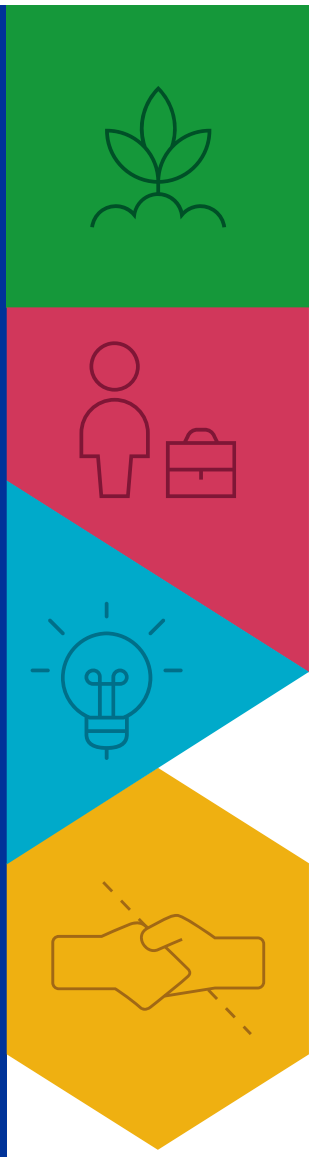
Interreg
Vlaanderen-Nederland

Gefinancierd door
de Europese Unie

welldata
DATARUIMTE VOOR PREVENTIE

Dataruimte voor preventie

D3.3.3 – Grensoverschrijdend governance model



Hoog
mikken voor
de lage landen!

grensregio.eu

Projectacroniem	WellData
Projecttitel	Dataruimte voor preventie
Startdatum	Mei 2024
Looptijd	3 jaar
Deliverable	D3.3.3 Grensoverschrijdend governance model
Werkpakket	WP3
Partner lead	VITO
Auteurs	Elfi Goesaert, Jildau Bouwman, Erik Laes, Andre Boorsma, Cato van Schyndel
Opleverdatum	31 mei 2026
Deliverable type	Rapport (R)
Versie	Versienummer: 2.0 Volgende versies: • 2.0 – verdere analyse dataruimtes vs persoonlijke dataruimtes en concept mapping, aanvullingen TNO rond gedelegeerd consent en consentprofielen • Finaal rapport met aanbevelingen en feedback uit taak 4.3 als bijlage • White paper(s) over regelgeving, opportuniteiten, burger governance modellen • Opiniestuk preventie & EHDS

Management Samenvatting

Het doel van het WellData-project is om individuen meer grip te geven op hun gezondheidsdata rondom leefstijl en preventie, door een veilige en transparante persoonlijke dataruimte te creëren die onderzoek en innovatie op het gebied van ziektepreventie en publieke gezondheid ondersteunt. Daarbij hoort ook een bijpassend governance binnen de bestaande juridische kaders. Dit rapport beschrijft de ontwikkeling van een grensoverschrijdend governance-model voor een persoonlijke gezondheidsdataruimte gericht op preventie en welzijn, waarbij de regie van burgers over leefstijl- en welzijnsdata centraal staat. Hiervoor zijn een aantal governance projecten geanalyseerd zoals de Europese datastrategie, technische raamwerken zoals het IDSA-model en relevante regelgeving (AVG, Data Act, Data Governance Act, EHDS). Uit de analyse komen een aantal hiaten naar voren en worden aanbevelingen gegeven voor ethisch, transparant en participatief datadelen.

Europese datastrategie en aandachtspunten

De International Data Spaces Association (IDSA) en het Data Spaces Support Centre (DSSC) vormen de kern van de technische en organisatorische modellen voor Europese dataruimtes. IDSA ontwikkelde het IDS Reference Architecture Model en het bijhorende rulebook als basis voor veilige, soevereine en interoperabele datadeling tussen organisaties, zonder centralisatie van data. Het DSSC ondersteunt dit met praktische bouwblokken en een toolbox, die organisaties helpen bij het opzetten van dataruimtes via een gestructureerde blauwdruk. Hierbij worden zowel business-organisatorische als technische componenten en governance-aspecten uitgewerkt, zodat deelnemers duidelijke rollen, regels en structuren kunnen vastleggen. Hoewel het basisconcept van een dataruimte overeind staat, zijn er nog veel keuzes en uitdagingen rond governance, duurzaamheid, deelname en interoperabiliteit. Bovendien blijft de betrokkenheid van burgers als actieve deelnemers en het delen van persoonlijke data onderbelicht, ondanks het belang hiervan in de Europese regelgeving.

Het regelgevend landschap

Het regelgevend landschap rond gegevensbescherming in Europa wordt vooral bepaald door de Algemene Verordening Gegevensbescherming (AVG), de Data Act (DA), de Data Governance Act (DGA) en de European Health Data Space (EHDS). De AVG vormt het fundament voor de bescherming van persoonsgegevens, met duidelijke spelregels rond verwerking, opslag en rechten van betrokkenen. Bijzondere aandacht gaat naar gevoelige gegevens zoals gezondheidsinformatie, waarvoor strenge voorwaarden gelden. De DA en DGA zijn recentere regelgeving die inspelen op nieuwe uitdagingen zoals datadeling binnen de data-economie, dataportabiliteit en de rol van databemiddelingsdiensten, datacoöperaties en data-altruïsme. Zij bieden individuen meer mogelijkheden om toegang te krijgen tot hun data, deze over te dragen of te delen, en zorgen voor meer transparantie en bescherming bij het (her)gebruik van data, onder andere in de context van het Internet of Things en sectoren als gezondheidszorg.

De EHDS bouwt voort op deze algemene wetgeving en introduceert sectorspecifieke regels voor gezondheidsdata, met het doel zowel de primaire (gezondheidszorg) als secundaire (onderzoek, beleidsvorming) aanwending van elektronische gezondheidsgegevens te faciliteren. De regelgeving voorziet in uitgebreide rechten voor burgers, zoals dataportabiliteit, inzage en correctie, maar ook opt-out mogelijkheden voor het delen van data. Tegelijk worden mechanismen opgezet om de governance en veilige toegang tot gezondheidsdata te waarborgen via instanties als Health Data Access Bodies (HDAB's), Trusted Health Data Holders (THDH's) en Health Data Intermediation Entities (HDIE's). Hoewel de regelgeving steeds meer rechten en ondersteunende mechanismen aanbiedt, blijft het een uitdaging deze rechten voor burgers laagdrempelig en effectief uit te oefenen, zeker in een snel evoluerend datalandschap waar ook preventieve en door burgers gegenereerde gegevens (zoals via wellnessapps) steeds belangrijker worden.

Een grensoverschrijdend burgergedreven governancemodel

Tenslotte wordt het concept van een grensoverschrijdend, burgergedreven governancemodel voor het beheer van gezondheidsdata geïntroduceerd, waarbij databemiddelaars en collectieve beheerstructuren zoals datacoöperaties, data trusts en commons centraal staan. Door burgers meer zeggenschap te geven en hen actief te betrekken bij het beheer en de deling van hun gezondheidsgegevens, wordt gestreefd naar een evenwichtigere machtsverhouding tegenover grote instellingen en bedrijven. Diverse voorbeeldinitiatieven zoals MyData, MIDATA, Gezond Akkoord en We Are illustreren hoe collectief en democratisch beheer in de praktijk kan worden gebracht, met aandacht voor autonomie, transparantie, ethiek en maatschappelijke waarde. Deze modellen bieden burgers niet alleen individueel controle over hun data, maar ook de mogelijkheid om samen publieke waarden en normen rond datagebruik vast te leggen.

