inge vulde Aangifte, MijnPensioenOverzicht, Nibud, Ockto, Moneyview, HDN, NNEK³³⁸ en Finbox.

2.6.2.9 FinRust

FinRust³³⁹ (voorheen PensioenRust) levert financiële planningssoftware en adviessoftware die adviseurs helpt om de financiële situatie van particulieren en ondernemers in kaart te brengen en het doelkapitaal te bepalen voor aanvulling op het (vroeg)pensioen, overlijden en arbeidsongeschiktheid. FinRust heeft onder meer een koppeling met Ockto. De koppeling van Ockto met FinRust zorgt ervoor dat de door Ockto opgehaalde brondata nu ook via Elements (van Faster Forward) direct in Finrust wordt geladen³⁴⁰.



2.6.2.10 Pensioenpod

Pensioenpod³⁴¹ is een toepassing van ValueQuest waarmee inzicht kan worden verkregen in de eigen financiële situatie. De primaire focus is pensioenen. Data wordt opgehaald uit MijnPensioenoverzicht en de voor ingevulde aangifte van de Belastingdienst.



2.6.2.11 ACTU-IT

ACTU-IT³⁴² een ICT-leverancier die maatwerkoplossingen (onder meer pensioenplanners) verzorgt voor veel spelers in de pensioensector.



2.6.2.12 Adviesbox

Intersoftware³⁴³ is de leverancier van Adviesbox, een pakket vooral bestemd voor de financieel adviseur. Met dit pakket beschikken financieel adviseurs over een eigen financiële planningtool.

Brondata wordt opgehaald uit verschillende databronnen:

- Belastingdienst
- DUO
- MijnPensioenOverzicht
- MijnOverheid



³³⁷ <https://www.omniplan.nl/personal-finance-platform/>

³³⁸ <https://www.nnek.nl/maatschappelijke-rol/>

³³⁹ <https://finrust.nl/>

³⁴⁰ <https://www.ockto.nl/2020/07/29/ockto-koppeling-finrust/>

³⁴¹ <https://www.pensioenpod.nl/fag>

³⁴² <https://www.linkedin.com/company/actuit/?originalSubdomain=nl>

³⁴³ <https://www.adviesbox.nl/>

- UWV

2.6.3 Huishoudboekjes

2.6.3.1 Inleiding

Sprake is van een grote hoeveelheid aan tools die personen hulp bieden om een 'huishoudboekje' bij te houden. Deze tools helpen onder andere om inzicht te krijgen in de financiële situatie, faciliteren het maken van 'spaarpotjes' en geven saldomeldingen. Deze huishoudboekjes combineren vaak de rollen operator en data afnemer.

Wanneer we naar de functionaliteiten van deze applicaties kijken, zien we dat ze verschillende mogelijkheden voor het verzamelen van gegevens bieden: applicaties die automatisch transactie informatie aggregeren van meerdere rekeningen (ongeacht bij welke banken de gegevens staan), applicaties die werken met informatie die handmatig geïmporteerd wordt door de gebruiker en applicaties die wel automatisch transactie informatie verwerken, maar zich beperken tot één rekening.



Het verdienmodel van deze applicaties is verschillend. Daar waar de huishoudboekjes vanuit een bank of bankrekening ontwikkeld is, wordt deze gratis aangeboden als service vanuit de bank. Bij de onafhankelijk ontwikkelde applicaties is sprake van jaarlijkse of maandelijkse abonnementen aangeboden. Waarbij er veelal een gratis 'basis versie' beschikbaar is en een 'premium' variant tegen betaling.

Volgens Wijzingeldzaken.nl³⁴⁴ maakt 3% van de Nederlanders gebruik van een digitaal huishoudboekje. Dit percentage is al langere tijd stabiel. Onderstaande voorbeelden zijn een greep uit het overzicht aan huishoudboekjes dat te vinden is op Wijzingeldzaken.nl; dat onder andere overzicht biedt in de huishoudboekjes die op dit moment in de markt beschikbaar zijn.

2.6.3.2 BankTrans

BankTrans is een offlineapplicatie waarin de gebruiker handmatig banktransacties moet importeren. Van een automatische koppeling met de bank is geen sprake.

2.6.3.3 Cashflow Online

Cashflow Online is een online huishoudboekje waarbij de gebruiker handmatig gegevens moet uploaden en vervolgens de uitgave geschiedenis kan inzien. Het verdienmodel van dit huishoudboekje is een voorbeeld van het freemium model: de basis versie van de applicatie is gratis. Daarna kunnen gebruikers tegen betaling verschillende versies met meer functionaliteiten aanschaffen door middel van een jaarlijks abonnement.

2.6.3.4 Flow Your Money

Dit is een gratis app, met premiumabonnement van zo'n 5 euro per maand met extra functies. De Nederlandse startup Flow Your Money ontving een Nederlandse PSD2-licentie op 13 juli 2020. Hiermee is Flow een van de eerste FinTechs in Nederland die namens de klant zowel betalingen kan doen als banktransacties kan inzien. De app – die vanaf september 2020 beschikbaar is - beheert geldstromen³⁴⁵. Een freelancer kan bijvoorbeeld instellen dat de inkomstenbelasting automatisch opzij wordt gezet na elke betaalde factuur. De app berekent hoe hoog dit bedrag moet zijn. Dankzij de betalingsinitiatiefunctie kan dit bedrag automatisch worden overgemaakt naar een andere bankrekening.

2.6.3.5 Dyme

Dyme³⁴⁶ is een voorbeeld van een huishoudboekje dat automatisch transactiegegevens ophaalt bij banken, met toestemming van de gebruiker. Binnen de Dyme applicatie wordt een uitstap gemaakt

³⁴⁴ <https://www.wijzingeldzaken.nl/platform-wijzingeldzaken/publicaties/monitor-financieel-gedrag-wijzer-in-geldzaken-2019.pdf>

³⁴⁵ <https://flowyour.money/blog/news/flow-receives-psd2-license-dutch-central-bank>

³⁴⁶ <https://dyme.app/>

naar de desbetreffende banken waar de persoon een rekening heeft lopen. Daar wordt toestemming gegeven om (voor bepaalde periode) transactiegegevens te delen met Dyme. Dyme werkt onder een PSD2 vergunning.

Dyme helpt de gebruiker onder andere met:

- Het verkrijgen van informatie over geldzaken en het inzichtelijk maken van persoonlijke financiën.
- Het opzeggen van (ongewenste) abonnementen.
- Het heronderhandelen van lopende contracten voor een beter tarief.

Het verdienmodel van Dyme is afwijkend ten opzichte van andere huishoudboekjes: wanneer de gebruiker een abonnement via Dyme opzegt, wordt daarvoor een vergoeding gevraagd. Bij overstap naar een nieuwe energieleverancier ontvangt Dyme een commissie van de nieuwe leverancier en er wordt vergoeding gevraagd voor de onderhandel-service. De gemiddelde Dyme-gebruiker bespaart momenteel €720 op haar vaste lasten, aldus Dyme. Dyme Premium biedt extra functionaliteit en kost ongeveer 30 euro per jaar.

2.6.3.6 Grip

Grip³⁴⁷ van ABN AMRO is ook een voorbeeld van een gratis huishoudboekje dat automatisch gegevens ophaalt bij banken en daarover analyses uitvoert. Sinds 2019 heeft Grip hiervoor een PSD2 vergunning, waardoor niet alleen klanten van ABN AMRO, maar ook van andere banken Grip kunnen gebruiken.



ABN vraagt gebruikers (optionele) toestemming om aanbiedingen te doen van de bank zelf, die gepersonaliseerd zijn op basis van betaalgegevens, en van derden, die voor iedereen hetzelfde zijn. Grip toont per maand wat binnenkomt, wat eruit gaat en wat het verschil is. De gebruiker kan ook budgetten instellen. De app laat daarbij zien hoeveel andere gebruikers gemiddeld uitgeven aan zaken. Gebruikers kunnen sinds september 2020 inzicht krijgen in welke abonnementen ze hebben lopen en kunnen die ook opzeggen binnen de app. Binnen de app kunnen gebruikers hiernaast aanbiedingen van andere ABN AMRO diensten krijgen, op basis van het profiel van de gebruiker.

2.6.3.7 MijnGeldzaken.nl

Voorheen AFAS Personal, nu het online huishoudboekje van MijnGeldzaken.nl heeft een koppeling met de meeste banken in Nederland en sommige banken in België. Automatisch (via Invers/PSD2) of handmatig kunnen transacties worden ingelezen. Transacties worden direct in de juiste categorieën gezet.



Het huishoudboekje is in verschillende varianten beschikbaar, basis, plus, compleet en comfort. Een koppeling bestaat met MijnPensioenoverzicht en de Voor Ingevulde Aangifte van de Belastingdienst.

Andere functionaliteiten:

- Het is mogelijk een financieel plan te maken. MijnGeldzaken.nl geeft met een cijfer een duidelijk beeld van de financiële gezondheid. Dit bij verschillende risico scenario's; bijvoorbeeld arbeidsongeschiktheid, overlijden of werkloosheid. Het resultaat is een FPK (financieel periodieke keuring).
- Voorts is het mogelijk een onafhankelijk adviseur te consulteren in de online-advieskamer. Als de gebruiker de adviseur toegang geeft tot dossiergegevens kan deze de financiële situatie snel analyseren. Hoe meer een persoon zelf doet, hoe sneller en goedkoper het advies kan worden gegeven.
- Onderdeel van MijnGeldzaken.nl is een kluis waarin documenten opgeborgen kunnen worden.
- Als de werkgever van de gebruiker de loonstroken verstrekt met de salarissoftware van AFAS, dan kunnen deze in het Huishoudboekje worden ingelezen.
- Het is mogelijk verzekeringen te vergelijken (zorg, auto, reis, aansprakelijkheid, inboedel, opstal, rechtsbijstand) en af te sluiten.

³⁴⁷ <https://www.abnamro.nl/nl/prime/internet-en-mobiel/apps/grip/index.html>

MijnGeldzaken.nl kwam december 2020 met een mobiele app als aanvulling op de website³⁴⁸. Met de nieuwe app ziet de gebruiker in één oogopslag of de bestedingen nog in lijn zijn met het opgestelde budget en hoeveel nog te besteden is. De 'Dagelijkse uitgaven teller' helpt voorkomen dat de gebruiker in verleiding komt om te veel uit te geven. Dankzij PSD2 en automatische categorisatie van transacties is de app altijd actueel.

Coaches uit het landelijk dekkend netwerk van Budgetcoach.nl en MijnGeldzaken.nl werken samen om mensen te helpen die in problematische schuldsituaties dreigen te komen³⁴⁹. MijnGeldzaken biedt budgetcoaches de mogelijkheid om de financiële situatie van hun cliënten snel inzichtelijk te krijgen en duurzaam te verbeteren. Door de PSD2 koppeling met de betaalrekening van de cliënt worden alle uitgaven direct ingelezen en gecategoriseerd.

2.6.3.8 Huishoudboekje - Virtueel Inkomsten Lokaal, VNG Realisatie

Huishoudboekje is een Open Source product waarmee burger meer grip krijgen op hun financiële situatie. Het Huishoudboekje is voor financieel kwetsbare burgers waar vaak schuldenproblematiek speelt. De initiële ontwikkeling van het Huishoudboekje is gedaan door de gemeente Utrecht. Veel andere gemeenten in Nederland hebben hun interesse voor het Huishoudboekje kenbaar gemaakt. VNG Realisatie heeft, in samenwerking met de gemeente Utrecht de regie op zich genomen om het Huishoudboekje geschikt te maken voor generiek gebruik en dat op te schalen naar andere gemeenten in Nederland. De kopgroep voor deze opgave bestaat uit de gemeente Utrecht en Rotterdam en zal de komende periode groeien tot maximaal 5 gemeenten. Met deze kopgroep wordt op basis van de Common Ground principes, een landelijke Open Source service ontwikkeld.

2.6.4 Tools bij schuldhulpverlening en voorkomen van schulden

2.6.4.1 Buddy Payment

Buddy Payment³⁵⁰ is een internetbankieren applicatie die is gemaakt om mensen te helpen met hun bankzaken. De Buddy app geeft een overzicht van de financiële situatie van de gebruiker, scheidt vaste kosten van leefgeld en geeft financiële tips. De gebruikers kunnen zelf hun gegevens vanuit de banken en schuldeisers in de applicatie laden. Buddy is ontstaan vanuit een samenwerking tussen gemeentes en de Rabobank.

Buddy
Internetbankieren
& budget coaching

Buddy heeft begin maart 2020 een PSD2-vergunning ontvangen van De Nederlandsche Bank (DNB)³⁵¹. Met deze licentie voor Account Information Service Provider (AISP) heeft Buddy toegang tot transactiegegevens en kan het kwetsbare Nederlanders helpen financiële problemen te voorkomen en schulden te innen. Buddy doet dit door actief te budgetteren, de mogelijkheden voor toeslagen te beoordelen en ervoor te zorgen dat de vaste kosten altijd worden betaald.

De Buddy-app was oorspronkelijk een product van acht Nederlandse gemeenten, Buddy Payment en Rabobank. Buddy wil de schuldpositie van kwetsbare Nederlanders verbeteren en waar mogelijk voorkomen dat ze in een dergelijke situatie terechtkomen. Op basis van betalingsgegevens maakt de app een overzicht van iemands vaste kosten en het bedrag dat per periode vrij besteed kan worden. De app kan ook automatisch berichten naar autoriteiten sturen om naheffingen te voorkomen, bijvoorbeeld bij te late betaling of onjuiste betalingen. Het is juist dit laatste dat regelmatig de problemen veroorzaakt die al bestaan.

Naast het geven van prioriteit aan de betaling van vaste kosten, gebruikt Buddy toegang tot de betalingsgegevens om de inkomsten te schatten. Op basis hiervan beoordeelt het systeem of iemand recht heeft op toeslagen voor bijvoorbeeld huur, zorg of kinderopvang. Een kleine inkomensstijging leidt er soms toe dat iemand net boven een bepaalde grens valt en het recht op de uitkering verliest. Wie te laat komt, kan in ernstige financiële moeilijkheden komen.