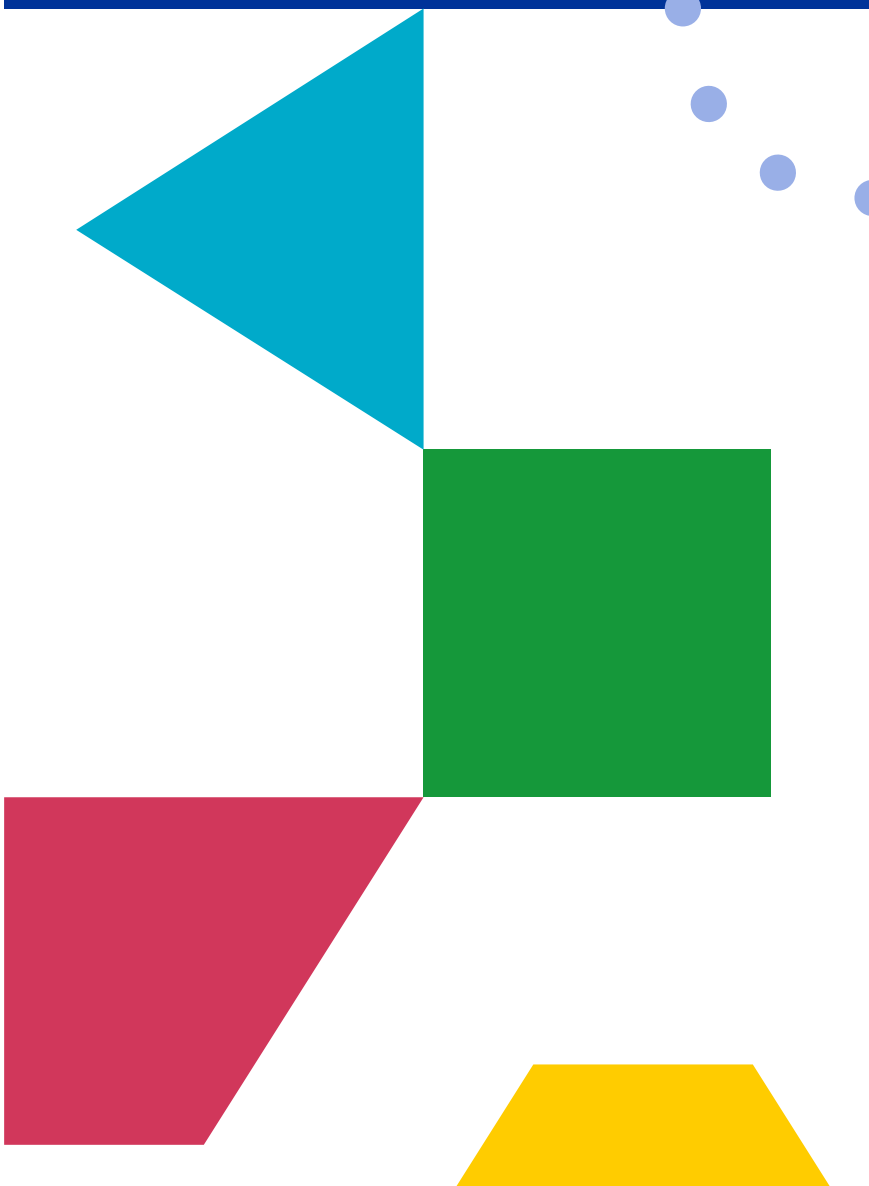
Tenslotte worden in het rapport enkele aanbevelingen geformuleerd voor een burgergedreven governancemodel rond gezondheidsdata, met als kernpunten transparantie, collectieve inspraak, versterking van burgerrechten en flexibele, toekomstgerichte kaders. Burgers krijgen momenteel te weinig zicht en controle over wie hun data gebruikt en voor welk doel, wat het vertrouwen ondermijnt. Aanbevolen wordt onder meer om toegankelijke platformen te ontwikkelen voor data-inzicht, collectieve governancevormen zoals coöperaties in te zetten, en persoonlijke datakluizen en consent-opties op maat te voorzien. WellData operationaliseert deze principes reeds via co-creatie, datakluizen, nieuwe consentmechanismen en actieve burgerbetrokkenheid, met als doel een robuust, ethisch en participatief dataruimtemodel te realiseren dat ook het preventie- en wellnessdomein omvat.

Inhoud

Afkortingen

AMA	Access Management Applicatie
AVG	Algemene Verordening Gegevensbescherming
BDVA	Big Data Value Association
DA	Data Act
DGA	Data Governance Act
DPO	Data Protection Officer
DSP	Data Spaces Protocol
DSSC	Data Spaces Support Centre
EDPB	European Data Protection Board
EHDS	European Health Data Space
EPD	Elektronisch patiëntendossier
HDAB	Health Data Access Body
HDIE	Health Data Intermediary Entity
IDSA	International Data Spaces Association
IDS-RAM	International Data Spaces Reference Architecture Model
IoT	Internet of Things
MDOG	Mijn data onze gezondheid
PGO	Persoonlijke gezondheidsomgeving
SPE	Secure Processing Environment
THDH	Trusted Health Data Holder

1. Inleiding



Als het gaat om het hergebruik van gezondheidsdata is de meerderheid van Europese en nationale projecten gericht op medische data. Ook in de uitvoering van de European Health Data Space (EHDS) wordt voornamelijk gekeken naar medische data, bijvoorbeeld data uit elektronische patiëntendossiers (EPD's). WellData heeft als eerste doel om individuen te ondersteunen bij het uitoefenen van zeggenschap over hun gezondheidsdata, meer bepaald de gezondheidsdata gelinkt aan levensstijl en welzijn, veeleer buiten medische context verzameld. Deze ondersteuning van zeggenschap gebeurt door middel van een veilige, transparante en ethische persoonlijke gezondheidsdataruimte gericht op preventie. Hiervoor genereert WellData een data-ecosysteem dat onderzoek en innovatie naar ziektepreventie en positieve gezondheid voor het algemeen welzijn bevordert. Daarnaast creëert WellData een vertrouwde, persoonlijke gezondheidsdataruimte die preventieve gezondheid mogelijk maakt, welzijn bevordert en kennis voor het maatschappelijk welzijn stimuleert door ethisch, verantwoordelijk en innovatief gebruik van gezondheidsdata. Gezondheidsdata worden binnen deze dataruimte gezien als alle data die van belang zijn om de gezondheid te monitoren en verbeteren en zijn dus veel breder dan alleen de medische data zoals vastgelegd bij de arts. Om dit mogelijk te maken is het van belang dat er een governancemodel is dat over de Vlaams-Nederlandse grens deze dataruimte ondersteunt binnen de geldende wettelijke kaders. Dit rapport beschrijft eerst de relevante kaders en hun relevantie voor preventie. Daarna wordt een overzicht gegeven van relevante modellen voor de governance van een gezondheidsdataruimte voor preventie, worden de hiaten beschreven en worden aanbevelingen gedaan voor het ontwikkelen van een governance model voor deze dataruimte.

2. Context en juridisch kader voor gebruik en delen van gezondheidsdata

2.1 Europese datastrategie en aandachtspunten

2.1.1 Algemeen

Wat betreft het gebruiken van persoonsgegevens, is de Europese regelgeving en datastrategie sterk bepaald door de grondrechten van de Europese burgers, waar onder meer ook het recht op bescherming van persoonsgegevens is verankerd. Dit recht is vastgelegd in de 'Algemene Verordening Gegevensbescherming' of AVG (zie 2.2.1). Hoewel de AVG ten doel had om het gebruik, delen en verwerking van deze gegevens te faciliteren, ontbrak het aan voldoende stimulansen of kaders voor bedrijven om in Europa echt competitief te kunnen zijn in de data-economie. Dat bracht de Europese Commissie ertoe om een Europese datastrategie te ontwikkelen, die op zijn beurt werd ondersteund door specifieke regelgeving (o.a. Data Act, Data Governance Act en European Health Data Space, zie 2.2.2, 2.2.3 en 2.2.4).

De kern van de Europese datastrategie draait rond het makkelijker kunnen delen van gegevens tussen bedrijven, met respect voor de Europese waarden en normen, en het creëren van een gelijk speelveld voor alle partijen in de data-economie. In dat kader zijn bijkomende regelgevingen geïntroduceerd die misbruik door zogenaamde gatekeepers, of technologiebedrijven met een uitzonderlijk machtige positie wat betreft toegang tot gegevens, moeten tegengaan. Het uiteindelijke doel van de Europese datastrategie is om te komen tot zogenaamde dataruimtes (of in het Engels data spaces), een kader dat het delen van data mogelijk maakt in een data ecosysteem, en alle participanten duidelijke structuren en richtlijnen biedt om gegevens te delen, met aandacht voor een eerlijke behandeling van alle partijen in het ecosysteem, inclusief het recht van de burger op zeggenschap. De eerste van deze domein specifieke dataruimtes is de European Health Data Space (EHDS). De EHDS is een specifieke verordening voor gezondheidsgegevens, in tegenstelling tot de meer algemene Europese datawetten. De EHDS geeft behalve het juridische kader en de bestuursstructuur, ook het technische kader hoe dataruimtes moet worden ingericht.

In de volgende secties gaan we dieper in op de beschrijving van technische dataruimtes, en het meest gebruikte kader hierrond, om dan te kijken naar de regelgeving die de voornaamste impact heeft op zowel deze dataruimtes als het delen en hergebruik van persoonsgegevens, in het bijzonder gezondheidsgegevens.

2.1.2 Technische model dataruimtes IDSA- en DSSC-bouwblokken

2.1.2.1 Overzicht: International Data Space Alliance (IDSA)

Sinds het concept van dataruimtes aan tractie wint in Europa, is er een sterke bottom-up beweging actief om de concepten te testen en daar waar de voordelen aantoonbaar zijn deze concepten in de praktijk te brengen. Initieel was er veel versnippering, maar zijn de structuren en concepten rond dataruimtes nu meer aan het convergeren vanuit de impuls van enkele grote organisaties. 'The International Data Spaces Association - IDSA' is hier een sterkhouder in, naast Gaia-X (focus op gefedereerde en veilige infrastructuur), Simpl community[1] (bouwen van secure secure middleware platform bouwt dat data toegang en interoperabiliteit tussen European data spaces faciliteert), de Big Data Value Association/Adra (BDVA, promoten van datagedreven innovatie en AI-ontwikkeling in Europa) en de Fiware foundation (open-source tech stack). Tussen deze organisaties is ook wel interactie en er zijn overlappen in de deelnemende partijen. De organisaties, en het hele dataruimtes-ecosysteem in het algemeen worden verder ondersteund door het Data Spaces Support Centre (DSSC), een project bestaande uit verschillende expertorganisaties die de kennis rond dataruimtes consolideren en uitwerken naar concretere bouwblokken op technisch, legaal en business vlak.

IDSA heeft als doelstelling het opzetten van betrouwbare, veilige gestandaardiseerde kaders om data te gaan delen, die dan dataruimtes gaan vormen. Vanuit deze werking leverde IDSA het 'IDS Reference Architecture Model' (IDS-RAM) aan, een blauwdruk voor het opzetten van dataruimtes door het aanbieden van een technisch en governance kader. Het definieert verder kernconcepten rond dataruimtes die het mogelijk maken om op een soevereine manier data te gaan

[1] https://digital-strategy.ec.europa.eu/en/policies/simpl

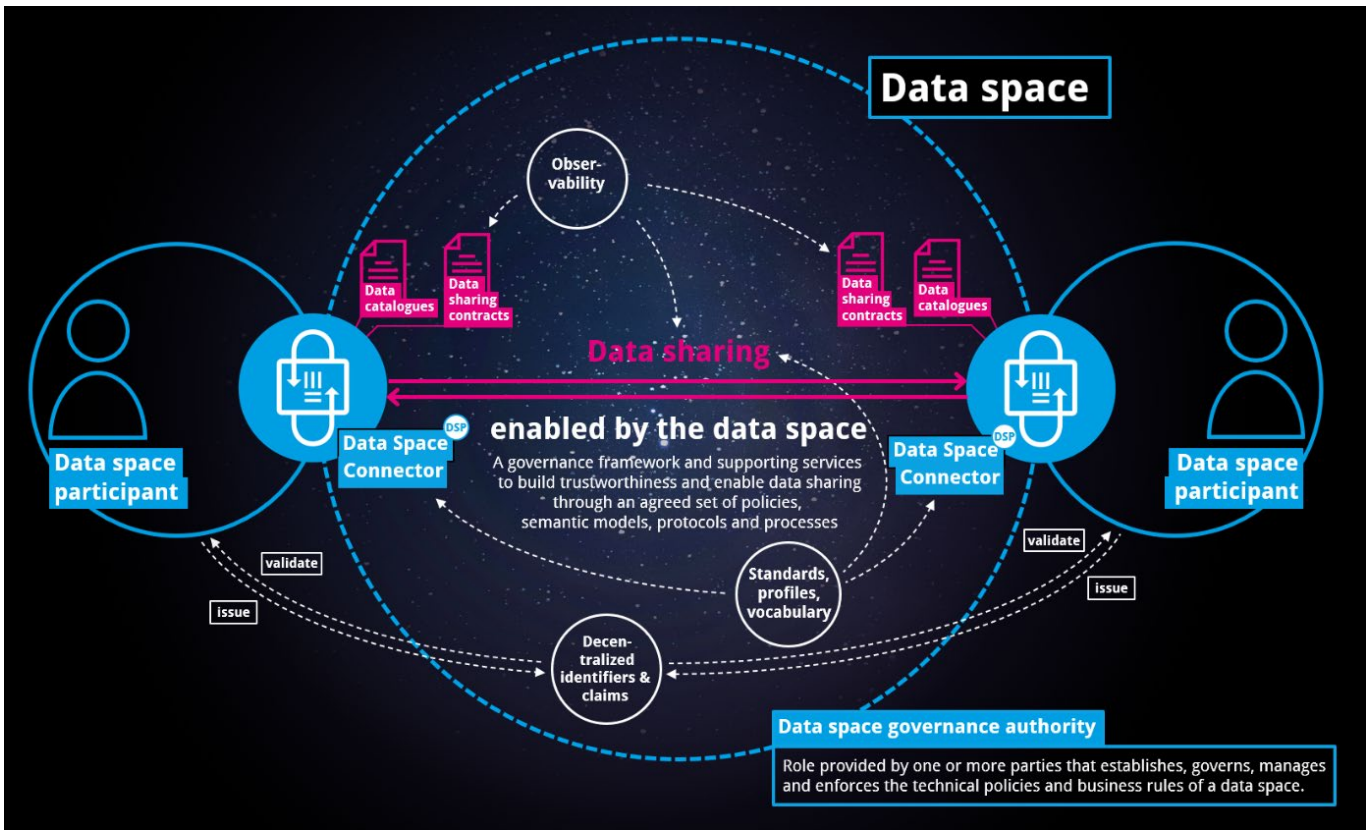
delen tussen organisaties. Dit wil zeggen dat organisaties controle houden over data onder hun verantwoordelijkheid en dat datadeling niet zorgt voor centralisatie van data in een apart platform maar dat door een gefedereerde aanpak de data veilig en onder controle worden gehouden. Hiervoor ontwikkelde IDSA het 'IDSA rulebook', dat de regels en interacties rond de rollen, verantwoordelijkheden en componenten vastlegt. Het 'Rulebook' vormt samen met IDS-RAM de kern van het Data Spaces Protocol (DSP)[2], een set regels gelijkaardig aan de richtlijnen rond het internet, een universele standaard die los van businessmodellen of specifieke technische componenten kan gebruikt worden. Het uiteindelijke doel van IDSA is interoperabiliteit en datadeling over alle dataruimtes mogelijk te maken en het tot een ISO-standaard te ontwikkelen.

Het DSP geeft aan hoe bedrijven of organisaties informatie over de data die ze willen delen kunnen aanleveren, zodat deze efficiënt kunnen worden gedeeld. Daarvoor moeten datasets worden omschreven in een **catalogus**, inclusief regels rond het gebruik van deze data. Als er data worden gebruikt, zijn er regels nodig rond het datagebruik en moeten er **overeenkomsten** afgesloten worden tussen de datahouder en datagebruiker, en ten slotte moet er omschreven worden hoe er toegang tot de data kunnen worden verkregen, en hoe de interacties in een dataruimte via verschillende **connectoren** worden opgezet en zorgt voor interoperabiliteit van deze informatie.

Het Simpl-programma is een EU-project dat de IDSA-standaarden implementeert in een real-world dataruimte oplossing. Simpl is een open source, smart en secure middleware platform dat toegang tot data en interoperabiliteit ondersteunt tussen Europese dataruimtes.

In Figuur 1 worden de verschillende componenten van een dataruimte weergegeven. In de kern draait het om een datahouder aan de ene kant, en een datagebruiker aan de andere kant. Om de datadeling te faciliteren is het nodig dat er informatie beschikbaar is over de databronnen in een dataruimte zoals hun structuur, inhoud, kwaliteit, enz. Deze informatie wordt ter beschikking gesteld door de 'broker'. Daarnaast is er een vocabularium nodig, dat gestandaardiseerde omschrijvingen voor de data voorziet. Om een betrouwbare uitwisseling mogelijk te maken, moeten de verschillende partijen correct worden geïdentificeerd door de 'identity provider'. In een 'app store' kunnen verschillende applicaties worden verzameld die bewerkingen op de data mogelijk te maken bv. data transformaties. Tussen de handelende partijen worden connectoren opgezet, waar de afspraken kaders en gebruiksregels worden bijgehouden. Alles wordt ten slotte gemonitord door de 'clearing house', die alle data en financiële transacties bijhoudt.

[2] https://internationaldataspaces.org/offers/dataspace-protocol/



Figuur 1. Componenten in een data space volgens IDSA[3]. Deze figuur toont de verschillende componenten, rollen en taken in een data space om de uitwisseling van data mogelijk te maken tussen een datahouder (data owner) en een datagebruiker (data user).

2.1.2.2 BLT – business, legaal, technisch: DSSC-bouwblokken

Ondanks het vastleggen van het protocol en rulebook, in combinatie met de verschillende andere, vaak meer technische componenten die worden aangeleverd door onder meer BDVA en Fiware, wil dit niet zeggen dat het opzetten van een dataruimte een evidentie is, en dat het eenvoudig starten is met de beschikbare informatie. Daarom is vanuit de Europese Commissie een project gelanceerd om alle informatie, technische, organisatorische en governance aspecten rond dataruimtes te gaan bundelen en vertalen naar praktische tools voor projecten, organisaties, consortia, enz. die van start willen gaan met een dataruimte. Dit is het Data Spaces Support Centre[4] (DSSC), en in deze sectie kijken we naar de beschikbare bouwblokken en activiteiten van het DSSC. Om een overzicht te geven op alle mogelijke data spaces componenten die zijn ontwikkeld, bundelde het DSSC alle gekende tools in de 'Data Spaces Toolbox'[5], gerangschikt volgens type van dienst die het aanbiedt (bv. catalogus, vocabularium, federatie, etc.). Daarnaast werd er een Blueprint[6] uitgewerkt, om ervoor te zorgen dat er een duidelijke gids voorhanden is om organisaties sneller en efficiënter dataruimtes te gaan opzetten, met oog voor efficiëntie van keuzes en aandacht voor de kostprijs en financiële haalbaarheid van de dataruimte. Door duidelijke richtlijnen te voorzien, is het derde doel de overdraagbaarheid van data en uitwisseling tussen dataruimtes mogelijk te maken. Organisaties krijgen inzichten in de kernconcepten van een dataruimte en door middel van een co-creatie methode worden ze vervolgens door de Blueprint geleid. Verder zijn er een