Buddy richtte zich in 2021 met succes op een PISP-licentie. Nu kan Buddy Payment transacties namens hun gebruikers uitvoeren.

³⁴⁸ <https://www.vvponline.nl/nieuws/mijngeldzaken-introduceert-app?mid=k6SXpGtrI2SYkQ==>

³⁴⁹ <https://finbase.nl/artikelen-en-persberichten/budgetcoach-samenwerking/>

³⁵⁰ <https://buddypayment.nl/>

³⁵¹ <https://www.enigmaconsulting.nl/digitale-schuldhulpverlener-buddy-payment-ontvangt-psd2-licentie/>

In het voorjaar van 2020 was Buddy alleen te downloaden door klanten van gemeenten, zorginstellingen en schuldhulpverleners. Later in 2020 kwam Buddy breder beschikbaar³⁵². De nieuwste functionaliteit waaraan eind 2020 wordt gewerkt is het toetsen van toeslagen op geautomatiseerde basis.

2.6.4.2 FiKks

FiKks³⁵³ biedt gebruikers de mogelijkheid tot schuldinzage bij schuldeisers. Gebruikers kunnen FiKks machtigen inzage te krijgen op hun schulden. Deze worden geanonimiseerd opgehaald bij de authentieke bron. Een netwerk van vrijwilligers geeft vervolgens advies aan de anonieme gebruiker over oplossingen voor de schulden. Gebruikers zijn en blijven anoniem tot zij er zelf voor kiezen hun anonimiteit prijs te geven.



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

2.6.4.3 Schuldwisser

Schuldwisser³⁵⁴ is gericht op studenten en een manier om schulden in kaart te brengen. Per schuld is te zien hoelang het gaat duren voor het is afgelost.

2.6.4.4 Seev³⁵⁵

Seev (voorheen Monnie) levert een app die is gericht op jongeren en schulden moet helpen voorkomen.

2.6.4.5 MoneyFit

MoneyFit³⁵⁶ is de jongerenportal van <https://schuldhulpmaatje.nl/>.

2.6.4.6 Krap.nl

De Krap.nl app is een initiatief van de gemeente 's-Hertogenbosch en vooral bedoeld voor jongeren. De app helpt zicht te houden op inkomsten en uitgaven.

2.6.4.7 Roos

Roos³⁵⁷ zet terugkerende maandelijkse uitgaven op een rijtje. De gebruiker krijgt een seintje als hij/zij in actie moet komen omdat een abonnement afloopt. Roos regelt overstap, verlenging of opzegging.

2.6.4.8 Budlr

Budlr³⁵⁸ is gericht op financiële zorgverleners die hulp bieden aan mensen met schulden. De klant verzamelt met behulp van zijn DigiD en bankgegevens de benodigde informatie bij MijnOverheid, de Belastingdienst en zijn bank en geeft toestemming om dit te delen.

³⁵² <https://www.emerce.nl/wire/buddy-ontvangt-uniqinvestering-app-die-financieel-kwetsbare-mensen-controle-financin-helpt-terug-krijgen>

³⁵³ <https://wijgaanhetfikksen.nl>

³⁵⁴ <https://www.appone.nl/portfolio/case/schuldwisser/>

³⁵⁵ <https://www.seevapp.nl/>

³⁵⁶ <https://moneyfit.nl/>

³⁵⁷ <https://halloroos.nl/>

³⁵⁸ <https://www.budlr.nl/>

2.6.4.9 Schuldenwijzer

Schuldenwijzer³⁵⁹ is een platform dat inzicht geeft in schulden en bijbehorende informatie en de mogelijkheid biedt deze op te halen zodat deze gedeeld kan worden met partijen zoals schuldhelpverleners. Gegevens op Schuldenwijzer worden opgehaald uit het Digitaal Beslagregister (DBR). Momenteel zijn dus alleen beslagen die gerechtsdeurwaarders gelegd hebben op inkomen te zien op Schuldenwijzer. In een latere fase zullen niet alleen beslagen, maar ook andere schulden die bij gerechtsdeurwaarders bekend zijn in de Schuldenwijzer worden opgenomen. Schuldenwijzer is een initiatief van Stichting Netwerk



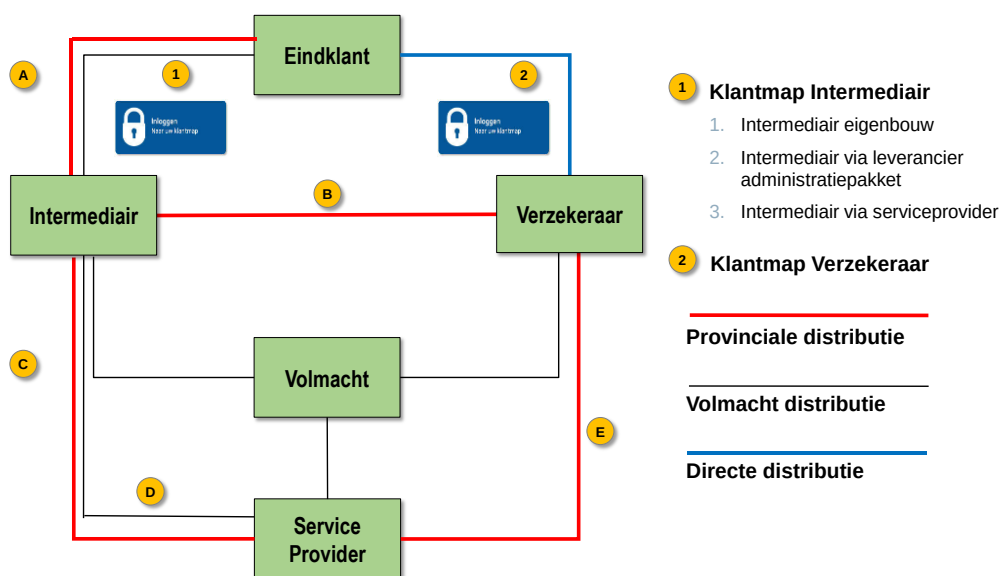
Gerechtsdeurwaarders (SNG). Aangezien partijen zoals het CJIB, gemeenten en de belastingdienst geen gebruik maken van gerechtsdeurwaarders, maar van eigen (belasting)deurwaarders zijn deze (nog) niet aangesloten op Schuldenwijzer en eventuele schulden of betalingsachterstanden bij deze partijen zijn dus niet opgenomen in de Schuldenwijzer. Belangrijk om te melden is dat de schuldenwijzer tevens geen inzicht geeft in kredieten (leningen). Deze staan geregistreerd bij BKR.

2.6.5 Klantmappen

In de Ketenintegratie Monitor Schade Particulier van SIVI is aandacht geschonken aan klantmappen. Een aantal bevindingen wordt hierna gedeeld.

Via een klantmap heeft de klant online toegang tot zijn/haar eigen klantdossier. De klant kan hier veelal heel eenvoudig polissen bekijken, mutaties doorgeven of zelf documenten uploaden. De klant ziet zo in één oogopslag welke producten hij/zij heeft lopen en heeft vierentwintig uur per dag, zeven dagen per week toegang tot zijn/haar gegevens. Daarnaast beschikt de klantmap over services waarmee de klant gemakkelijk contact op kan nemen, vragen kan stellen of zelf direct eventuele schades kan melden.

Wie biedt klantmappen aan (figuur-14):



Figuur-14: Klantmappen in de verzekeringsketen

- Klantmap Intermediair
- Intermediair Zelfbouw
- Intermediair via leverancier administratiepakket
- Intermediair via serviceprovider

³⁵⁹ <https://schuldenwijzer.nl/>

Het inrichten van klantmappen kent nog te veel drempels/vereist te veel aandacht. Intermediair kan eigenlijk alleen bij voldoende omvang of via een serviceprovider een serieuze online propositie neerzetten.

Bij de inrichting van klantmappen is datakwaliteit vaak een punt van aandacht. Vooral voor het tonen van provinciale verzekeringen binnen een klantmap is de informatieverstrekking door verzekeraars (ADN-berichten) niet altijd van voldoende niveau of compleet genoeg. Dit maakt dat met de hand moet worden aangevuld.

In de klantmap van een intermediair ziet de klant veelal alleen de polissen die via desbetreffende intermediair zijn afgesloten.

De klant kan in een klantmap zijn gegevens beheren, maar het delen met anderen wordt niet ondersteund.

(1) Klantmap Verzekeraar

In de online omgeving van de verzekeraar heeft de klant toegang tot zijn/haar klantdossier. Dit speelt vooral bij directe distributie, maar ook bij intermediaire distributie, bijvoorbeeld hypotheek.

De klantmap over alle aanbieders heen – Mijnverzekeringenopeenrij – hield in 2019 op te bestaan. Volgens het Verbond van Verzekeraars was onvoldoende capaciteit bij de verzekeraars om de website tot een volwaardige dienst te ontwikkelen³⁶⁰. Het initiatief voor Mijnverzekeringenopeenrij werd al in 2012 genomen en lag in het verlengde van de vraag vanuit de consument. Wat zeker ook meespeelde was het gegeven dat voor Mijnverzekeringenopeenrij het Burgerservicenummer van de klanten niet gebruikt mocht worden om analoog aan MijnPensioenoverzicht een Verwijsindex op te bouwen.

A. Intermediair - Eindklant

Vooral grote intermediaire organisaties ontwikkelen zelf een klantmap of kopen een hiervoor ontwikkelde software omgeving. ANVA levert generieke klantmappen, deze zijn responsive en ook op mobiel beschikbaar. ANVA gaat de PDM van Doccle hieraan verbinden. Het lijkt erop dat dit een brugfunctie gaat vormen van klantmappen naar PDM.

Veel assuratiesoftware leveranciers bieden in meer of mindere mate de optie een klantmap voor eindklanten in te richten. Daarnaast zijn er leveranciers die losse klantmap omgevingen aanbieden.

Bij het zelf ontwikkelen van een eindklantomgeving of de samenwerking met een derde leverancier is het koppelen met de assuratiesoftware niet altijd mogelijk of in functie van de omvang van het intermediair kostbaar.

A. Verzekeraar – Intermediair

Sprake is van onvoldoende ondersteuning voor kwalitatief goede data in klantmap intermediair. Huidige ADN-berichten geven geen compleet polisbeeld. Daardoor is sprake van incomplete informatie binnen assuratiesoftware en klantmap, tenzij handmatig aangevuld. Anno 2019 waar de eindklant inzicht en overzicht verwacht is een compleet update bericht en/of raadpleeg webservice gewenst.

C/D Serviceprovider – Intermediair

Een aantal serviceproviders biedt een uitgebreide ondersteuning voor de in volmacht gesloten posten. Voor provinciale verzekeringen is de ondersteuning minder, doordat een compleet polisbeeld vanuit de verzekeraar ontbreekt.

³⁶⁰ <https://www.amweb.nl/schade/nieuws/2019/03/mijnverzekeringenopeenrij-geen-lang-leven-beschoren-website-vanaf-mei-offline-101115586>

E. Verzekeraar – Serviceprovider

De afhandeling van provinciale verzekeringen creëert veel overhead bij serviceproviders. Bijkomend is het lastig een compleet polisbeeld te presenteren in dossier/klantmap. Huidige ADN-berichten geven geen compleet polisbeeld. Daardoor is sprake van incomplete informatie binnen assuratiesoftware en klantmap, tenzij handmatig aangevuld.

2.6.6 Toegang tot klantmappen: Apps

Apps bieden veelal toegang tot klantmappen en daarnaast andere functionaliteiten.

Veel zorgverzekeraars hebben apps waarmee je onder meer kunt declareren³⁶¹, onder meer door foto's te maken van je nota's. Verder zijn er vaak mogelijkheden voor correspondentie en het inzien van zorgverbruik van het lopende jaar. Inloggen kan vaak met behulp van DigiD³⁶².

De apps van schadeverzekeraars bieden veelal vergelijkbare functionaliteit:

- Schademelden;
- Polissen bekijken;
- Schadehersteller zoeken;
- Groene kaart raadplegen.

Voorbeelden van apps:

- De OHRA app³⁶³ is een verzamelplaats voor alle verzekeringen die bij Ohra lopen. Niet alleen de zorgverzekering, maar ook de reisverzekering, autoverzekering en andere producten.
- Met de Univé app³⁶⁴ is het mogelijk de voortgang van een schademelding te bekijken.
- De app van Interpolis³⁶⁵ faciliteert inloggen via iDIN.
- De app van Centraal Beheer³⁶⁶ biedt functionaliteit ten aanzien van alle financiële producten die bij Centraal Beheer zijn afgenomen.
- MijnAegon app is bedoeld voor het regelen van geldzaken³⁶⁷.
- De Nationale-Nederlanden app biedt functionaliteiten rond sparen, beleggen, schademelden, zorgkosten declareren³⁶⁸.
- De Verzekeringsapp³⁶⁹ is bedoeld voor iedereen die via een adviseur verzekerd is bij Nh1816 Verzekeringen.
- Assurantie-apps³⁷⁰ levert een app die adviseurs kunnen bieden aan hun klanten. De app bevat onder meer een PDF-scanner. Door koppelingen met systeemhuispakketten wordt toegang tot de data verleend.
- Systeemhuizen bieden apps voor de communicatie van adviseurs met klanten:
 - CCS biedt Assurantie Apps³⁷¹;
 - ANVA biedt Assurantie Apps³⁷²
- Voogd&Voogd biedt adviseurs de Polismap app³⁷³.
- De Van Kampen Groep biedt een zogenaamde progressieve webapp. Een progressieve webapp is een hybride vorm tussen een app en een website³⁷⁴.
- Serviceprovider RISK en Com Tec Co (CTCO) richtten recent een Joint Venture op om consumenten een Swift.Online app te bieden waarin je al je polissen bewaart en eenvoudig en

³⁶¹ <https://www.droidapp.nl/specials/zorgverzekering-apps/>

³⁶² <https://www.zorgwijzer.nl/zorgverzekering-2019/welke-zorgverzekeraars-hebben-een-app>

³⁶³ <https://www.ohra.nl/klantenservice/ohra-app>

³⁶⁴ <https://www.unive.nl/app>

³⁶⁵ <https://www.interpolis.nl/app>

³⁶⁶ <https://www.centraalbeheer.nl/app>

³⁶⁷ <https://www.aegon.nl/particulier/klantenservice/mijn-aegon/app>

³⁶⁸ <https://www.nn.nl/nationalederlanden-app.htm>

³⁶⁹ <https://www.verzekeringapp.nl/#Veelgestelde vragen>

³⁷⁰ <https://assurantie-apps.nl/over-ons/>

³⁷¹ <https://www.ccs.nl/partners/concapps/>

³⁷² <https://anva.nl/koppeling/assurantie-apps/>

³⁷³ <https://www.voogd.com/klant/>

³⁷⁴ <https://www.vkg.com/>

onafhankelijk verzekeringen vergelijkt, afsluit en beheert³⁷⁵. Swift Online is daarmee een van de eerste mobile-only verzekeringsplatforms.