[3] https://internationaldataspaces.org/why/data-spaces/

[4] https://dssc.eu/

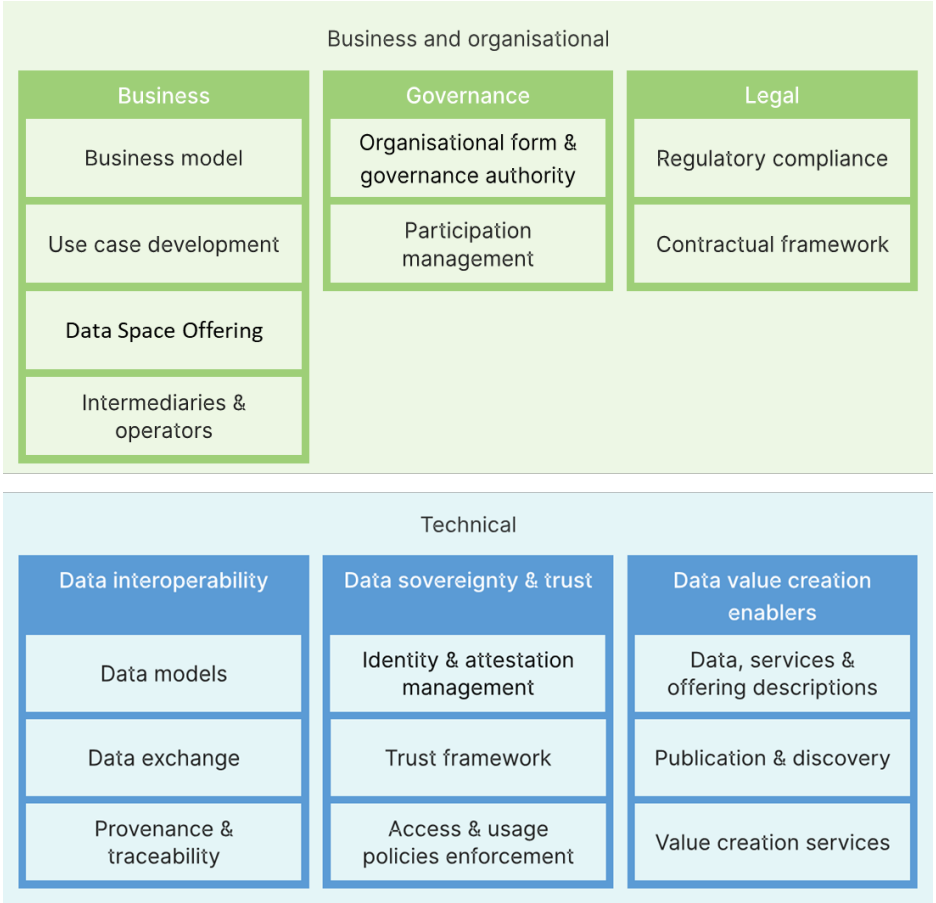
[5] https://toolbox.dssc.eu/

[6] https://dssc.eu/space/BVE2/1071251457/Data+Spaces+Blueprint+v2.0+-+Home

aantal technische en business-organisatorische bouwblokken gedefinieerd, waarna de tools en diensten in de Toolbox kunnen worden opgezocht.

De DSSC is met het concept van bouwblokken gestart om het concept van een dataruimte in behapbare blokken te kappen. Verschillende bouwblokken kunnen met elkaar gecombineerd worden om tot een dataruimte te komen.

Het business-organisatorische luik bestaat uit drie grote onderdelen met daaronder acht bouwblokken, het technisch luik uit drie onderdelen met in totaal negen bouwblokken (zie Figuur 2). De start van een succesvolle dataruimte start in het business-organisatorische luik: de meerwaarde van een dataruimte en de componenten en diensten die het aanbiedt om met de data te gaan werken moeten duidelijk zijn voor de deelnemers. In de volgende sectie gaan we dieper in op governance in een dataruimte, belangrijk hier nog is aan te geven dat het opbouwen van vertrouwen deel uitmaakt van de technische bouwblokken. Vertrouwen wordt hier geïnterpreteerd in onder meer het correct kunnen identificeren van de betrokken partijen, het vastleggen en opvolgen van toegangsregels tot de data. Contractuele en regulatorische regels worden daarentegen vastgelegd in het legale luik onder de business-organisatorische bouwblokken.



Figuur 2. De DSSC dataruimte-bouwblokken[7]. Het DSSC heeft een blauwdruk ontwikkelt die de verschillende bouwblokken omschrijven voor een dataruimte of data space. Die kunnen zich enerzijds op meer business-organisatorisch vlak bevinden, of meer technisch van aard zijn. Voor beide grote thematieken worden bouwblokken en adviezen voor implementatie omschreven.

[7] https://dssc.eu/space/BVE2/1071252426/Building+Block+Overview

2.1.2.3 Governance

We kijken hier specifiek naar governance-aspecten zoals gedefinieerd onder de DSSC-bouwblokken[8]. Onder het business-organisatorische luik zijn er twee governance bouwblokken terug te vinden: (1) organisational form & governance authority en (2) participation management. De bouwblokken hebben tot doel om de structuur, het beslissingsproces en het engagement van de deelnemers in de dataruimte vorm te geven. Het eerste bouwblok gaat over het keuzeproces om tot de correcte legale entiteit (wel of geen rechtspersoon) en organisatiestructuur van een dataruimte te komen, naast het vastleggen van het governance kader en autoriteit (o.a. vastleggen van interne regels en beleid, handhaven ervan, conflicten oplossen en ontwikkelingen van de dataruimte). Idealiter worden deze zaken voor de start van een dataruimte opgezet, zodat het afsprakenkader duidelijk is, al kan de governance structuur nog wijzigen doorheen het implementatieproces naarmate meer functionaliteiten bij een dataruimte worden toegevoegd, deze wijzigen of deze sterk groeit.

Het opzetten van een dataruimte start met een groep geïnteresseerde partijen die de basisdoelstellingen van de dataruimte vastleggen (welke sector, andere sectoren betrokken, welke data, enz.). Daarnaast dient er gewerkt te worden aan een realistisch businessmodel, dat gepaard gaat met bijkomende vragen rond de organisatorische structuur van de dataruimte (o.a. rechtspersoon of niet, tijdelijke of langdurige dataruimte, winstdoelmerk, enz.). Voor zowel dataruimtes met als zonder rechtspersoonlijkheid wordt dan verder ingegaan op de legale en organisatorische gevolgen van deze keuze, en het vormgeven van de governance-autoriteit. Ten slotte wordt het opzetten van het governance kader toegelicht, en naast de regulatorische aspecten die van buitenaf worden opgelegd, de interne spelregels die in de dataruimte zullen worden geïmplementeerd, dit houdt ook spelregels in rond de technische bouwblokken die in de dataruimte worden uitgebouwd.

2.1.2.4 Gap analyse en conclusies

De bovenstaande overzichten zijn slechts zeer beknopte aspecten van het brede domein dat dataruimtes inhoudt. Het basisconcept van een dataruimte zoals omschreven door IDSA kan als grotendeels gevestigd worden beschouwd. Wel zijn er nog heel wat vrijheidsgraden rond het implementeren van een dataruimte, zoals de sectie rond business en governance duidelijk maakt. Wel of geen rechtspersoon, wel of geen winstoogmerk, de interne spelregels, het hanteren van welke specifieke bouwblokken: het zijn allemaal nog keuzes die de participanten in de dataruimte dienen te maken. Dat vraagt een significant engagement van alle betrokken partners. Een recente white paper met analyses rond het succes en de rendabiliteit van dataruimtes geeft aan dat de duurzaamheid van een dataruimte nog niet gegarandeerd is, allicht omwille van die complexiteit[9], naast de uitdagingen om tot een voldoende datavolume te komen in een dataruimte om voldoende waardecreatie te garanderen voor de betrokken partijen. Allicht is er nog wel wat werk aan de winkel om de deelname aan een dataruimte voldoende eenvoudig te maken zodat niet-technische geïnteresseerde datahouders/eigenaars en datagebruikers laagdrempelig kunnen participeren. Kijk naar de analogie tussen het data ruimte protocol en het internetprotocol: bedrijven en personen hoeven nu geen technische bagage meer te hebben om een website op te zetten, dat gebeurt op de achtergrond, maar was in de begindagen nog wel nodig. Net zoals we niet verwachten dat om mails uit te wisselen we zelf nog een mailserver moeten gaan inrichten, moeten de dataruimtes evolueren naar eenvoudige plug-&-play elementen zodat de grote groep organisaties eenvoudig kan aansluiten. Ook de interoperabiliteit tussen dataruimtes kent nog vele uitdagingen: hoewel expliciet opgenomen in de doelstellingen van IDSA, werken sectoren vaak met eigen standaarden zodat de vertaalslag niet altijd evident is.