- Mobiel Schademelden van het Verbond van verzekeraars biedt een app³⁷⁶. Hier maken meerdere verzekeraars en serviceproviders gebruik van.

2.7 Internationale PDM-Diensten

2.7.1 Yolt

Yolt is een initiatief van ING, maar richt zich op een internationale markt en met name het Verenigd Koninkrijk.³⁷⁷ Het is een applicatie die transactie-informatie vanuit meerdere rekeningen, credit cards en rekeninginformatie (zoals rentestanden) samenvoegt tot een overzicht. Dit gebeurt middels beveiligde API's, van op dit moment 25 banken.³⁷⁸ Met de applicatie kan een persoon bijvoorbeeld budgetten opstellen of een overzicht maken van lopende abonnementen. Daarnaast is betalingsfunctionaliteit beschikbaar in Yolt Pay. Waarmee vanuit de applicatie betalingen gedaan kunnen worden of geld tussen eigen accounts uitgewisseld kan worden. Het verdienmodel van Yolt is helder: er worden aanbiedingen gedaan aan personen in de app. Wanneer een aankoop wordt gedaan ontvangt Yolt hiervoor een commissie.



Yolt Technology Services (YTS) stelt andere bedrijven – techbedrijven, fintechondernemingen, financiële instellingen – in staat met elkaar te communiceren via API's. Sinds de zomer van 2019 heeft YTS een miljard API-calls afgehandeld. YTS legt verbindingen tussen partijen die actief zijn in het Open Banking ecosysteem en valt net als Yolt onder het moederbedrijf ING³⁷⁹.

2.7.2 DataYogi

DataYogi is een operator die ontwikkeld wordt in het Verenigd Koninkrijk. Het helpt bij het creëren van een overzicht in financiële gegevens. DataYogi maakt daarbij gebruik van het JLINC-protocol. Het is in DataYogi mogelijk om transactiegegevens vanuit bank of creditcard service te importeren, zodat een gebruiker zelf een overzicht kan maken. Met partijen die waarde kunnen toevoegen kunnen gegevens worden gedeeld. DataYogi is zeer recentelijk opgericht (november 2019) en nog in ontwikkeling.



2.7.3 N26 Online Bankieren

N26 is een Duitse bank en biedt een huishoudboekje dat alleen gebruikt kan worden in combinatie met een N26 betaalrekening³⁸⁰. De N26 app is geschikt voor mensen die graag hun rekeningen online of met de kaart betalen. Alle betalingen met de kaart of app worden automatisch onderverdeeld in 22 vooraf gedefinieerde categorieën en bijgehouden in een handig overzicht.



2.7.4 Swish

Swish³⁸¹ is een financiële applicatie geïnitieerd in 2015 door een consortium van zes Zweedse banken. Inmiddels zijn er meer dan zeven miljoen actieve gebruikers van Swish en 230.000 bedrijven dat betaling accepteert via Swish. Swish maakt het mogelijk om betalingen te doen aan personen en bedrijven middels een telefoonnummer. Het bedrag wordt vrijwel direct bijgeschreven op de rekening die aan



³⁷⁵ <https://www.risk.nl/risk-en-com-tec-co-starten-het-eerste-mobile-only-platform-voor-verzekeringen-swift-online/>

³⁷⁶ <https://www.mobielschademelden.nl/#/landingspagina>

³⁷⁷ <https://www.yolt.com/fags>

³⁷⁸ <https://www.yolt.com/accounts>

³⁷⁹ <https://www.banken.nl/nieuws/22661/open-banking-provider-yts-bereikt-mijlpaal-van-miljard-api-calls>

³⁸⁰ <https://n26.com/en-eu>

³⁸¹ <https://www.swish.nu/about-swish>

dat mobiele nummer is gekoppeld. In juni 2020 vonden meer dan 50 miljoen betalingen plaats.

Daarnaast zijn betalingen ook mogelijk via QR-codes, bluetooth of NFC-tags. Swish is gratis in gebruik voor personen, organisaties betalen een fee per transactie. Een account registreren is alleen mogelijk wanneer een persoon in het bezit is van een Zweedse BankID. Een gebruiker moet eerst registreren bij de bank dat hij/zij gebruik wil maken van Swish. Vervolgens moet de mobiele BankID app geïnstalleerd worden. Daarna kan het Swish account geactiveerd worden en wordt het telefoonnummer aan de betreffende bankrekening gekoppeld. Betalingen moeten steeds bevestigd worden met het BankID.

Zowel in Zweden als Noorwegen (waar de vergelijkbare Vipps-app inmiddels door het merendeel van de Noren wordt gebruikt) richtten de verschillende partijen een apart instituut op, dat de e-identity van de bankrekeninghouders beheert en beschermt.

2.7.5 Satispay

Satispay³⁸² is een Italiaanse financiële applicatie. Het is een 'wallet' applicatie die gebruikers aan een rekeningnummer koppelen. De wallet kan in winkels als betaalmiddel gebruikt worden, om contacten te betalen en om spaarpotjes aan te maken.

Een gebruiker heeft een Italiaans btw-nummer, IBAN-code en een ID nodig. Tijdens het aanmaken van een account moet een foto gemaakt worden van het paspoort, rijbewijs of ID kaart.



2.7.6 Mint

Mint³⁸³ is een Amerikaans bedrijf dat toegang regelt tot rekeningen en allerlei diensten biedt op basis van de geaggregeerde data:

- Alle accounts op één plek
- Doeltracker voor budgettering
- Gratis kredietscore
- Budgetwaarschuwingen
- Banktransacties categoriseren
- Beleggingstracker

Mint levert tevens de Mint App.



2.7.7 Finanda

Finanda³⁸⁴ is een Israëlisch bedrijf dat aggregatie diensten levert en een Personal Finance Management app.



2.7.8 Plaid

Plaid³⁸⁵ is een toonaangevende Open Banking provider in het VK, Europa en Noord-Amerika en verbindt meer dan 3.000 apps met meer dan 11.000 financiële instellingen, allemaal via een enkele API. Plaid is daarmee een API-provider voor financiële gegevensaggregatie, waarmee ontwikkelaars fintech-apps kunnen bouwen die rechtstreeks verbinding maken met bankrekeningen, betalingen mogelijk maken en financiële risico's beheren. Wat de API van Plaid doet, is dat het een directe verbinding creëert tussen de bankrekeningen van gebruikers en applicaties, waardoor deze veilig toegang hebben tot de financiële gegevens en door gemakkelijke authenticatie de veiligheid voor gebruikers garandeert.



³⁸² <https://www.satispay.com/it-it/privati/>

³⁸³ <https://www.mint.com/>

³⁸⁴ <https://www.finanda.com/en/>

³⁸⁵ <https://plaid.com/eu/>

Plaid wordt al veelvuldig gebruikt door fintech-bedrijven, zoals Venmo, TransferWise, Gusto en Level Money. Level Money, een budgetteringsapp, gebruikt bijvoorbeeld plaid om gegevens te verzamelen en te categoriseren van de verschillende bankrekeningen die de gebruiker mogelijk heeft en gebruikt die gegevens om hun klanten te helpen hun financiën te budgetteren.

2.7.9 Saltedge

Saltedge³⁸⁶ is een aggregator van bankgegevens.

De Global Data Aggregation API is de hoeksteen van de technologie van Salt Edge, met een dekking van 5461 financiële instellingen in 67 landen. Het geeft de transactiesgeschiedenis van de eindklant in een gemakkelijk te begrijpen formaat, waarbij alle transacties worden gesorteerd via een innovatieve categorisatie-engine op basis van zelflerende machine-algoritmen.



Salt Edge Connect is een widget waarmee eindklanten hun betaalrekeningen selecteren en koppelen aan een app van een andere dienstverlener. Het kan moeiteloos worden geïntegreerd met de richtlijnen van gedetailleerde documentatie. De widget is eenvoudig aan te passen onder eigen branding, zodat eindklanten zich vanaf de eerste klik op hun gemak voelen.

2.7.10 Eurobits

Eurobits³⁸⁷ is een Duitse aggregator van bankgegevens die tevens worden gecategoriseerd. Vanaf eind 2020 is Eurobits onderdeel van Tink.



2.7.11 Investnet | Yodlee

Investnet | Yodlee³⁸⁸ is een Amerikaans bedrijf voor het samenvoegen van financiële rekeningen.

Het bedrijf biedt API-oplossingen voor bedrijven die actief zijn op het gebied van Fintech met de nadruk op transactiegegevens. Investnet | Yodlee biedt tools die de werking van Fintech-apps mogelijk maken. Deze apps bieden financiële diensten aan gebruikers. De 15 grootste banken in de Verenigde Staten behoren tot hun klanten en er zijn meer dan 25 miljoen gebruikers die via genoemde apps gebruikmaken van diensten.



Investnet | Yodlee onderscheidt zich door de methodes voor gegevensverrijking. Terwijl ze onbewerkte gegevens verzamelen van een uitgebreid netwerk van financiële instellingen, gebruiken ze machine learning om de verstrekte gegevens te verfijnen en te verrijken. Het eindresultaat is een goed gestructureerde, gestandaardiseerde en gecategoriseerde data, wat een grote aanwinst is voor elk fintech-bedrijf dat inzicht wil krijgen in hun gebruikersgedrag en bestedingspatroon. Bovendien kunnen de gegevens rechtstreeks aan de klanten worden geleverd in een gemakkelijk te begrijpen formaat.

2.7.12 MX

MX werkt samen met meer dan 1.800 financiële instellingen en meer dan 40 van de top 50 aanbieders van digitaal bankieren in de Verenigde Staten en Canada. Naarmate het bedrijf is gegroeid, heeft het meer toegevoegd dan alleen gegevensaggregatie, waarbij de waardeketen is opgeschoven naar persoonlijk financieel beheer, gegevensvisualisatie en gegevensanalyse. MX werkt samen met andere data-aggregatieproviders, zodat het verkeer naar 48.000 verbindingen kan leiden, waardoor toegang tot de onderliggende accountgegevens wordt gegarandeerd. Het bedrijf straalt een partnerschapsethos uit en ziet concurrenten in de ruimte als partners. "De vraag is niet hoe hard



³⁸⁶ www.saltedge.com

³⁸⁷ <https://eurobits.com/>

³⁸⁸ <https://www.yodlee.com/europe>

andere spelers concurreren - het is wie het beste resultaat voor de gebruikers behaalt," zei medeoprichter van MX en CTO Brandon Dewitt.

Hoewel aggregatie een focus is voor het bedrijf, is MX gespecialiseerd in het leveren van andere gegevensdiensten, waaronder gegevensverbetering, presentatie en gegevensanalyse.

2.7.13 Finicity

Finicity claimt connecties bij 15.000 Noord-Amerikaanse financiële instellingen, met 95 procent dekking van Amerikaanse depositorekeningen en vergelijkbare dekking in vermogensbeheer.

Finicity onderscheidt zich bij kredietbeslissing. Het fungeert eigenlijk als een kredietrapportagebureau voor sommige van zijn producten en heeft samen met Experian en FICO onlangs een nieuwe kredietscoremethode, UltraFICO, uitgerold die de krediettoegang voor miljoenen Amerikanen zou kunnen uitbreiden.



2.7.14 CashEdge (Fiserv)

Financiële technologieprovider Fiserv kocht CashEdge in 2011 en het is nu de hoeksteen van het aanbod van Fiserv voor het samenvoegen van accounts. Fiserv heeft zijn tools voor gegevensaggregatie georganiseerd in drie verschillende producten voor een algemeen publiek, de sector financiële adviseurs, en een die fungeert als PFM.



Het aggregatieproduct van Fiserv beweert dat het \$ 30 miljard aan activa per dag verwerkt uit 18.000 gegevensbronnen, waaronder bank-, creditcard-, beleggings-, pensioen-, verzekerings- en leningsrekeningen.

2.7.15 Kontamatik

Kontamatik³⁸⁹ is een aggregator van bankgegevens. Actief in Polen, Brazilië en Tsjechië onder meer.



2.7.16 Tink³⁹⁰

Tink geeft toegang tot financiële gegevens van meer dan 3.400 banken in 18 Europese landen. De afnemer krijgt up-to-date, opgeschoonde en gecategoriseerde transactiegegevens. Tink verwerkt meer dan 1 miljard maandelijkse API-aanroepen met 99,9%+ uptime. Tink levert tevens Personal Finance Management Tools.

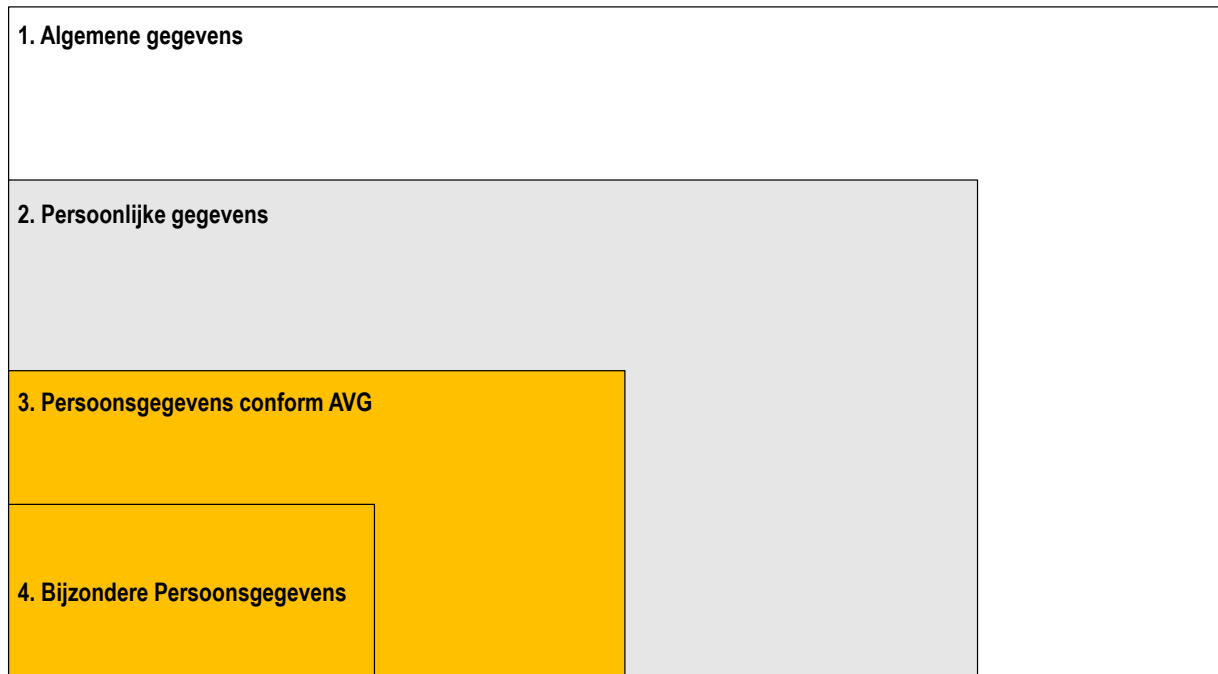


³⁸⁹ <https://www.kontomatik.com/>

³⁹⁰ <https://tink.com/>

3. BIJLAGE C - WAT ZIJN PERSOONSgegevens?

In de greenpaper 'De consument bepaalt!' uit 2017 schreef SIVI al het nodige over persoonsgegevens. Figuur-15 toont een verdeling van de verschillende categorieën gegevens.



Figuur-15: 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.

Aangifte diefstal

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 en mogen niet zomaar verstrekt worden, tenzij er een expliciete uitzondering voor is.

Persoonsgegevens, Bijzondere persoonsgegevens, Algemene gegevens

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. BIJLAGE D – AFKORTINGEN- EN BEGRIPPENLIJST

4.1 Afkortingen

Afkorting	Betekenis
ACM	Autoriteit Consument en Markt
AFCAR	Alliance for the Freedom of Car Repair
AFM	Autoriteit Financiële Markten
AISP	Account Information Service Provider
AP	Autoriteit Persoonsgegevens
API	Application Programming Interface
AVG	Algemene verordening gegevensbescherming
BEUC	Bureau Européen des Unions de Consommateurs
BoF	Bits Of Freedom
BZK	Het ministerie van Binnenlandse Zaken
CDR	Consumer Data Right - Australië
DBC	Dutch Blockchain Coalition
DBI	Digitale Bron Identiteit
DDMA	Data Driven Marketing Association
DDTF	Dutch Digital Trust Framework
DNB	De Nederlandse Bank
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eIDAS	Electronic Identification Authentication and trust Services Dit is een Europese verordening "betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt"
ESSIF	Europees Self-sovereign Identity Framework
ETD	Elektronische toegangsdiensten
HDN	Hypotheken Data Netwerk
ICTU	ICT Uitvoeringsorganisatie
IDSA	International Data Spaces Association
IDSA	International Data Spaces Association
IRMA	I Reveal My Attributes, een techniek waarmee een persoon alleen die persoonlijke gegevens hoeft te delen die op dat moment relevant zijn ter controle
MIT	Massachusetts Institute for Technology
MKBA	Maatschappelijke kosten-batenanalyse
NEN	Stichting Koninklijk Nederlands Normalisatie Instituut
NLX	NLX is een open source peer-to-peer systeem dat federatieve authenticatie, veilige verbindingen en protocollering mogelijk maakt in een grootschalig, dynamisch API-ecosysteem met veel organisaties
NVB	Nederlandse Vereniging van Banken
OAuth	OAuth (Open Authorization) is een open standaard voor autorisatie
PDEC	Personal Data Ecosystem Consortium
PDM	Personal Data Management
PDS	Personal Data Stores
PDW	Personal Data Wallets
PET	Privacy Enhancing Technologies
PGO	Persoonlijke Gezondheidsomgeving
PI-lab	Privacy & Identity Lab
PIMS	Personal Information Management Systems
PISP	Payment Initiation Service Provider
PKI	Public Key Infrastructure
PSD2	De Payment Services Directive is een Europese richtlijn die in 2007 werd aangenomen door de Europese Commissie om betaaldiensten te reguleren. Op basis van PSD2 halen bijvoorbeeld dienstverleners als Invers met toestemming van de klant banktransacties op en analyseren deze.
ROG	Regie Op Gegevens
ROPG	Regie Op Persoonsgegevens

Afkorting	Betekenis
RvIG	Rijksdienst voor Identiteitsgegevens
SAML	Security Assertion Markup Language is een standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen
SDG	Single Digital Gateway
S-OTP	Secure On-Board Telematics Platform
SSI	Self Sovereign Identity. De gebruiker kan met SSI zijn identiteit bewaren in een soort digitale portefeuille en bepalen welke gegevens gedeeld worden met dienstverleners
SZW	Ministerie van Sociale Zaken en Werkgelegenheid
TNO	Nederlandse Centrale Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
UMA	User-Managed Access is een op OAuth gebaseerde protocolstandaard voor toegangsbeheer
vID	Virtueel identiteitsbewijs
Wabb	Wet algemene bepalingen Burgerservicenummer
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
WAMCA	Wet afwikkeling massaschade in collectieve actie
WDO	Wet Digitale Overheid
Wegiz	wetsvoorstel elektronische gegevensuitwisseling in de zorg
WGBO	Wet Geneeskundige Behandelovereenkomst
WID	Wet op de Identificatieplicht
WRR	Wetenschappelijke Raad Regeringsbeleid

4.2 Gedefinieerde begrippen

A

Account aggregatie
 Afgeleid digitaal/elektronisch identificatiemiddel
 Afgeleid gegeven
 Afsprakenstelsel
 Algoritme
 Anoniem (of: geanonimiseerd)
 Anonimisering
 API
 Artikel 29 werkgroep
 Authenticatie (authenticeren)
 Authenticatiedienst
 Authenticatiefactor
 Authenticatiemiddel
 Autorisatie
 Autoritatieve bron
 AVG en gewone en bijzondere persoonsgegevens
 AVG en Persoonsgegevens
 AVG en Proportionaliteit en subsidiariteit
 AVG en Toestemming
 AVG en verwerken van persoonsgegevens

B

Betrouwbaarheidsniveau
 Bijzonder gegeven
 Biometrie
 Blockchain
 Brongegeven
 Burger
 Burger

C

Categorieën Persoonsgegevens
 Community
 Concept

Consument

D

Data aanbieder

Data afnemer

Data Exchange

Data Governance

Data-aggregator

Dataminimalisatie

Derden bewering

Dienstverlener

Digitaal/elektronische identificatiemiddel

Digitale bron identiteit (DBI)

Digitale identiteit

Digitale/elektronische identificatie

Digitale/elektronische identiteit

Digitale/elektronische identiteit infrastructuur

E

Ecosysteem

Ecosysteem voor gegevensuitwisseling

eIDAS

Eigen bewering

F

Federatieve Authenticatie

Feit

G

Gegevenscatalogus

Gegevensoverdraagbaarheid

Gespecificeerde toestemming (zorgsector)

Gezaghebbende bron

Governance

I

Idemix

Idensys

Identificatie

Identificatie/Identificeren

Identificeerbaar

Identiteit

Inbreuk in verband met persoonsgegevens

Individu

Inlogmiddel

Interoperabiliteit

M

Machtiging

Middelenuitgever

Multi-factor Authenticatie (MFA)

O

OAuth

Open Finance

OpenID

Operator

Overheid

P

PDM Afsprakenstelsel

PDM-Dienst

Persoon

Persoonlijk Data Management (PDM)

Persoonlijke Digitale Omgeving

Persoonlijke financiële planning
 Persoonlijke Gezondheidsomgeving
 Persoons identificerende gegevens
 Persoonsgegevens
 Persoonsgegevens
 Persoonsidentificatiegegevens
 Privacy By Design
 Privacy Enhancing Technologies (PET)
 Protocol
 Pseudonimisering

Q

Qiy Trust Principles (belangrijkste)

R

Recht om vergeten te worden
 Regie Op Gegevens (overheid)
 Regie op Persoonsgegevens (ROPG)
 Regietoepassing

S

SAML
 Scraping
 Self-sovrin identity
 Single Sign On (SSO)
 Standaard

T

Toestemming/consent
 Token

U

Verifiable credentials
 Vertegenwoordiger

W

Waarmerk

X

X-Tee

Z

Zero Knowledge Proof

4.3 Definities

Begrip	Uitleg
Account aggregatie	Account aggregatie staat soms ook wel bekend als financiële data-aggregatie. Het is een methode die het verzamelen van gegevens uit verschillende rekeningen op 1 plaats mogelijk maakt.
Afgeleid digitaal/elektronisch identificatiemiddel	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P. Een middel om een (rechts)persoon aan een bepaalde geregistreerde identiteit te linken. Deze identiteit is afgeleid van een digitale bronidentiteit van een (rechts)persoon zoals door de overheid vastgelegd.
Afgeleid gegeven	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Een afgeleid gegeven is een gegeven dat verkregen wordt door de toepassing van regels (algoritmen) op brongegevens of andere afgeleide gegevens. Afgeleid gegeven en conclusie worden hier als synoniem gebruikt.

Begrip	Uitleg
Afsprakenstelsel	Set van vastgelegde specificaties, regels en afspraken om samenwerking en zekerheid te garanderen op het gebied van technische functionaliteiten, beveiliging en privacy voor het uitwisselen van persoonlijke data. Afsprakenstelsels geven hiermee richting of stellen eisen aan PDM-oplossingen. Eisen kunnen van technische aard zijn, bijvoorbeeld door het gebruik van bepaalde standaarden af te dwingen, maar kunnen bijvoorbeeld ook ingaan op het verdienmodel van een PDM-oplossing. Horizontale afsprakenstelsels Een afsprakenstelsel voor PDM kan sectoronafhankelijk zijn. Dit is een horizontaal afsprakenstelsel. Een voorbeeld is Qiy en het afsprakenstelsel van de overheid voor Elektronische Toegangsdiensten. Verticale afsprakenstelsels 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 (MedMij) en de sector logistiek voor iSHARE. iSHARE timmert qua implementatie flink aan de weg. MedMij is een belangrijk verticaal afsprakenstelsel in Nederland. Enerzijds vanwege het belang dat het delen van medische gegevens heeft voor mensen, maar ook omdat het qua opzet en gedetailleerde uitwerking breed gedragen wordt, geflankeerd door wetgeving die een en ander afdwingt. Voorts is over de adoptiestrategie veel nagedacht.
Algoritme	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Een <u>algoritme</u> is een set instructies om een bepaalde taak uit te voeren. Aan de hand van data die in het algoritme worden ingevoerd, wordt in verschillende stappen toegewerkt naar het beoogde eindresultaat, bijvoorbeeld het toekennen van een toeslag. Op basis van dat resultaat kan men dan actie ondernemen (toeslag wel of niet toekennen). De precieze stappen die worden doorlopen verschillen per algoritme. In het algemeen geldt dat deze stappen variabelen bevatten, bijvoorbeeld de hoogte van het inkomen als relevante factor voor het toekennen van de toeslag. Er bestaan verschillende typen algoritmes. Het algoritme voor het toekennen van een toeslag heeft doorgaans het karakter van een eenvoudige beslisboom (rule based) met een beperkt aantal variabelen en drempelwaarden, bijvoorbeeld dat om voor een toeslag in aanmerking te komen het inkomen lager dient te zijn dan bedrag x. Een algoritme kan ook meer complex zijn en bijvoorbeeld op basis van een aantal casussen voorspellingen doen over nog niet bekende gevallen (case based) of gebruikt worden voor gezichts- of objectherkenning. We betreden dan de wereld van machine learning, deep learning, zelflerende algoritmes en kunstmatige intelligentie.
Anoniem (of: geanonimiseerd)	Niet traceerbaar naar de persoon.
Anonimisering	Bron: https://wso2.com/library/article/2018/2/identity-and-access-management-to-the-rescue/ Anonimisering is het proces waarbij persoonlijk identificeerbare informatie uit datasets wordt verwijderd. Na anonimisering is een persoon niet langer identificeerbaar op basis van de resterende gegevens binnen het systeem.
API	Een application programming interface (API) is een gestructureerd en gedocumenteerd koppelvlak voor communicatie tussen applicaties. Voor steeds meer organisaties vormen API's (bibliotheek met webservices) de sleutelrol in het

Begrip	Uitleg
	aanbieden van transacties, het distribueren van content of het ontsluiten van een workflow tussen schakels in de keten. Binnen de synchrone communicatie initieert de distributie (intermediairs, volmachten, serviceproviders) het merendeel van de transacties. De reden hiervoor is dat de meeste synchrone services midden in primaire processen als tariefberekening, offerte, aanvraag, mutaties en claim gebruikt worden. Deze services stellen intermediairs, volmachten en serviceproviders in staat direct hun werk te doen.
Artikel 29 werkgroep	De Artikel 29-werkgroep bestond uit de nationale privacytoezichthouders 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 had een onafhankelijk en raadgevend karakter. De belangrijkste taak van de werkgroep was het bevorderen van een uniforme toepassing van de principes uit de privacyrichtlijn in alle lidstaten door samenwerking tussen de Europese toezichthouders. Ook coördineerde de werkgroep gezamenlijk onderzoek en de hieruit voortvloeiende nationale handhaving van de toezichthouders. Met de komst van de European Data Protection Board is de Artikel 29 werkgroep opgeheven.
Authenticatie (authenticeren)	De controle van een geclaimde identiteit (set geclaimde attributen) van een entiteit, op een gegeven betrouwbaarheidsniveau. Authenticatie is dus het proces dat nagaat of een gebruiker daadwerkelijk is wie hij/zij beweert te zijn. Dat wil zeggen: daadwerkelijk de identiteit bezit die hij/zij opgeeft. Deze vastgestelde identiteit bepaalt of de betreffende gebruiker gerechtigd is om een bepaalde handeling te verrichten of een service af te nemen; deze volgende stap noemen we autorisatie. Authenticatie bestaat uit twee stappen. Bij de registratiefase wordt eenmalig een account gemaakt op basis van persoonsgegevens. Hoe grondig hierbij wordt gecontroleerd of de persoonsgegevens daadwerkelijk bij de betreffende persoon horen, bepaalt de betrouwbaarheid: face-to-face-controle met een paspoort bij een balie, leidt tot een hogere mate van betrouwbaarheid dan een gebruiker die online zijn/haar gegevens invoert. Heeft de gebruiker eenmaal een account, dan kan hij/zij zich hier voortaan mee authenticeren. In deze inlogfase wordt vanaf nu alleen nog vastgesteld dat het om dezelfde gebruiker gaat als die ook de account aanmaakte. Ook hier hangt de betrouwbaarheid af van de mate waarin dit gecontroleerd wordt: enkel het invullen van een wachtwoord wordt als minder betrouwbaar verondersteld dan bijvoorbeeld een gezichtsscan of het invoeren van een extra code via de gsm van de gebruiker.
Authenticatiedienst	Een dienstverlener die tenminste identiteitsgegevens van entiteiten aanmaakt, onderhoudt en beheert, en hen authenticiseert ten behoeve van online-dienstverlening. Treedt vaak ook op als middelenuitgever.
Authenticatiefactor	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de drie volgende categorieën valt. (1) Op bezit gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is. (2) Op kennis gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt. (3) Inherente authenticatiefactor: een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit.