Ten slotte, als we dataruimtes zoals gedefinieerd bij IDSA, DSSC en de overige organisaties bekijken, stellen we vast dat het vooral vanuit de industrie benaderd wordt. Al of niet omgaan met persoonlijke data wordt eerder abstract behandeld, en valt eerder onder het navolgen van de regelgeving terzake. Een persoon als een actor in de dataruimte wordt niet als dusdanig gedefinieerd, terwijl de Europese regelgeving wel een grote rol voor personen in het delen van hun data faciliteert (zie Data Act 2.2.2 en Data Governance Act 2.2.3). Hoewel de eerder algemene aanpak van de DSSC rond de bouwblokken en het governance kader dit niet uitsluit, zou het beter zijn om inzichten te hebben in hoe een dataruimte

[8] https://dssc.eu/space/BVE2/1071253634/Governance+Building+Blocks

[9] https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Data-Spaces-Business-Models.pdf

waarin ook burgers participeren en hun persoonlijke data willen delen er uit zou kunnen zien (bv. gegevens over autobatterij om efficiënter energiebeheer mogelijk te maken, levensstijldata delen en impact op gezondheid om gezondere levensstijl te bevorderen, enz.), met daarrond een even duidelijk kader met bijhorende bouwblokken.

2.2 Regelgevend landschap

2.2.1 Algemene Verordening Gegevensbescherming (AVG)

2.2.1.1 Algemeen

De Algemene Verordening Gegevensbescherming of AVG dateert van 2016, en ging volledig van kracht in mei 2018. Het is een Europees geldende regelgeving om de gegevens van personen beter te gaan beschermen, en was deels gedreven door de explosie van datageneratie en datagebruik, en ook soms misbruik door derde partijen. De AVG legt spelregels vast om persoonsgegevens te gaan definiëren in het licht van deze ontwikkelingen, en waarborgen te gaan bieden aan data subjecten voor een meer rechtmatige, veilige en transparante verwerking van persoonsgegevens. Hoewel er te discussiëren valt hoe effectief de regelgeving is in deze doelstellingen, onder meer door verschillende accenten of interpretaties van de verschillende lidstaten, is het onmiskenbaar dat de regelgeving een sterke impact heeft gehad. Doordat de regelgeving van toepassing is op alle bedrijven met vestiging in de EU, en op alle verwerkingen van persoonsgegevens van betrokkenen die zich in de Unie bevinden, ook door niet in de Unie gevestigde organisaties, werden ook internationale bedrijven aan de regelgeving onderworpen. Dit had tot gevolg dat ook de grote techspelers zoals Meta en Amazon aan rechtszaken en hoge boetes werden onderworpen.

Ondanks alle nieuwe regelgeving rond het uitwisselen van gegevens binnen Europa, die we verder zullen bespreken, blijft de AVG het belangrijkste referentiekader om na te gaan of er bij het verwerken van persoonlijke gegevens de juiste rechtsgronden, doelen van verwerking en aandacht voor de rechten van de betrokken burgers zijn. Elk bedrijf of initiatief dat de ambitie heeft om persoonlijke gegevens te gaan verwerken, zal in de eerste plaats dus dit kader moeten volgen. Om vorm te geven aan een sluitend governancekader dient in overeenstemming met de AVG te zijn.

Belangrijk in de AVG is de brede definitie van zowel persoonsgegevens en de verwerking van persoonsgegevens. Persoonsgegevens betreffen alle informatie over een geïdentificeerde of identificeerbare persoon. Dat laatste punt is relevant, aangezien heel wat schijnbaar neutrale gegevens als een persoonsgegeven kunnen worden beschouwd indien ze door combinatie van gegevens tot de identificatie van de persoon kunnen leiden. Door de explosie aan (digitale) dataverzameling en geavanceerde analysetechnieken is dat veel makkelijker geworden dan ooit tevoren, in die mate dat er soms wordt getwijfeld of er nog over echt anonieme data kan gesproken worden. Geanonimiseerde data vallen expliciet niet onder de AVG, maar de drempel om over anonieme data te spreken, is hoog en wordt steeds hoger. Als we kijken naar de verwerking van persoonsgegevens, wordt hier ook breed gekeken: gegevens opslaan, wissen, gebruiken, ordenen, verstrekken, enz. Algemeen wordt gesproken over een ‘bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens’.

Verder legt de AVG de bescherming van persoonsgegevens vast rond een aantal principes, met een verantwoordingsplicht voor de verwerkingsverantwoordelijke (de persoon of organisatie die doel en middelen bepaalt voor de verwerking van persoonsgegevens):

1. Rechtmatigheid, behoorlijkheid en transparantie – Rechtmatig wil zeggen dat er een duidelijke wettelijke basis dient te zijn voor de verwerking van gegevens, door de AVG vastgelegd in art. 6.
2. Doelbinding – enkel voor welbepaalde gerechtvaardigde doeleinden, en geen verdere verwerking voor onverenigbare doeleinden. Met gerechtvaardigd wordt bedoeld dat er een duidelijke wettelijke basis moet zijn voor de verwerking van de gegevens, die eveneens door de AVG worden bepaald.
3. Minimale gegevensverwerking – enkel die gegevens mogen worden verwerkt die strikt noodzakelijk zijn voor het beoogde het doel.
4. Juistheid – de gegevens moeten juist zijn, en worden waar nodig gecorrigeerd.
5. Opslagbeperking – de opslag van persoonsgegevens kan niet onbeperkt, er dient een termijn te worden bepaald voor hoe lang de opslag van gegevens verantwoord is met betrekking tot het doel.
6. Integriteit en vertrouwelijkheid – er worden passende maatregelen genomen om de gegevens te beschermen tegen misbruik, verlies of beschadiging.

2.2.1.2 Rechten onder de AVG

Hoofdstuk 2 gaat uitgebreid in op informatie en toegang tot persoonsgegevens, Hoofdstuk 3-4 gaan over de rechten van de betrokkene en Hoofdstuk 5 legt beperkingen op deze rechten vast. Vooreerst is er informatieplicht om de betrokkene op de hoogte te stellen dat er gegevens van hem worden verwerkt, zowel wanneer de verwerkingsverantwoordelijke deze zelf heeft verzameld (art. 13) als wanneer deze niet rechtstreeks bij de betrokkene zijn verkregen (art.14).

De betrokkene heeft vervolgens volgende rechten:

1. Recht op inzage – hier wordt bepaald tot welke informatie de betrokkene toegang heeft, en het recht op een kopie van de verwerkte persoonsgegevens
2. Rectificatie – recht op het laten corrigeren van onjuiste informatie
3. Wissing – recht om vergeten te worden, echter enkel van toepassing indien aan een aantal voorwaarden is voldaan, onder meer dat er een toestemming is die ingetrokken is geweest, dat de gegevens niet meer nodig zijn voor verdere verwerking, of dat er een bezwaar is aangetekend en goedgekeurd.
4. Beperking van de verwerking – onder bepaalde voorwaarden kan een betrokkene vragen dat de verwerking van persoonsgegevens beperkt wordt. In die situatie worden de gegevens niet verder verwerkt buiten de opslag ervan, tenzij om gewichtige redenen zoals het uitoefenen van een rechtsvordering of het beschermen van de rechten van natuurlijke personen
5. Overdraagbaarheid van gegevens – dit is het dataportabiliteitsprincipe (zie ook 2.2.2.2), het recht om gegevens naar een andere verwerkingsverantwoordelijke over te dragen
6. Recht van bezwaar – betrokkenen kunnen bezwaar aantekenen tot de verwerking van hun gegevens onder de rechtsgronden van algemeen of gerechtvaardigd belang, of voor doelen van direct marketing. De verwerking wordt gestopt tenzij er gerechtvaardigde gronden zijn die zwaarder doorwegen dan de rechten van de betrokkenen.
7. Recht niet onderworpen te worden aan geautomatiseerde besluitvorming – dit betreft het recht om niet onderworpen te worden aan besluit uitsluitend gebaseerd op geautomatiseerde besluitvorming of profilering die de betrokkene kunnen treffen. Dit betreft een referentie naar systemen van artificiële intelligentie, in meer detail uitgewerkt in de recente AI Act.

Deze rechten zijn niet absoluut. Waar er voor sommige rechten al randvoorwaarden worden gesteld, zoals het recht op wissen dat enkel kan bij o.a. ingetrokken toestemming, goedgekeurd bezwaar van verwerking en onrechtmatige verwerking, is er een volledig artikel gewijd aan de beperkingen op deze rechten. Toch zijn ze vaak van toepassing, en dienen verwerkingsverantwoordelijken mechanismen op te zetten om te zorgen dat de betrokkenen in de mogelijkheid zijn om hun rechten uit te oefenen. Vaak worden deze vragen rond de rechten gekanaliseerd via een apart contactkanaal, of via de data protection officer (DPO) van een organisatie.

2.2.1.3 Aandachtspunten gezondheidsgegevens

Naast de algemene bepalingen rond het beschermen van persoonsgegevens, is er in de AVG uitgebreide aandacht voor zogenaamde ‘bijzondere categorieën van persoonsgegevens’. Dit zijn persoonsgegevens met een grote sensitiviteit, en waarrond extra beschermingsmaatregelen en verwerkingsbeperkingen worden opgelegd. Het betreft gegevens rond ras en etniciteit, genetische, biometrische en gezondheidsgegevens, politieke of religieuze/levensbeschouwelijke opvattingen, vakbond lidmaatschap of gegevens rond seksueel gedrag of geaardheid.

Bijzonder in de AVG is dat er een feitelijk verbod geldt op het verwerken van deze persoonsgegevens, tenzij er aan een aantal voorwaarden wordt voldaan, die in art. 9 staan gedefinieerd. In combinatie met de rechtsgronden die in art. 6 zijn opgenomen, dient er dus voor de verwerking van gezondheidsgegevens zowel een duidelijke wettelijke basis te zijn (art. 6), én moet er voldaan zijn aan minstens één van de voorwaarden onder art. 9. Die voorwaarden zijn onder meer toestemming, beschermen van vitale belangen, archivering in algemeen belang, wetenschappelijk onderzoek, of voor preventieve of arbeidsgeneeskunde of gezondheidszorg.

Hoewel er geen specifieke beveiligingsmaatregelen worden voorgesteld in de AVG, dienen deze proportioneel te zijn naar risico en impact op de betrokkenen (art. 32 en overweging 74), en wordt in de overwegingen voorafgaand aan de

AVG duidelijk aangegeven dat de impact wat betreft gezondheidsgegevens hoog is, en de beschermingsmaatregelen daaraan te dienen worden aangepast (overweging 75).

2.2.1.4 Delen/(her)gebruik van data met derde partijen

Zoals eerder aangehaald, moet er voor de verwerking van persoonsgegevens een welbepaald doel en rechtsgrond worden voorzien. De persoonsgegevens mogen dan enkel voor dit doel worden verwerkt. Als er verdere verwerking zou plaatsvinden, moet dat voor een doel zijn dat verenigbaar is met het oorspronkelijke doel van de verwerking, en in dat geval is geen andere rechtsgrond nodig (overweging 50). Dat heeft met name betrekking op de rechtsgronden van gerechtvaardigd belang, overeenkomst of vitale belangen[10], voor toestemming of op wettelijke basis kan verdere verwerking enkel als er een nieuwe toestemming of wettelijke basis is. Wetenschappelijk onderzoek of statistische doeleinden worden verder altijd als verenigbaar gezien (zie voor meer detail sectie 2.2.1.5). Voor overige doeleinden dient er een toetsing te gebeuren om na te gaan of het nieuwe doel verenigbaar is (art. 6.4), en dient men het verband tussen beide doelen in rekening te nemen, de context waarin de gegevens zijn verzameld, de soort en aard van de gegevens, de mogelijke gevolgen van de verwerking en het bestaan van passende veiligheidsmaatregelen. Indien de gegevens voor een ander doel worden gebruikt, dient dit voor deze nieuwe verwerking te worden meegedeeld aan de betrokkene (overweging 61, art. 13.3 en art. 14.4). Indien het doel van de verdere verwerking direct marketing is, heeft de betrokkene altijd recht van bezwaar.

Wat betreft delen van gegevens of doorgeven van gegevens aan andere partijen dan de oorspronkelijke verwerkingsverantwoordelijke, kan het zijn dat de gegevens worden verwerkt in opdracht van de verwerkingsverantwoordelijke door een verwerker (bv. elektronisch patiëntendossiersysteem verwerkt patiëntengegevens van een arts, die de verwerkingsverantwoordelijke is). De rechten en plichten van de verwerkingsverantwoordelijke en verwerker zijn uitvoerig beschreven in de AVG, en eveneens in welke mate de betrokkene dient geïnformeerd te worden. Het is ook mogelijk dat de gegevens worden doorgegeven aan andere verwerkingsverantwoordelijken. Dit kan enkel indien dit rechtmatig is, en valt onder het doel van de verwerking. Bij eerste doorgifte van de gegevens dient de betrokkene geïnformeerd te worden (overweging 61).

Derde partijen die zich buiten de Europese Unie bevinden, kunnen ontvangers zijn van persoonsgegevens, maar daar moeten er garanties zijn dat er dezelfde passende veiligheidsmaatregelen kunnen worden getroffen als de data binnen de EU zouden verwerkt worden (overweging 101, 102 en 103 en Hoofdstuk V). Met een aantal niet-EU landen werden overeenkomsten afgesloten waardoor de uitwisseling van gegevens met deze landen als voldoende veilig worden beschouwd, en deze overeenkomst voldoende garanties biedt voor veilige doorgifte. Echter, in het geval van onder meer de Verenigde Staten zijn deze overeenkomsten onderhevig geweest aan rechtszaken die deze waarborgen in vraag stellen, met vernietiging van de geldigheid van deze overeenkomsten tot gevolg (zie oa. Schrems I en Schrems II).

2.2.1.5 Delen/(her)gebruik van data voor onderzoek

In verschillende secties wordt ingegaan op het gebruik van persoonsgegevens voor wetenschappelijk onderzoek. In de praktijk komt het vaak neer op het omschrijven van uitzonderingsmaatregelen voor gebruik van persoonsgegevens voor wetenschappelijk onderzoek, archiverings- of statistische doeleinden. Wat er juist begrepen wordt onder wetenschappelijk onderzoek, is terug te vinden in overweging 159.

Zo gaan een aantal van de overwegingen in op de bijzondere omstandigheden rond wetenschappelijk onderzoek, zoals het niet altijd exact kunnen omschrijven van het doel van de gegevensverwerking, vereist in het principe van doelbinding (overweging 33). Verdergaand op de doelbinding, wordt verwerking voor wetenschappelijk onderzoek beschouwd als verenigbaar met het oorspronkelijke doel van de verwerking (overweging 50 en art. 5.1.b). Waar in de meeste omstandigheden een nieuwe verwerking of hergebruik van data voor een ander doel bijkomend moet worden verantwoord of niet toegestaan is, is dit in het geval van wetenschappelijk onderzoek vaak niet nodig.

[10] https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_nl

Voor de beperking van de verwerking van gevoelige gegevens onder art. 9 wordt eveneens wetenschappelijk onderzoek gezien als een rechtmatige uitzondering (overweging 52 en 53 en art. 9.2.j).

De informatieplicht ten opzichte van de betrokkene kan wegvallen in geval van wetenschappelijk onderzoek indien het onmogelijk blijkt of onevenredig veel inspanning zou kosten (overweging 62 en art. 14.4.b). Ook op de beperking van de opslag kan in het geval van wetenschappelijk onderzoek afgeweken worden (overweging 65 en art. 5.1.e), net zoals onder omstandigheden ook andere uitzonderingen op de uitoefening van rechten van betrokkenen. Art. 89 handelt specifiek over de waarborgen en afwijkingen in verband met wetenschappelijk onderzoek.

Wel is wetenschappelijk onderzoek geen vrijgeleide. De passende beschermingsmaatregelen dienen ook hier in acht genomen te worden, evenals het gegevensminimalisatieprincipe. Dat laatste is geen evidentie in tijden van AI-analyses die op grote datasets worden losgelaten, en waar soms schijnbaar niet-relevante gegevens een voorspellende waarde kunnen hebben. Het kan ertoe leiden dat onderzoekers geneigd zijn eerder meer dan minder gegevens in hun analyses op te nemen. Wat betreft beschermingsmaatregelen, geldt voor wetenschappelijk onderzoek onder meer de opties van anonimisatie of pseudonimisatie van gegevens (overweging 156 en art. 89).

2.2.2 Data Act (DA)

2.2.2.1 Algemeen

In de Europese datastrategie wordt vooropgesteld dat data makkelijker moet kunnen gedeeld worden tussen organisaties om de data-economie te gaan versterken, en innovatie op basis van data te vergemakkelijken[11]. Dit past in het concept van zogenaamde ‘data spaces’ of dataruimtes (zie 2.1.2). Ter ondersteuning van deze datastrategie, en om het oprichten van dataruimtes te gaan bevorderen, werden er de voorbije jaren een aantal regelgevingen uitgewerkt. Een aantal daarvan, zoals de Data Act en de Data Governance Act (zie 2.2.3), zijn overkoepelende regelgevingen, terwijl andere sectorspecifiek zijn (met als eerste voorbeeld de ‘European Health Data Space’ of EHDS, zie 2.2.4).

De focus van de Data Act ligt op het makkelijker gaan ontsluiten van industriële data. Door de enorme explosie van data-genererende toestellen en applicaties de laatste jaren (o.a. ‘Internet of Things’ of IoT, dit is het verbonden zijn van toestellen, applicaties, enz. via het internet of andere netwerken), is er een enorm datapotentieel ontstaan. Dit potentieel blijft onderbenut doordat meestal enkel de producenten van deze toestellen of applicaties toegang hebben tot deze data. Via de Data Act wil men daarom een eerlijke, gelijkwaardige toegang verzekeren tot deze databronnen. Daarnaast krijgen ook de datasubjecten (personen waarover data worden gegenereerd door het gebruik van toestellen of applicaties), meer zeggenschap over hun eigen data. Meer specifiek gaat het over de gebruiker van het geconnecteerde product, waaronder de eigenaar wordt verstaan of iemand die contractuele rechten heeft bv. via huur of leasing.

De aanpak van de Data Act specifiek rond datadeling bestaat uit een aantal grote componenten[12]:

1. het delen van data in de context van IoT, waar gebruikers (individuen of bedrijven) van dergelijke toestellen of applicaties toegang kunnen krijgen tot de door hen gegenereerde data, deze kunnen gebruiken en ook overdragen (zie ook 2.2.2.2)
2. het vastleggen van de randvoorwaarden waarrond bedrijven verplicht zijn data te delen met andere bedrijven
3. het vastleggen van de voorwaarden waaronder overheden toegang kunnen krijgen tot industriële data in situaties van uitzonderlijk publiek belang
4. het beschermen van (niet-persoonlijke) data tegen onrechtmatige toegang door derde landen (dit zijn niet-Europese landen)
5. de randvoorwaarden voor interoperabiliteit waaraan bedrijven moeten voldoen die willen deelnemen aan een data ruimte.