Begrip	Uitleg
Authenticatiemiddel	Het middel dat de gebruiker aanwendt bij authenticatie; iets wat de gebruiker weet, bezit of is.
Autorisatie	Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren. Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie. Autorisatie is geen synoniem voor machtiging.
Autoritatieve bron	Gezaghebbende, erkende bron van persoonlijke gevalideerde gegevens.
AVG en gewone en bijzondere persoonsgegevens	De AVG kent gewone en bijzondere persoonsgegevens. Deze laatste categorie is nader uitgewerkt in de AVG en in de UAVG. Persoonsgegevens die door hun aard bijzonder gevoelig zijn verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden. Voor de bijzondere persoonsgegevens geldt daarom een verwerkingsverbod tenzij voldaan is aan in de AVG en in de UAVG opgesomde voorwaarden. Een voorbeeld van een gewoon persoonsgegeven is een naam of een adres en een voorbeeld van bijzondere persoonsgegevens zijn gegevens over gezondheid.
AVG en Persoonsgegevens	Persoonsgegevens zijn alle gegevens die informatie bevatten over een in leven zijnde persoon. Dat kan direct zijn, maar ook indirect als het gegeven tot een burger te herleiden is.
AVG en Proportionaliteit en subsidiariteit	Het vereiste van proportionaliteit houdt in dat het doel van het uitwisselen van gegevens in verhouding moet staan tot de inmenging in de persoonlijke levenssfeer. Het vereiste van subsidiariteit houdt in dat het doel niet ook op een andere manier dan het uitwisselen van gegevens kan worden behaald.
AVG en Toestemming	Een andere rechtsgrond genoemd in de AVG is de toestemming van de burger voor het verwerken van zijn persoonsgegevens voor een of meer specifieke doeleinden. Deze rechtsgrond is nader uitgewerkt in de AVG. Zo moet toestemming vrijelijk, specifiek en ondubbelzinnig worden gegeven.
AVG en verwerken van persoonsgegevens	Bij het verwerken van persoonsgegevens gaat het om alle handelingen die met persoonsgegevens kunnen worden uitgevoerd, zoals bijvoorbeeld verzamelen, vastleggen, bewaren, opslaan, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen. Als er geen persoonsgegevens worden verwerkt is de AVG niet van toepassing. Dat zal echter niet snel het geval zijn.
Betrouwbaarheidsniveau	Een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie. Dit niveau wordt bepaald door een samenhangend geheel van factoren, zoals de sterkte van de identiteitsverificatie tijdens de registratie en uitgifte van het authenticatiemiddel, de sterkte van het middel zelf en de sterkte het authenticatiemechanisme.
Bijzonder gegeven	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Dit zijn gegevens over iemands: • ras of etnische afkomst; • politieke opvattingen; • godsdienst of levensovertuiging;

Begrip	Uitleg
	• lidmaatschap van een vakbond; • genetische of biometrische gegevens met oog op unieke identificatie; • gezondheid; • seksuele leven; • strafrechtelijk verleden. Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is.
Biometrie	Bron: Biometrie voor identiteitsverificatie, Verkenning van de mogelijkheden, InnoValor 2020 Biometrische identiteit: Unieke set van onveranderlijke dan wel langdurig stabiele fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon. Deze kenmerken zijn uniek identificerend en worden gebruikt in biometrische systemen om iemand te herkennen en de identiteit vast te stellen.
Blockchain	Een Blockchain, ook wel een toepassing van distributed ledger, is een lijst van transacties (blokken), die aan elkaar gelinkt zijn. Blockchain transacties kunnen, nadat het grootste deel van de deelnemers in de blockchain de transactie heeft goedgekeurd, niet meer worden gewijzigd. Dit maakt het blockchain systeem erg uniek, samen met het decentrale karakter: er is niet één organisatie die alles te zeggen heeft. Blockchain implementaties zijn geen voor de hand liggende manier om persoonsgegevens uit te wisselen, omdat data voor iedereen toegankelijk is, kan iedereen alles zien. Blockchain biedt mogelijk oplossingen als er geen vertrouwen is in de sector of een centrale partij.
Brongegeven	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Brongegeven is het gegeven zoals deze zich in de administratie van de overheid bevindt.
Burger	Bron: Programmaplan Regie op Gegevens, Fase II Fundament en doorkijk naar de invoering 26/11/2020, consultatie concept stuurgroep RoG. Dit betreffen natuurlijke personen in de rol van burger (relatie met de overheid) of consument (relatie met ondernemingen) die namens zichzelf of voor een andere burger handelt (horizontale vertegenwoordiging). Voorbeelden van de laatste categorie is de mantelzorger of de ouder/kind relatie.
Burger	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Onder burger wordt hier verstaan iedere natuurlijke persoon die ingezetene is in Nederland (zoals opgenomen in de BRP) en iedere natuurlijke persoon die opgenomen is in het Register Niet-Ingezetenen RNI (niet-ingezetene met een relatie met de Nederlandse overheid).
Categorieën Persoonsgegevens	Bron: Programmaplan Regie op Gegevens, Fase II Fundament en doorkijk naar de invoering 26/11/2020, consultatie concept stuurgroep RoG

Begrip	Uitleg
	• (persoons)gegevens in (basis-)registers en administraties zoals geboortedatum, geboorteplaats, adres. Feitelijk betreffen dit de eigenschappen en/of kenmerken in records behorend bij de burger. In deze fase zal bepaald worden of hier sprake moet zijn van persoonsgebonden of persoon gerelateerde (in termen van 'betreffende een persoon') gegevens. • beweringen die iets zeggen over de burger op basis van bewerking op een gegeven bijv. ouder dan 21 jaar, afloscapaciteit bij schuldsanering of informatie op basis van een bewerking in een proces bijv. een verklaring omtrent gedrag, BIG registratie. • Gewaarmerkte digitale waardedocumenten, niet zijnde de fysieke documenten of gescande 'platte' Pdf-bestanden: identiteitsdocumenten zoals paspoort, NIK en/of rijbewijs, diploma's, verzekeringsdocumenten.
Community	Binnen een community zijn partijen met een gezamenlijk doel op het terrein van ketenoptimalisatie met elkaar verbonden. Een community maakt hierover afspraken. Overleg vindt plaats met grote betrokkenheid van deelnemers omdat de deelnemers dezelfde interesse en doelen delen.
Concept	Een concept is een abstract idee of plan van hoe bepaalde technologie kan werken om een proces te laten verlopen. Technologische concepten kunnen doorgroeien tot bijvoorbeeld protocollen, standaarden.
Consument	De natuurlijke, levende persoon. Ook klant of gebruiker genoemd.
Data aanbieder	Een partij die persoonlijke data verzamelt en verwerkt die de andere partijen/rollen mogelijk willen inzien of gebruiken.
Data afnemer	Partij die geautoriseerd kan worden om data in te zien of gebruiken van een of meerdere data aanbieders.
Data Exchange	Data Exchange binnen de financiële sector is de techniek waarbij de data van verschillende geautomatiseerde toepassingen op geautomatiseerde wijze met elkaar uitwisselbaar zijn op basis van gemaakte afspraken over onder andere standaarden.
Data Governance	Een systeem dat interoperabiliteitscomponenten (standaarden en beleidsregels) toepast om het acceptabele gebruik en de hoge kwaliteit van gegevens binnen een specifiek ecosysteem te garanderen. Beheert de beschikbaarheid, bruikbaarheid, consistentie, integriteit en beveiliging van de gebruikte gegevens.
Data-aggregator	En toepassing die data uit meerdere databronnen verzamelt met de bedoeling gecombineerde datasets voor te bereiden voor dataverwerking.
Dataminimalisatie	Bron: Referentiearchitectuur ROG, ICTU 2021 Binnen de context van RoG zijn hierbij globaal drie strategieën te onderkennen: • Alleen die gegevens die strikt noodzakelijk zijn voor het beantwoorden van de vraag (dataminimalisatie door filteren) • Conclusie als gegeven en niet de gegevens die leiden tot de conclusie (dataminimalisatie door delen conclusies) • Cryptografisch bewijs over gegevens zonder de gegevens zelf te delen (dataminimalisatie door wiskundig bewijs)
Derden bewering	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021

Begrip	Uitleg
	Een derden bewering is een bewering die (in deze context) de overheid over een burger doet.
Dienstverlener	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 De dienstverlener is iedere private partij die een dienst levert.
Digitaal/elektronische identificatiemiddel	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst.
Digitale bron identiteit (DBI)	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een unieke, betrouwbare, inclusieve, veilige en door de overheid uitgegeven en erkende digitale identiteit voor entiteiten.
Digitale identiteit	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie, object of apparaat) representeren in het digitale domein.
Digitale/elektronische identificatie	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.
Digitale/elektronische identiteit	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een identiteit in de onlinewereld voor entiteiten. Een digitale identiteit kan bestaan uit verschillende aspecten (attributen) die over een bepaalde entiteit geregistreerd staan. ISO/IEC stelt: een digitale identiteit is een set attributen die te relateren zijn aan een entiteit.
Digitale/elektronische identiteit infrastructuur	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Het geheel van stelsels, afspraken, standaarden en voorzieningen, rond de digitale identiteit van (rechts)personen.
Ecosysteem	Het totale systeem dat is gecreëerd door de activiteiten en verbindingen tussen actoren en infrastructuur volgens een gemeenschappelijke reeks regels. Meerdere ecosystemen kunnen bestaan, overlappen en samenwerken. Governance is in dit verband een systeem van regels, praktijken en processen dat wordt gebruikt om een Ecosysteem te managen.
Ecosysteem voor gegevensuitwisseling	Bron: Programma Regie Op Gegevens van de Nederlandse overheid Een (eco-)systeem voor gegevensuitwisseling is een online omgeving voor het uitwisselen en delen van persoonsgegevens. Zo'n systeem kan in de vorm van een afsprakenstelsel worden beheerd. Individuen, organisaties, services en apparaten kunnen elkaar daarbij vertrouwen omdat gezaghebbende bronnen de gegevens en de uitwisseling verifiëren. Een dergelijk ecosysteem onder beheer van een afsprakenstelsel betreft: • Een reeks regels, methoden, procedures, technologie, normen, beleid en processen; • Van toepassing op een groep deelnemende entiteiten;

Begrip	Uitleg
	- Met betrekking tot de verzameling, verificatie, opslag, uitwisseling, authenticatie en vertrouwen op attribuut-informatie over een persoon, organisatie, apparaat of digitaal object; - Ten behoeve van het faciliteren van gegevensuitwisseling.
eIDAS	eIDAS staat voor Electronic Identification (eID) and Trust Services (AS). Het is een initiatief van de Europese Commissie met als doel om elektronische interacties tussen ondernemingen, burgers en organisaties veiliger en efficiënter te maken en alle EU landen elkaars eID en AS erkennen.
Eigen bewering	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Onder bewering wordt hier de neutrale en niet-geverifieerde status van een gegeven verstaan en deze kan dus waar of niet waar zijn. Een eigen bewering is een bewering die de burger zelf doet.
Federatieve Authenticatie	Wanneer men federatief authenticiseert wordt aan een vertrouwde partij gevraagd om de authenticatie af te handelen. Deze vertrouwde partij geeft vervolgens terug of er juist geauthentiseerd is, en geeft een aantal gevraagde attributen terug zodat eventueel ook geautoriseerd kan worden. Bron: https://kb.grip-on-it.com/nl/service-integration/openidconnect/ Federatieve authenticatie betekent simpel gezegd dat een dienst (Service Provider) de authenticatie 'uitbested' aan een Identity Provider.
Feit	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Zodra een bewering geverifieerd en/of geaccepteerd is, krijgt dit gegeven de status van feit en is daarmee uitgangspunt voor het vervolg van het proces.
Gegevenscatalogus	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Een gegevenscatalogus is een beschrijving van zowel bron- als afgeleide gegevens die door de (in casu) overheid geleverd kunnen worden. Deze beschrijving bevat tenminste per gegeven de metadata, context, semantiek, uitspraken over kwaliteit en levercondities. Een voorbeeld van zo'n gegevenscatalogus is de Stelselcatalogus.
Gegevensoverdraagbaarheid	Dataportabiliteit. De mogelijkheid om gegevens gemakkelijk te verplaatsen tussen interoperabele toepassingen en domeinen.
Gespecificeerde toestemming (zorgsector)	Per een nader vast te stellen data moeten burgers hun eigen gegevens digitaal kunnen inzien (online inzage) en kunnen aangeven welke soort gegevens met welke zorgaanbieders mogen worden uitgewisseld bij behandeling (gespecificeerde toestemming). Gespecificeerd betekent dat burgers straks kunnen specificeren welke categorie van gegevens met welke categorie zorgverleners wel of niet gedeeld mag worden.
Gezaghebbende bron	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P. Elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond.