[11] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[12] https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

Daarnaast zijn er nog hoofdstukken die bedrijven beschermen tegen onrechtmatige bepalingen in contracten, het makkelijker maken om te wisselen tussen clouddiensten en het vastleggen van de relevante autoriteiten om de bepalingen in de Data Act op te gaan volgen.

2.2.2.2 Dataportabiliteit

We bekijken even de impact van de Data Act op persoonlijke data en meer bepaald wat dit betekent voor de data subjecten zoals gedefinieerd onder de AVG. Hoofdstuk II handelt hier specifiek over. Hoewel dit ook bedrijven omvat die toestellen gebruiken die data genereren (bv. landbouwbedrijf en de door hen gebruikte machines), beschouwen wij hier enkel de persoonlijke data en individuen. In de context van een dataruimte voor preventie waar er wordt gekeken naar applicaties, toestellen en toepassingen die levensstijl en welzijnsinformatie capteren, is dit een belangrijk nieuw element in het bestaande regelgevend kader. De Data Act werd goedgekeurd december 2023 en zal van toepassing worden 12 september 2025, wat het tot één van de meest recente regelgevingen maakt rond datagebruik en de impact op de rechten van burgers.

We kiezen hier voor 'dataportabiliteit' als titel, omdat er een duidelijke link te leggen is tussen de dataportabiliteitsrechten van data subjecten onder de AVG en de rechten van gebruikers van IoT toestellen op de door hen gegenereerde data. Hoofdstuk II legt immers een verplichting vast naar de producenten van deze toestellen om data toegankelijk te maken tot de gebruikers van deze toestellen. Het gaat meer specifiek over de IoT toestellen en de daaraan verbonden diensten, en de data van het product en de gerelateerde dienst, inclusief de metadata moeten direct toegankelijk zijn voor de gebruikers. Daarnaast hebben de gebruikers het recht om deze data over te dragen aan derde partijen. Er zijn echter wel beperkingen op, zo is dit niet van toepassing op toestellen die nog niet op de markt zijn, en is er ook een beperking tot welke derde partijen deze data mogen krijgen. Zo worden een aantal grote tech spelers, de zogenaamde 'gatekeepers' uitgesloten (Alphabet, Amazon, Apple, Booking, ByteDance, Meta, Microsoft)[13]. Deze spelers hebben immers een sterke impact op de interne markt en hebben een poortwachter functie: ze zijn een belangrijke toegangspoort van bedrijven tot eindgebruikers (o.a. via sociale media, via advertentie of via bemiddelingsdiensten zoals Booking). Door hun omzet en bereik kunnen ze de interne markt verstoren, en via bijkomende regelgeving[14] worden deze bedrijven verder gereguleerd om eerlijke digitale markttoegang te gaan verzekeren.

In hoofdstuk II worden verder nog bepalingen vastgelegd om deze uitwisseling tussen de producent en de derde partij te regelen: er mag niet meer informatie uitgewisseld worden over de persoon dan nodig om vast te stellen dat de vraag terecht is, en ook mag de producent geen informatie bijhouden over de derde partij dan strikt noodzakelijk is om de vraag uit te voeren. Hier zien we weer principes die refereren aan het data minimalisatieprincipe uit de AVG (zie art. 5). De datahouder/producent wordt ook beschermd, zo worden bedrijfsgeheimen maximaal gevrijwaard en mag de derde partij geen druk uitoefenen om de data te bekomen, of mag de data niet gebruikt worden voor het ontwikkelen van een competitief product. Ook mag de datahouder weigeren als er zwaarwegende negatieve economische impact wordt verwacht, al dient deze dat wel te onderbouwen.

Er wordt vaak gerefereerd naar de AVG in dit hoofdstuk, onder meer in het bepalen dat de data beschikbaar dienen worden gesteld in een makkelijk, veilig, omvattend, gestructureerd en machine-leesbaar formaat, en dit vrij van kosten. Indien mogelijk dient deze data zelfs in real-time ter beschikking te worden gesteld. Mochten data-houder en de derde partij er overeenkomen over hoe de data moeten worden uitgewisseld, blijft het dataportabiliteitsprincipe van de AVG van toepassing (art. 20). Verder wordt er naar de AVG verwezen als het gaat over vragen tot toegang tot de data door iemand anders dan het datasubject zelf. Dit kan enkel als daar een wettelijke basis voor is (art. 6 van de AVG en relevante bepalingen van art. 9 van toepassing). Ten slotte wordt er naar de AVG verwezen door vast te leggen dat de rechten van de data subjecten rond de bescherming van hun data gevrijwaard is. Dit wil zeggen dat het beschikbaar stellen van de data aan de datasubjecten niet ten koste mag gaan van de veiligheid.

[13] https://digital-markets-act.ec.europa.eu/gatekeepers_en

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925#d1e1494-1-1

We kunnen deze Hoofdstuk II en meer bepaald art. 3 beschouwen als een uitbreiding van het dataportabiliteitsprincipe van de AVG. Het dataportabiliteits-principe van de AVG is van toepassing bij de wettelijke basis van toestemming of contract, en hier handelen de rechten van de gebruikers over toestellen die ze in bezit hebben, huren of leasen, en waar meestal wel een contractuele basis rond bestaat. Het contract dient zelf als basis om te bepalen wie de datahouder is (bv. auto en een app om instellingen in de auto te gaan wijzigen. Als dit twee verschillende bedrijven zijn, zijn er twee mogelijke datahouders). De AVG spreekt van overdracht naar een andere verwerkingsverantwoordelijke, terwijl de Data Act het enkel over 'derde partijen' heeft, die bedrijven of individuen kunnen zijn. Waar de AVG enkel uitspraak doet over persoonlijke gegevens, includeert de Data Act ook niet-persoonlijke gegevens. Verder gaat de Data Act iets meer in op het transparant zijn over de door de datahouder verwerkte data, en het makkelijk maken van de toegang tot de data en de data overdracht.

2.2.3 Data Governance Act (DGA)

2.2.3.1 Algemeen

De Data Governance Act[15] is de tweede grote Europese regelgeving die overkoepelend werd ontwikkeld ter ondersteuning van het ontwikkelen van een gemeenschappelijke Europese Dataruimte, en wil het vertrouwen in het delen van data gaan bevorderen en de beschikbaarheid van data gaan verhogen. Om dit te realiseren zet de Data Governance Act[16] in op volgende grote pijlers:

1. het reguleren van het (her)gebruik van publieke sector data (dit is data in beheer van overheden of overheidsdiensten)
2. het bevorderen van het delen van data via databemiddelingsdiensten
3. door het aanmoedigen van het delen van data om altruïstische redenen.

Waar er via de 'Open Data Directive' al richtlijnen waren rond het gebruik van data uit de publieke sector, zijn veel data die hieronder vallen beschermd waardoor ze niet kunnen hergebruikt worden. De Data Governance Act legt de spelregels vast waaronder deze data kunnen gedeeld worden, met voldoende waarborgen die er moeten zijn rond de veiligheid van deze data. De Data Governance Act is al eerder goedgekeurd dan de Data Act, in 2022, en is van toepassing sinds september 2023. De nationale autoriteiten die bevoegd zijn rond de Data Governance Act waren wel niet allemaal beschikbaar vanaf dat moment, de adoptie van de Data Governance Act in de nationale regelgeving en het aanwijzen van de bevoegde autoriteiten dateren voor zowel België als Nederland van 2024[17,18].

2.2.3.2 Databemiddelingsdiensten en gegevenscoöperaties

Relevant voor persoonlijke data en de data subjecten zijn de bepalingen rond onder meer databemiddelingsdiensten en gegevenscoöperaties (hoofdstuk III). We bekijken eerst de databemiddelingsdiensten als overkoepelende term. Dit concept werd in het leven geroepen om voldoende garanties te bieden aan bedrijven zodat er geen misbruik zou gemaakt worden van het delen van data, of dat ze daardoor een competitief voordeel zouden gaan verliezen. Door een neutrale tussenpartij te hebben tussen dat bedrijf en een derde partij, wordt er zo een veilige omgeving gecreëerd om in vertrouwen data te gaan delen in alle transparantie, met voldoende zeggenschap voor de individuen of bedrijven waarover de data gaan of die belang hebben in de data. Deze diensten kunnen ook gebruikt worden door individuen die data willen gaan delen, waardoor op deze manier ook data subjecten meer zeggenschap en beslisrecht krijgen met wie ze hun data gaan delen.