Begrip	Uitleg
Governance	Bron: Analyse Governance afsprakenstelsels voor Programma Regie Op Gegevens, PBLQ 2019 Een reeks van processen (tradities, beleid of regels) die formeel en/of informeel worden toegepast om verantwoordelijkheden tussen actoren van een bepaald systeem te verdelen. Governance gaat daarmee over actoren, relaties en de manier waarop een gezamenlijk doel wordt bereikt. De governance omschrijft op welke wijze de afspraken worden beheerd, welke rollen daarin te onderkennen zijn en door welke partijen die rollen worden vervuld.
Idemix	Bron: IBM Idemix is een protocol waarmee een partij gegevens kan opvragen van verschillende partijen en deze vervolgens weer anoniem en unlinkable³⁹¹ kan delen met andere partijen. Idemix gebruikt zero-knowledge proofs en wordt gebruikt in IRMA.
Idensys	Met Idensys konden gebruikers op verschillende veiligheid niveaus inloggen bij publieke en private diensten. Bij Idensys kon worden ingelogd via een speciaal account aangevraagd bij KPN, Reconi of Digidentity. Het Idensys afsprakenstelsel deed samen met iDIN mee aan een overheids-pilot voor het gebruik van private inlogmiddelen bij publieke diensten, zoals de Belastingdienst. De Idensys pilot is in 2018 stopgezet; er kan niet meer mee worden ingelogd bij overheidsdiensten.
Identificatie	Uit de eIDAS regulering, art 3. 'Definities Registratie van een unieke identiteit (vaststelling en creatie) en vervolgens het uitgeven van een identificatiemiddel om personen in staat te stellen om deze identiteit te laten verifiëren.
Identificatie/Identificeren	Het overleggen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden.
Identificeerbaar	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Als <u>identificeerbaar</u> wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Identiteit	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een identiteit bestaat uit de geregistreerde aspecten (attributen) die in voldoende mate bepalen wie iemand of iets is.
Inbreuk in verband met persoonsgegevens	De AVG kent net als de oude Wet Bescherming Persoonsgegevens 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:

³⁹¹ the ability of a single identity to send multiple transactions without revealing that the transactions were sent by the same identity (<https://hyperledger-fabric.readthedocs.io/en/release-2.0/Idemix.html>)

Begrip	Uitleg
	- 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.
Individu	Persoon. Een persoon in relatie tot de overheid wordt vaak aangeduid als burger. Een persoon in relatie tot de dienstverleners wordt vaak aangeduid als consument.
Inlogmiddel	Zie authenticatiemiddel.
Interoperabiliteit	Het vermogen van verschillende systemen om met elkaar samen te werken en voor apparaten, applicaties of producten om verbinding te maken en te communiceren in een gecoördineerde manier, zonder inspanning van de persoon. In het European Interoperability Framework³⁹² worden drie vormen van interoperabiliteit onderscheiden: 1. Technische interoperabiliteit – Om systemen te kunnen koppelen, moeten er afspraken worden gemaakt over interfaces, standaarden en protocollen voor communicatie, berichtenformaten, gegevensintegratie, beveiliging, beschikbaarheid, etc. 2. Semantische interoperabiliteit – De informatie die partijen uitwisselen, moet wederzijds begrijpelijk zijn. Context en betekenis van gegevens moet eenduidig zijn vastgelegd. 3. Organisatorische interoperabiliteit – Om gezamenlijke diensten te kunnen leveren, moeten organisaties op elkaar zijn afgestemd in termen van hun businessdoelen, verdeling van verantwoordelijkheden en uitwisselingsprocessen.
Machtiging	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Een toestemming van de burger aan de dienstverlener om namens hem gegevens over hem in te winnen bij de overheid. Deze toestemming kan ook vooraf gegeven worden bij de bron: de overheid machtigt de overheid om (onder bepaalde condities) persoonsgegevens te leveren aan een dienstverlener indien deze daarom vraagt.
Middelenuitgever	Verantwoordelijk voor de uitgifte van authenticatiemiddelen en alle daaraan verbonden processen: aanvraag, registratie, activering, blokkering/heractivering, inname en opheffing. Vaak treedt de middelenuitgever ook op als authenticatiedienst.
Multi-factor Authenticatie (MFA)	Dit is een authenticatie methode waarbij de onlinegebruiker twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen.

³⁹² <https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/eif-european-interoperability-framework-0>

Begrip	Uitleg
OAuth	OAuth 2.0 ³⁹³ is een standaard die ingezet kan worden om iemand tijdelijk toegang te geven tot een deel van je gegevens zonder hiervoor je wachtwoord te delen met de betreffende partij.
Open Finance	Het samenbrengen van alle financiële gegevens van een consument. Van het pensioenpotje tot de beleggingsrekening en van het spaartegoed tot de hypotheek.
OpenID	OpenID Connect ³⁹⁴ is een standaard waarbij gebruikers federatief kunnen inloggen. Dit betekent dat iemand kan inloggen met een account van partij A (ook wel, de authenticatie provider) bij partij B (de resource provider). Er wordt dus een vertrouwde partij gebruikt voor authenticatie. Een bekende variant hiervan is het gebruik maken van een Google inlog voor een dienst. OpenID Connect bouwt, net als UMA, verder op de OAuth standaard.
Operator	Een operator maakt het mogelijk voor het individu om veilig persoonlijke data in te zien, te gebruiken en te managen. Daarnaast maakt de operator het mogelijk om de uitwisseling van persoonlijke data met en tussen data aanbieders en afnemers te controleren. Buiten deze rollen kan er nog een rol of entiteit zijn die het beheer van de afspraken en toezicht op het systeem regelt (governance). De operator acteert als 'broker' van gegevens: de operator maakt persoonlijke gegevens inzichtelijk, faciliteert gegevensuitwisseling en voorziet in consentmanagement. Functioneel kan een operator verschillende vormen aannemen: niet elke operator voorziet bijvoorbeeld in het wijzigen van consent. Sommige operators fungeren als 'datakluis' terwijl andere puur gegevens uitwisselen, maar niet zelf bewaren.
Operator	De rol die verantwoordelijk is voor de operationele infrastructuur en het leveren van tools voor de persoon in een mensgericht systeem van uitwisseling van persoonsgegevens. Operators stellen mensen in staat om veilig toegang te krijgen tot persoonlijke gegevens en deze te beheren en te gebruiken en controle uit te oefenen over de stroom van persoonsgegevens tussen gegevensbronnen en services die gegevens gebruiken.
Overheid	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Iedere overheidsorganisatie die persoonsgegevens over een burger administreert die door die burger ingezien mogen worden.
PDM Afsprakenstelsel	Set van vastgelegde afspraken om samenwerking en zekerheid te garanderen op het gebied van technische functionaliteiten, beveiliging en privacy voor het uitwisselen van persoonlijke data. Bron: Programma Regie Op Gegevens van de Nederlandse overheid Een afsprakenstelsel is een juridisch afdwingbare set specificaties, regels en overeenkomsten dat een ecosysteem bestuurt. Binnen het kader van Regie Op Gegevens betreft dit een systeem voor gegevensuitwisseling.
PDM-Dienst	Een dienst die een individu in staat stelt om zijn persoonlijke data duurzaam te beheren en te onderhouden om deze, wanneer de gebruiker dit in zijn belang acht, te kunnen delen met anderen.

³⁹³ <https://oauth.net/2/>

³⁹⁴ <https://openid.net/connect/>

Begrip	Uitleg
	Andere termen zijn om deze diensten aan te duiden zijn PDM-services, PDM-oplossingen, Regietoepassingen, Personal Information Management Systems (PIMS), Personal Data Stores (PDS) en Personal Data Wallets (PDW).
Persoon	Natuurlijk persoon of ondernemer.
Persoonlijk Data Management (PDM)	Het concept rond het duurzaam beheren en onderhouden van persoonlijke data. Persoonlijk datamanagement, ofwel PDM, betekent dat mensen (persoonlijke) gegevens kunnen gebruiken om hun leven, werk of bedrijf te organiseren, terwijl belangrijke waarden als veiligheid en privacy geborgd zijn. Persoonlijk datamanagement gaat over toegang, corrigeren en delen van persoonlijke data, maar ook inzicht hebben in wie deze persoonlijke gegevens gebruikt, onder controle van het individu.
Persoonlijke Digitale Omgeving	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Een persoonlijke digitale omgeving is in deze context iedere digitale toepassing met toegangsfunctie waar een burger of dienstverlener gegevens in kan plaatsen en beheren.
Persoonlijke financiële planning	Persoonlijke financiële planning is het proces waarbij individuen/huishoudens hun huidige persoonlijke en financiële informatie in overweging nemen, toekomstige financiële doelen bepalen en een financieel plan ontwikkelen om deze doelen te bereiken (Dawes, 1998) ³⁹⁵ .
Persoonlijke Gezondheidsomgeving	Een persoonlijke gezondheidsomgeving (PGO) is een website of app waarmee een persoon toegang heeft tot eigen gezondheidsgegevens. Het gaat dan om informatie die ergens anders opgeslagen is, bijvoorbeeld bij de huisarts of bij een specialist in het ziekenhuis. Tot nu toe waren deze gegevens niet altijd makkelijk in te zien. In een persoonlijke gezondheidsomgeving kan een persoon ze eenvoudig verzamelen, beheren en delen. Daarnaast kan een persoon zelf meetgegevens toevoegen aan de PGO.
Persoons identificerende gegevens	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Gegevens die het mogelijk maken de <i>identiteit</i> van een persoon te achterhalen, te weten geslachtsnaam, voornamen, geboortedatum en woonplaats.
Persoonsgegevens	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Een <u>persoonsgegeven</u> is alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 4 AVG). Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens.
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.

³⁹⁵ Dawes, J. (1998). Nieuwe klanten werven in financiële dienstverlening: gebruik van relatiemarketing en informatietechnologie bij financiële dienstverlening aan consumenten. *European Management Journal*, 16 (2), 249–259.

Begrip	Uitleg
Persoonsidentificatiegegevens	Bron BZK, Presentatie 16 juli 2020, Klantportaal A&P Een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld.
Privacy By Design	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. Pseudonimisering is een vorm van encryptie. Het is bijvoorbeeld mogelijk om namen weg te halen door deze te vervangen door numerieke codes. De sleutel waarmee de nummers weer omgezet kunnen worden in namen wordt veilig in een ander systeem bewaard, dat zeer beperkt toegankelijk is. Dit impliceert 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.
Privacy Enhancing Technologies (PET)	PET is de verzamelnaam voor verschillende technieken in informatiesystemen om de bescherming van persoonsgegevens te ondersteunen. PET omvat alle technische maatregelen om de privacy te waarborgen. PET kunnen bijvoorbeeld worden gebruikt om de identiteitsgegevens los te koppelen van de overige gegevens die zijn vastgelegd over een persoon. Alleen met bepaalde hulpmiddelen kan dan de koppeling worden gemaakt tussen de identificerende gegevens en de overige persoonsgegevens.
Protocol	Protocollen beschrijven hoe bepaalde processen verlopen en zijn vaak implementaties van concepten. Protocollen zijn nog niet als standaard opgenomen.
Pseudonimisering	Bron: https://wso2.com/library/article/2018/2/identity-and-access-management-to-the-rescue/ Pseudonimisering is het proces waarbij persoonlijk identificeerbare informatie uit datasets wordt verwijderd of vervangen door middel van kunstmatige identificatoren. Na pseudonimisering is een bepaald individu niet langer identificeerbaar zonder het gebruik van aanvullende informatie.
Qiy Trust Principles (belangrijkste)	Mijn gegevens Mijn gegevens mogen alleen met mijn toestemming worden gebruikt. Of die zich nu bevinden bij een organisatie of dat ik ze zelf heb gegeven. Delen van mijn gegevens Organisaties mogen mijn gegevens alleen delen met een andere partij wanneer ik daarvoor toestemming heb gegeven. Deze toestemming kan niet 'voor altijd' zijn. De

Begrip	Uitleg
	enige uitzondering is dat organisaties dit verplicht zijn vanwege bestaande wet- of regelgeving. Dergelijke uitzonderingen moeten te allen tijde traceerbaar zijn. Keuze termijn ter beschikking stellen. Ik kan besluiten (een deel van) mijn gegevens éénmalig of voor een bepaalde periode ter beschikking te stellen. Ik kan dit besluit altijd wijzigen, tenzij er een contractuele reden is waarom dit niet kan. Informatieplicht Als een organisatie mijn gegevens wil gebruiken moeten ze me eerst informeren waarom ze dat willen en hoe vaak. Anonimiteit Ik kan mijn gegevens altijd anoniem delen, behalve als dat wettelijk verboden is. In dat laatste geval kan ik kiezen of ik identificerende gegevens wil verstrekken of dat ik de transactie af wil breken. Data minimalisatie Een organisatie mag mij alleen die gegevens vragen die echt nodig zijn voor het beoogde doel, of die gegevens gevalideerd zijn of niet. Waarborgen Wanneer een organisatie een waarborg vraagt over mij, moet de gevraagde waarborg echt nodig zijn voor het beoogde doel. Toegang Organisaties die deelnemen aan het Qiy Afsprakenstelsel zijn verplicht mij 'toegang' te geven tot mijn gegevens. Dit geldt niet voor anonieme gegevens, maar verder wel voor alle gegevens die over mij gaan, ook als die ontstaan zijn op basis van gegevens die ik ter beschikking heb gesteld. Bescherming gegevens Iedere partij die deelneemt aan het Qiy Afsprakenstelsel en mijn gegevens gebruikt of erover beschikt, beveiligd deze gegevens volgens de eisen die daar door de Qiy Foundation aan gesteld zijn. Privacy statements Voor iedere organisatie die via het Qiy Afsprakenstelsel met mijn gegevens te maken heeft, hebben deze Qiy Principes voorrang boven hun eigen privacy statements.
Recht om vergeten te worden	Het '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.
Regie Op Gegevens (overheid)	De mate waarin de betrokkene (burger, consument, ondernemer, etc.) zeggenschap over en de regie (controle) kan hebben over de binnen en buiten de overheid, aanwezige persoonlijke gegevens over hem.
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.

Begrip	Uitleg
	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.
Regietoepassing	Bron: Programma Regie Op Gegevens van de Nederlandse overheid Dit is een applicatie die een betrokkene in staat stelt regie te voeren over zijn geverifieerde gegevens. Een regietoepassing kan worden geleverd door een publieke of private dienstverlener en is niet noodzakelijk onderdeel van een afsprakenstelsel.
SAML	Bron: http://saml.xml.org/protocols SAML is een standaard waarbij gebruikers federatief kunnen inloggen. Dit betekent dat iemand kan inloggen met een account van partij A (ook wel, de authenticatie provider) bij partij B (de resource provider). Er wordt dus een vertrouwde partij gebruikt voor authenticatie. Een bekende variant hiervan is het gebruik maken van een Google inlog voor een dienst. SAML wordt onder andere gebruikt in bijvoorbeeld SURFconext, iDIN, DigiD, eHerkenning en voorheen Idensys.
Scraping	Bij scraping worden gegevens van webpagina's onttrokken en geïmporteerd in de tools en apps van de burger/consument. Scraping is een ongestructureerde manier van gegevensdeling. Dit wordt vooral toegepast als geen API's of downloadinterfaces beschikbaar zijn.
Self-sovrin identity	Basic building blocks of SSI. https://livebook.manning.com/book/self-sovereign-identity/chapter-2/v-1/89 Self-sovrin identity is een digitale identiteit waarbij de gebruiker en diens privacy centraal staat. De gebruiker kan met SSI zelf zijn identiteit bewaren. In tegenstelling tot de klassieke identiteiten waarbij een gebruiker, of bij elke organisatie opnieuw moet inloggen met een andere identiteit, of bij elke organisatie inlogt via een andere organisatie (denk aan knoppen met tekst 'Login met DigiD' of 'Login met Google') en deze haar identiteit vervolgens doorgeeft aan die organisatie. In SSI krijgt de gebruiker eenmalig, van bijvoorbeeld DigiD, een digitaal identiteit met daarin al haar gegevens en kan deze vervolgens met andere organisaties delen. Met de self-sovereign identiteit die de gebruiker zelf bezit, kan de gebruiker buiten DigiD om, zelf inloggen bij andere partijen, zonder dat DigiD daarvan op de hoogte is. Bij het inloggen middels een 'login met DigiD of Google', weten deze partijen op welke sites een gebruiker zijn identiteit gebruikt. Met SSI heeft de gebruiker dus meer privacy. Er zijn verschillende voorbeelden die als SSI benoemd kunnen worden, zoals Sovrin, welke een blockchain gebruikt en IRMA, welke het Idemix protocol gebruikt.

Begrip	Uitleg
Single Sign On (SSO)	Een functie die wordt gefaciliteerd waardoor een authenticatie van een gebruiker wordt hergebruikt, waardoor deze gebruiker niet opnieuw hoeft in te loggen.
Standaard	Een standaard kan verschillende dingen beschrijven, bijvoorbeeld het maken van een product, doorlopen van een proces of leveren van een dienst. Dit kan binnen een enkele organisatie, maar met name gaat het om standaardisatie afspraken tussen een grotere groep organisaties. Standaarden worden vastgelegd en onderhouden door standaardisatieorganisaties (zoals bijvoorbeeld ISO of SIVI).
Toestemming/consent	Twee van de eisen die de AVG stelt aan 'toestemming' zijn dat deze 'geïnformeerd' en 'specifiek' gegeven is. Om geldige toestemming aan te tonen is het dan ook essentieel dat een organisatie kan laten zien op basis van welke informatie de betrokken personen de toestemming heeft gegeven. Het is dus onvoldoende om alleen de toestemming zelf vast te leggen.
Token	https://nl.wikipedia.org/wiki/Token_(identificatie) Een token is over het algemeen een reeks cijfers of karakters die geheim is en soms ook uniek. Iemand die in het bezit is van een correct token heeft dit hoogstwaarschijnlijk niet geraden en bewijst daarmee het token te hebben.
UMA	(User management access) is een standaard waarmee gebruikers toegang tot bepaalde gegevens kunnen geven aan andere gebruikers. UMA bouwt verder op de OAuth standaard.
Verifiable credentials	Een credential is een uitspraak over een persoon door een entiteit, die gecontroleerd kan worden. Denk bijvoorbeeld aan een paspoort, deze bewijst vanuit de overheid je identiteit. Dit kan gecontroleerd worden aan de echtheidskenmerken van een paspoort of door het uitlezen van de cryptografisch beveiligde chip in het document. Ook een diploma is een voorbeeld van een credential, deze bevat vaak de schriftelijke handtekening van de onderwijsinstelling. In de digitale wereld hebben we vergelijkbare credentials met hun echtheidskenmerken en deze worden verifiable credentials genoemd. Deze echtheidskenmerken kunnen variëren, van een copy van een document met handtekening tot cryptografische ondertekende documenten. Een digitale handtekening met behulp van asymmetrische encryptie, is een mooi voorbeeld. De entiteit gebruikt zijn cryptografische privé sleutel om een credential uit te geven, andere partijen kunnen de publieke sleutel gebruiken om te controleren dat de credential echt is uitgegeven door de entiteit. Het is in PDM belangrijk dat de data die van de gebruiker naar andere partijen gestuurd wordt ook gecontroleerd kan worden op echtheid, verifiable credentials zouden daarvoor gebruikt kunnen worden. Een voorbeeld van een open standaard van verifiable credential is gemaakt door W3C ³⁹⁶ , deze wordt veel gebruikt in SSI-oplossingen. Ook Idemix, wat gebruikt wordt in IRMA, is een vorm van verifiable credentials.
Vertegenwoordiger	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021 Burgers kunnen zich (vrijwillig of gedwongen, middellijk of onmiddellijk) laten vertegenwoordigen door iedere andere burger (particulier of professioneel).
Waarmerk	Bron: ICTU Referentiearchitectuur ROG, Onderdeel: Delen van gegevens, Versie 0.4 januari 2021

³⁹⁶ Verifiable credentials. <https://www.w3.org/TR/vc-data-model/>

Begrip	Uitleg
	Een waarmed is een extra kenmerk van (een set van) gegeven(s) waaruit blijkt dat de uitgever van het waarmed (meestal na onderzoek) de juistheid van het gegeven onderschrijft ("voor waar aanmerkt").
X-Tee	Bron: https://e-estonia.com/solutions/interoperability-services/x-road/ X-tee is een protocol waarmee een partij bij verschillende bronnen data kan ophalen. X-tee is ontwikkeld in het e-Estonia project. Voorheen stond X-Tee bekend als X-road.
Zero Knowledge Proof	Bron: https://en.wikipedia.org/wiki/Zero-knowledge_proof Een zero knowledge proof is een wiskundige manier om te bewijzen dat je kennis hebt van een zeker gegeven, zonder dat gegeven daadwerkelijk te laten zien. Dit gegeven kan dus ook een persoonlijk gegeven zijn. Dit draagt bij aan dataminimalisatie en voegt waarde toe vanuit privacy perspectief. Zero knowledge proofs worden gebruikt in Idemix, het protocol dat bijvoorbeeld gebruikt wordt in IRMA.

5. BIJLAGE E – USE CASES

5.1 Inleiding

Context voor de use cases is een digitaal financieel ecosysteem dat de consument in staat stelt inzicht te krijgen in zijn/haar financiële situatie en zich desgewenst te laten adviseren. Om dit ecosysteem te optimaliseren worden databronnen in het publieke/private domein ontsloten. Bij voorkeur worden gegevens gestructureerd uitgewisseld. Een ontvangende adviseur kan de data dan verwerken, mits hij/zij beschikt over een applicatie die de data kan verwerken.

Use cases kunnen bijvoorbeeld worden gebaseerd op:

- **Het laten uitvoeren van een Financiële APK;**
- **Het laten opstellen van een Persoonlijk Financieel Plan;**
- **Het advies dat een consument inwint bij overweging aanschaf van:**
 - Uitvaartverzekering;
 - Levensverzekering;
 - Bankspaarproduct;
 - Deelnemingen in een beleggingsfonds;
 - **Hypotheek;**
 - Betalingsbescherming die er voor zorgen dat bijvoorbeeld de hypotheek doorbetaald wordt bij inkomensterugval;
 - Overlijdensrisicoverzekering;
 - Individuele arbeidsongeschiktheidsverzekering.
- Het advies dat een consument inwint bij het bepalen van gevolgen van:
 - **Het aanschaffen van een huis;**
 - Trouwen;
 - In verwachting zijn;
 - Overlijden;
 - Pensioen.

De **vetgedrukte** cases zijn hierna kort uitgewerkt.

5.2 Financiële Apk

Een Financiële APK is idealiter een digitaal overzicht van het kenmerkende deel van de financiële situatie van een consument. Het extract wordt idealiter verkregen door met behulp van een tool realtime/online brongegevens te ontsluiten. Het informeert de consument over de feiten in functie van de kwaliteit van de beschikbare broninformatie. De Financiële APK ontwikkelt zich in de loop van de tijd, afhankelijk van het aantal bronnen dat realtime digitaal ontsloten wordt/kan worden. Een Financiële APK wordt laagdrempelig ter beschikking gesteld, en bestaat uit een Quick scan van de financiële situatie van een consument.

Kenmerken

- Analogie met auto's (APK) of zorg (tandarts).
- Gestandaardiseerde controle, al dan niet verplicht.

Voordeel voor consument

- Minder kosten kwijt voor inventarisatie van financiële data.
- Meer inzicht = meer grip op geld = meer geluk.
- Inzicht kan preventief werken, zodat consument niet in financiële problemen komt, doordat er eerder actie wordt ondernomen.
- Advies kan goedkoper worden: besparing honderden euro's voor consument die wel advies afneemt en extra investering voor consumenten die nu geen advies afnemen (vanwege de prijs).

Voordeel voor adviseur

- Minder (circa 1-2 uur) tijd kwijt aan inventarisatie = minder uren kunnen schrijven, maar ook meer tijd voor advies en acquisitie.
- Minder fouten in data, door directe toegang tot de bron.

Huidige en toekomstige situatie

Nu niet eenvoudig te ontsluiten, laat staan voor consument in een vorm waarbij regie mogelijk is.

Welke gegevens?

- Gegevens uit Voor Inge vulde Aangifte Belastingdienst (VIA)
- Gegevens uit Pensioenregister: AOW en tweede pijler pensioen.

Bron van gegevens

- Belastingdienst
- Pensioenregister

Afnemer

- Consument of persoon die de consument heeft gemachtigd
- Via consument kunnen gegevens aan adviseur ter beschikking worden gesteld.

Gestructureerd/ongestructureerd

Gestructureerd, digitaal waarmerk gewenst

5.3 Het opstellen van een persoonlijk financieel plan

Een Persoonlijk Financieel Plan geeft antwoord op vragen als:

- Is er voldoende spaargeld om mijn kinderen later te laten studeren?
- Bouw ik voldoende pensioen op?
- Als mij iets overkomt, laat ik mijn gezin dan financieel 'gezond' achter?
- Als ik eerder wil stoppen met werken, zijn mijn huidige voorzieningen wel toereikend?
- Als ik mijn baan kwijtraak, hoe lang heb ik dan recht op een uitkering en is kan ik hier mijn lasten van betalen?

Een Persoonlijk Financieel Plan is weten waar je aan toe bent, nu en in de toekomst. Het maakt voor een consument inzichtelijk welke gevolgen hypotheek, pensioen, arbeidsongeschiktheid en overlijden hebben op zijn/haar consumptief besteedbaar inkomen eventueel in combinatie met een partner. Het plan helpt de risico's te beheersen.

Huidige en toekomstige situatie

Nu een zeer arbeidsintensief proces. In de toekomst een digitaal (near) realtime proces.

Welke gegevens?

- Eerste- En Tweede Pijler Pensioenen
- Derde pijler producten
- Inkomen
- Eigen geld
- Hypotheken
- Schulden (leningen)

Gegevens	Bron
Eerste- En Tweede Pijler Pensioenen	Pensioenregister
Derde pijler producten	Banken/Verzekeraars
Inkomen • Aangifte inkomstenbelasting, gehele aangifte - Belastingdienst • Bankafschrift - banken ○ met bijschrijving netto salaris ○ Overige inkomsten	Belastingdienst Banken
Eigen geld • Afschrift spaarrekening(en) aanvrager(s) • Rekeningoverzicht beleggingsrekening(en)	Banken Diverse brokers
Hypotheken	Kadaster

Gegevens	Bron
Schulden (leningen)	BKR, DUO

Afnemers

Consument of persoon die de consument heeft gemachtigd. Via consument kunnen gegevens aan adviseur ter beschikking worden gesteld.

Gestructureerd/ongestructureerd

Bij voorkeur alleen gestructureerd: voor het maken van berekeningen. Digitaal waarmerk gewenst.

5.4 Hypotheekadvies

Als een consument een lening wil voor een nieuwe woning en hij/zij heeft een hypotheekvraag dan richt hij/zij zich tot een hypotheekadviseur. Deze onderzoekt de persoonlijke situatie (klantbeeld) en geeft hier een passend advies bij.

Huidige en toekomstige situatie

Nu is doorlooptijd 4 tot 8 weken. Door koppeling met databronnen en regie van de consument moet versnelling tot een paar dagen mogelijk zijn.

Welke gegevens?

Identiteit:

- Geldig paspoort of Europese identiteitskaart, kopie op ware grootte
- Huwelijksvoorwaarden
- Echtscheidingsconvenant met beschikking rechtbank
- Inschrijving in burgerlijke stand

Inkomen:

- Meest recente loonstrook
- Werkgeversverklaring (evt. intentieverklaring), Max. 3 maanden oud bij ontvangst bindende offerte
- Aangifte inkomstenbelasting, gehele aangifte
- Uniform Pensioen Overzicht (UPO) huidige werkgever,
- Pensioenopgave van mijnpensioenoverzicht.nl
 - pensioen per uitvoerder
 - overzicht bij overlijden voor nabestaanden
- Bankafschrift
 - met bijschrijving netto salaris
 - NAW-gegevens zichtbaar
 - recent afschrift
 - rekeningnummer zichtbaar
- Overige inkomsten
 - bijv. huur, pacht, freelancewerk
- Jaaropgave werkgever(s)/uitkeringsinstanties 2017
 - alleen voor flexwerkers

Eigen geld en leningen:

- Afschrift spaarrekening(en) aanvrager(s)
 - naam, datum en rekeningnummer zichtbaar
 - bij- en afschrijvingen laatste 3 maanden om saldohistorie aan te tonen
- Rekeningoverzicht beleggingsrekening(en)
 - naam, datum en rekeningnummer zichtbaar
- Opgave(n) van lening(en)
 - denk ook aan limiet op betaalrekeningen, klantenpassen, creditcards
 - en onderhandse leningen
- DUO (oorspronkelijke studieschuld)

Toekomstige woning:

- (Voorlopige) koopovereenkomst of koop-/aanneemovereenkomst

- liefst getekend door beide partijen
- Taxatierapport (bij bestaande bouw)
 - maximaal 6 maanden oud bij ontvangst bindende offerte
 - gevalideerd door gecertificeerd instituut
 - waarde voor en na verbouwing (indien van toepassing)
- Verbouwingsspecificatie
 - gelijk aan de omschrijving en het bedrag in het taxatierapport
- Of meerwerkspecificatie (Nieuwbouw)
 - Handgeschreven, op basis van schattingen

Gegeven/categorie	Bron
Voor adviseur (specifieke data voor advies)	
• Past aanvraag met nationale hypotheek garantie	Waarborgfonds Eigen Woningen (NHG)
• In geval van onderneming, uittreksel als bewijs van inschrijving, controle onderpand, werkgever bestaat? Is aannemer in geval bouwdepot een bestaand bedrijf?	Kamer van Koophandel
• Waarde ingeschreven hypotheek	Kadaster
• Met het rapport 'Wat is dat huis waard' van Calcasa kan de koop- of verkoopprijs van een woning worden vastgesteld	Calcasa
• Taxatierapport – is onderpand voldoende waard en zijn er bijzonderheden die waarde beïnvloeden?	Nederlands Woning Waarde Instituut (NWWI)
Identiteit	
• Huwelijks voorwaarden	Rechtbank
• Echtscheidingsconvenant met beschikking rechtbank	Rechtbank
• Inschrijving in burgerlijke stand	GBA
Inkomen	
• Meest recente loonstrook	Werkgever
• Werkgeversverklaring (evt. intentieverklaring), Max. 3 maanden oud bij ontvangst bindende offerte	Werkgever of UWV (arbeidsverleden met SV-loon in verzekeringsbericht)
• Aangifte inkomstenbelasting, gehele aangifte	Belastingdienst
• Uniform Pensioen Overzicht (UPO) huidige werkgever	Pensioenuitvoerder
• Pensioenopgave van mijnpensioenoverzicht.nl ○ pensioen per uitvoerder ○ overzicht bij overlijden voor nabestaanden	Pensioenregister
• Bankafschrift - banken ○ met bijschrijving netto salaris ○ NAW-gegevens zichtbaar ○ recent afschrift ○ rekeningnummer zichtbaar	Banken
• Overige inkomsten ○ bijvoorbeeld huur, pacht, freelancewerk	Contracten
• Jaaropgave werkgever(s)/uitkeringsinstanties 2017 - UWV ○ alleen voor flexwerkers	UWV
Eigen geld	
• Afschrift spaarrekening(en) aanvrager(s) ○ naam, datum en rekeningnummer zichtbaar ○ bij- en afschrijvingen laatste 3 maanden om saldohistorie aan te tonen	Banken
• Rekeningoverzicht beleggingsrekening(en) – diverse brokers ○ naam, datum en rekeningnummer zichtbaar	Diverse brokers
Leningen	

Gegeven/categorie	Bron
• Opgave(n) van lening(en) ◦ denk ook aan limiet op betaalrekeningen, klantenpassen, creditcards ◦ en onderhandse leningen • DUO (oorspronkelijke studieschuld)	BKR
Toekomstige woning	
• (Voorlopige) koopovereenkomst of koop-/aanneemovereenkomst – ◦ liefst getekend door beide partijen	Makelaar/notaris
• Taxatierapport (bij bestaande bouw) - NWWI ◦ maximaal 6 maanden oud bij ontvangst bindende offerte ◦ gevalideerd door gecertificeerd instituut ◦ waarde voor en na verbouwing (indien van toepassing)	NWWI
• Verbouwingsspecificatie - aannemer ◦ gelijk aan de omschrijving en het bedrag in het taxatierapport	Aannemer
• Of meerwerkspecificatie (Nieuwbouw) - aannemer ◦ Handgeschreven, op basis van schattingen	Aannemer

Afnemers

- Hypotheekadviseur
- Bank
- Consument
- Gemachtigde

Gestructureerd/ongestructureerd

Deels gestructureerd, deels ongestructureerd, gewaarmerkt.

6. BIJLAGE F – OPZET VRAGENLIJSTEN

6.1 Vragenlijst PDM-Diensten

Deze vragenlijst gaat over de kenmerken en functies van de Personal Data Management service (PDM-Dienst) die uw organisatie aanbiedt. De vragen hebben betrekking op governance, consent, opslag van gegevens, gegevensuitwisseling, datadiensten, authenticatie en het business model van de PDM-Dienst.

Onder PDM-Dienst verstaan wij: Een dienst die een individu in staat stelt om zijn/haar persoonlijke informatie duurzaam te beheren en te onderhouden om deze, wanneer de gebruiker dit in zijn belang acht, te kunnen delen met anderen.

Het invullen van de vragenlijst duurt ongeveer 30 minuten. Wanneer bepaalde vragen niet van toepassing zijn kunt u 'n.v.t.' invullen en eventueel een toelichting geven.

Algemeen

Naam PDM-Dienst

Contactpersoon

Algemene kenmerken

Doelstelling. Wat is de algemene positionering/doelstelling van de service?

Origine. Standplaats van het initiatief (land) en wanneer is het ontstaan?

Volwassenheid. In welke fase van ontwikkeling is de PDM-Dienst?

☐

Conceptfase

☐

Pilotfase (in ontwikkeling/wordt nog getest in gebruikerstest)

☐

Operationeel (bruikbaar voor personen in tenminste één live proces)

Dienst. Welke dienst levert de PDM-Dienst aan een gebruiker?

Marktfocus. Op welke sector en geografische regio richt de PDM-Dienst zich voornamelijk?

Bronnen: Wat zijn typische data-aanbieders waarvan de oplossing gebruik maakt?

Afnemers: Wat zijn typische data-afnemers voor de dienst?

Governance (besturing en beheer)

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

Zo niet:

Toetreding: welke regels zijn er voor toetreding van partijen (data-afnemers, gebruikers, data-bronnen) en het verwijderen ervan?

Incidenten: Op welke wijze kunnen gebruikers incidenten melden en worden ze geïnformeerd over incidenten?

Ontwikkeling: Wie is verantwoordelijk voor doorontwikkeling en beheer van de diensten?

Communicatie. Op welke wijze worden gebruikers geïnformeerd over de afspraken in de dienstverlening en de ontwikkeling daarvan?

Consent (toestemming)

Ophalen. Kan een persoon consent geven voor het ophalen van gegevens bij een data aanbieder?

Uitwisselen. Kan een persoon consent geven voor het uitwisselen van gegevens met een data afnemer?

Tijdsduur bepalen. Kan een persoon bepalen voor welke tijdsduur de consent geldig is?

Specifieke gegevens. Heeft de persoon keuze om een gedeelte van de set gegevens te delen met de afnemer?

Consent overzicht. Kan de PDM-Dienst een overzicht geven van de toestemmingen die zijn gegeven?

Consent aanpassen. Kan uitgegeven consent gewijzigd worden?

Consent intrekken. Kan gegeven consent ingetrokken worden?

Opslag van gegevens

Opslag. Worden persoonlijke gegevens opgeslagen?

Plaats van verwerking/opslag. Waar worden gegevens verwerkt/opgeslagen?

- ☐ Device van de gebruiker
- ☐ Op server van de PDM-Dienst
- ☐ Op zelf te kiezen cloudoplossing
- ☐ Overig – graag specificeren:

Duur van opslag. Hoe lang worden gegevens bewaard?

Is de opslag ten behoeve van gegevensuitwisseling of acteert de PDM-Dienst ook als 'kluis'?

Gegevensuitwisseling

Ophalen. Hoe worden gegevens opgehaald bij databronnen? (API, screen scraping, uploaden, anders?)

Manier van uitwisseling. Hoe worden gegevens uitgewisseld met data afnemers? (API, anders?)

Gegevens aanvullen. Kan een persoon zelf data toevoegen, of wordt alleen gewerkt met data uit bronsystemen?

Data diensten

Waarmerking. Zijn de gegevens gewaarmerkt door de bron, PDM-Dienst of niet?

Analyse. Worden er door de PDM-Dienst analyses gedaan over de gegevens? (vb. geboortedatum omzetten naar leeftijd)

Aggregatie. Worden gegevens geaggregeerd (of gecombineerd uit meerdere data aanbieders)?

Revocatie. Kunnen gegevens door de data-aanbieder ongeldig verklaard worden? (bijv. als een BIG registratie wordt ingetrokken, maar nog wel in de PDM-Dienst staat?)

Authenticatie

Inloggen bij de PDM-Dienst. Hoe bepaalt de PDM-Dienst de identiteit van de gebruiker?

Gegevens ophalen. Wordt er bij het ophalen van gegevens gebruik gemaakt van bestaande identificatiediensten zoals DigiD, EHerkenning, iDIN?

Autorisatie. Hoe worden autorisaties beheerd?

Privacy. Welke maatregelen, naast consent, zijn getroffen om de privacy van de gebruiker te borgen? (Privacy-by-design aspecten)

Business model

Inkomsten. Welke partijen/partners betalen in het ecosysteem (Data-aanbieders, data-afnemers, persoon, beheerorganisatie, anders)?

Vorm. Is dit in vorm van een abonnement, pay-per-use of vaste bijdrage?

Zijn er andere inkomstenbronnen? Zoals verkoop van anonieme data, advertenties, upselling/cross-selling

Overig

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

6.2 Vragenlijst PDM Afsprakenstelsels

Deze vragenlijst gaat over de kenmerken en functies van afsprakenstelsels met betrekking op regie op persoonlijke gegevens. De vragen hebben zijn met name gericht op governance, consent, opslag van gegevens, gegevensuitwisseling, datadiensten, authenticatie en het businessmodel van het afsprakenstelsel en hoe het zich daarover uitspreekt.

Het invullen van de vragenlijst duurt ongeveer 30 minuten. Wanneer bepaalde vragen niet van toepassing zijn kunt u 'n.v.t.' invullen en eventueel een toelichting geven.

Voor meer informatie over de achtergronden van dit onderzoek kunt u contact opnemen met Marlies Rikken (06-10418028).

Algemeen

Naam PDM afsprakenstelsel

Contactpersoon

Algemene kenmerken

Doelstelling. Wat is de algemene positionering/doelstelling van het afsprakenstelsel?

Origine. Standplaats van het stelsel (land) en wanneer is het ontstaan?

Beheerder. Welke organisatie of consortium beheert het afsprakenstelsel?

Volwassenheid. In welke fase van ontwikkeling is het stelsel?

☐

Conceptfase

☐

Pilotfase (in ontwikkeling/wordt nog getest in gebruikerstest)

☐

Operationeel (in gebruik door verschillende dienstenaanbieders)

Dienstaanbieders. Welke diensaanbieders werken op dit moment met het stelsel?

Marktfocus. Op welke sector en geografische regio richt het stelsel zich voornamelijk?

Bronnen: wat zijn typische data-aanbieders waarvan gebruik gemaakt wordt in het stelsel?

Afnemers: wat zijn typische data-afnemers?

Governance (besturing en beheer)

Toetreding: welke regels zijn er voor toetreding van partijen (data-afnemers, gebruikers, data-

aanbieders) en het verwijderen ervan?

Incidenten: op welke wijze kunnen gebruikers incidenten melden en worden ze geïnformeerd over incidenten?

Ontwikkeling: wie is verantwoordelijk voor doorontwikkeling en beheer van de diensten?

Communicatie. Op welke wijze worden gebruikers geïnformeerd over de afspraken in de dienstverlening en de ontwikkeling daarvan?

Functionaliteit

Consent

Welke functionele aspecten van consent worden voorgeschreven door het afsprakenstelsel?

- ☐ Consent voor ophalen gegevens
- ☐ Consent voor uitwisselen gegevens
- ☐ Bieden van een consent overzicht
- ☐ Mogelijkheid tot aanpassen van consent
- ☐ Anders, namelijk:

Opslag van gegevens

Welke functionele aspecten van gegevensopslag worden voorgeschreven door het afsprakenstelsel?

- ☐ Duur van de opslag
- ☐ Locatie van de opslag
- ☐ Anders, namelijk:

Gegevensuitwisseling

Welk model voor gegevensuitwisseling moet gebruikt worden binnen het afsprakenstelsel?

- ☐ Directe uitwisseling tussen twee partijen
- ☐ Uitwisseling via een derde neutrale partij (operator, orchestrator, PDM-Dienst)
- ☐ Anders, namelijk:

Data diensten

Zijn er vereisten die het afsprakenstelsel stelt aan datadiensten die geleverd worden?

- ☐ De diensten moeten een waarmerk bezitten
- ☐ Er zijn eisen aan de analyses die diensten mogen doen
- ☐ Er zijn eisen aan (de manier van) data aggregatie
- ☐ Anders, namelijk:

Authenticatie en autorisatie

Zijn er vereisten aan authenticatie? (Bijvoorbeeld wanneer een gebruiker zich moet authenticeren bij een bron, of wanneer er door data afnemers een verzoek aan de gebruiker wordt gedaan)

Gebruikersinteractie

Zijn er vereisten aan de manier waarop gebruikers interactie hebben met diensten in het stelsel? (Bijvoorbeeld betreffende de navigatie en vormgeving van diensten)

Business model

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

Overig

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