---

15 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022R0868

16 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

17 https://economie.fgov.be/nl/themas/online/data-economie/data-governance-act

18 https://www.acm.nl/en/publications/data-governance-act-registration-data-intermediation-service-providers-and-application-eu-label-now-online

Om te waarborgen dat een databemiddelingsdienst een neutrale partij is, moeten deze aan een aantal voorwaarden voldoen. Zo mogen deze diensten de data waarrond ze intermediëren niet voor eigen financieel gewin gaan gebruiken, of commerciële diensten aanbieden die gebruik maken van deze data. De databemiddelingsdiensten moeten dus structureel gescheiden zijn van andere diensten die ze aanbieden. Het gebruik van data of metadata kan enkel dienen om de databemiddelingsdiensten te gaan verbeteren. Ook mag de kostprijs voor de databemiddelingsdiensten niet afhankelijk zijn van het gebruik van andere diensten die het bedrijf bijkomend zou aanbieden. Verder wordt in de Data Governance Act vastgelegd dat deze diensten zich moeten aanmelden bij de bevoegde overheidsdienst om het label van erkende databemiddelingsdienst erkend door de EU te ontvangen. In België is dit de FOD Economie, in Nederland de Autoriteit Consument en Markt[19]. In het centrale register voor databemiddelingsdiensten zijn de erkende diensten terug te vinden[20]. In België zijn dit Athumi (Vlaams datanutsbedrijf, een verzelfstandigd agentschap opgericht vanuit Digitaal Vlaanderen) en DataJoy, een bedrijf gevestigd in Brussel dat dataportabiliteit makkelijker maakt, en waarmee de link met de stijgende dataportabiliteitsmogelijkheden die de Data Act biedt te maken valt. In Nederland zijn er vier databemiddelingsdiensten in het register opgenomen (fairsfair.io, Luminis Technologies, WeCity Data market en Yivi). Hun aanbod varieert van standaard databemiddelingsdiensten naar bijkomende cloudoplossingen en een digitale identiteit applicatie.

Een derde vorm van databemiddelingsdiensten (naast bemiddeling tussen gegevenshouders – bedrijven- en gegevensgebruikers enerzijds en datasubjecten of natuurlijke personen die persoons of niet-persoonsgebonden gegevens willen gaan delen met gegevensgebruikers anderzijds) zijn de gegevenscoöperaties. Die bemiddelen niet zozeer in het uitwisselen van data, maar vooral in het ondersteunen van het uitoefenen van rechten op data. Onder meer in het maken van onderbouwde keuzes vooraleer toestemming te gaan geven voor het gebruik van data, het onderhandelen over voorwaarden voor gegevensverwerking en het analyseren van de doeleinden van de verwerking. Naast de definitie, de positionering van de gegevenscoöperatie onder de databemiddelingsdiensten en een overweging voorafgaand aan de bepalingen van de Data Governance Act (overweging 31), gaat de Data Governance Act niet dieper in op dit type databemiddelingsdienst.

2.2.3.3 Data-altruïsme

Een laatste relevant hoofdstuk van de Data Governance Act betreft data-altruïsme. Hier wordt in de omschrijvingen, praktische uitwerking en redenering achter dit concept vaak verwezen naar de meerwaarde van data-altruïsme in de context van gezondheid. Data-altruïsme betreft het vrijwillig en zonder bijkomende vergoeding ter beschikking stellen van data gegenereerd door individuen of bedrijven voor gebruik in het kader van algemeen belang.

Hoewel studies aantonen dat er wel een bereidheid is om data te delen, wordt dit in de praktijk niet gedaan door het ontbreken van de juiste toepassingen of diensten om data te delen. Daarom roept de Data Governance Act, naar analogie met de databemiddelingsdiensten, data-altruïsme-organisaties in het leven als een vertrouwde en erkende dienst om data delen te gaan organiseren voor algemeen belang. Deze diensten kunnen erkend worden als data-altruïsmedienst, en net zoals de databemiddelingsdiensten, moeten ze aan een aantal voorwaarden voldoen. Zo moeten ze non-profit zijn, beantwoorden aan transparantievoorwaarden en moeten ze de rechten beschermen van de individuen die hun data delen. Daarnaast dienen ze de spelregels te volgen die de Europese Commissie vastlegt rond de te volgen voorwaarden o.a. interoperabiliteit, veiligheid, enz. Verder zullen deze organisaties worden opgenomen in het register voor erkende altruïsme-organisaties[21]. Momenteel bevat het register maar twee dergelijke organisaties, waarvan één in Spanje en één in België (101 Genomes, European Brain Data Hub)[22].

19 https://www.acm.nl/nl/digitale-economie/data

20 https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services

21 https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations

22 https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations

2.2.4 European Health Data Space (EHDS)

2.2.4.1 Algemeen

De European Health Data Space verordening is de eerste sectorspecifieke regelgeving die werd uitgevaardigd om naast de algemene verordeningen ter ondersteuning van het uitbouwen van dataruimtes (DA en DGA, zie 2.2.2 en 2.2.3) ook specifieke regels te hanteren binnen een specifiek domein. De COVID-19 crisis wordt in de overwegingen van de verordening vaak als reden aangehaald voor het belang van het opzetten van een Europese gezondheidsdataruimte, en gezien ook het algemeen belang van efficiënte datadeling in de gezondheidszorg, is daarom in de eerste plaats voor het gezondheidsdomein gekozen als eerste sectorspecifieke regelgeving. Daarnaast wordt ook de verschillende interpretaties van de lidstaten rond onder meer de categorieën van gevoelige gegevens, zoals gezondheidsgegevens, uit de AVG, en verschillen in interpretaties rond de rechtsgronden en uitzonderingen rond wetenschappelijk onderzoek als reden aangehaald waarom er nood is aan een meer eenduidig verhaal rond het delen van gezondheidsgegevens.

Het voornaamste doel van de EHDS is een kader creëren waarbinnen toegang tot gezondheidsgegevens makkelijker wordt in een primaire context (verschaffen gezondheidszorg) en een secundaire context (hergebruik van die gegevens). Voor primair gebruik beoogt de EHDS vooral om de toegang van natuurlijke personen tot hun persoonlijke elektronische gezondheidsgegevens en hun zeggenschap over die toegang voor derden te gaan verbeteren. Verder wordt in het bijzonder de cross-border context van gezondheidsgegevens aangehaald: de noodzaak van een uniform elektronisch format om personen de mogelijkheid te bieden makkelijker ook over de grens hun gegevens te delen (overweging 6). In dat kader is MyHealth@EU opgericht, een gemeenschappelijke infrastructuur die het uitwisselen zou moeten faciliteren (overweging 33, 34 en 35 en Afdeling 3).

2.2.4.2 Primair gebruik in preventie en wellnessapps

Onder **primair gebruik** wordt verstaan ‘de verlening van gezondheidszorg om de gezondheidstoestand van de natuurlijke persoon op wie die gegevens betrekking hebben te beoordelen, te behouden of te herstellen, waaronder het voorschrijven en het verstrekken van geneesmiddelen en medische hulpmiddelen, alsmede voor relevante sociale, administratieve of vergoedingsdiensten’ (art. 2.1d). Dit valt toch enigszins te onderscheiden van hoe de AVG aankijkt tot een oorspronkelijke of verdere verwerking van persoonsgegevens, daar wordt gekeken naar het oorspronkelijke doel van de verwerking. In de context van gezondheidsgegevens kan de verwerking ervan verschillende doelen hebben, verwerking in de context van gezondheidszorg is daar maar één van (bv. Art. 9.2h).

Door de expliciete koppeling met het verzamelen van gegevens voor gezondheidszorg, wordt ook de link gemaakt met de **Elektronische Patiëntendossiersystemen** (EPD) die ervoor moeten zorgen dat deze gegevens op een kwalitatieve en toegankelijke manier kunnen worden verwerkt, gelogd, gedeeld, etc. In verband met het primair gebruik van gezondheidsgegevens wordt bijgevolg uitgebreid ingegaan op de vereisten voor deze systemen (zie Hoofdstuk III). Toegang tot deze dossiersystemen moet verder ook nog voorzien worden volgens de EHDS onder meer via toepassingen voor toegang van personen tot hun elektronische gezondheidsgegevens, en toepassingen voor toegang voor zorgverleners (zie onder meer Artikel 4, Artikel 11 en Artikel 12).

Binnen het primair gebruik worden de **rechten van de betrokkenen** uitgebreid uitgelicht (overweging 8, 9, 10, 12, 13 en art. 3, 5, 6, 7). Er wordt weer expliciet verwezen naar de rechten onder de AVG, en de uitbreiding van deze rechten zoals bepaald in de EHDS. Er wordt onder meer specifiek ingegaan op het recht tot toegang tot de eigen elektronische gezondheidsgegevens, met minimale prioritaire categorieën, het recht op een kopie en het omschrijven van de mogelijkheid tot toegang via onder meer patiënten-portalen. Wel kan het recht op toegang worden beperkt, door bijvoorbeeld een vertraging in te bouwen indien het om ethische overwegingen beter is dat een zorgverlener de betrokkene eerst zelf informeert. Verder is er een bijkomend recht op zelf gegevens in het EPD te laten opnemen, al wordt aangegeven dat dit duidelijk moeten kunnen worden onderscheiden van de informatie aangeleverd door zorgverleners. Rechtstreekse wijzigingen van gegevens van zorgverleners zijn niet mogelijk, wel wordt het recht tot rectificatie verduidelijkt.

Personen kunnen ook meer **zeggenschap** uitoefenen op de toegang tot hun gezondheidsgegevens. Vooreerst wordt het dataportabiliteitsrecht uitgebreid, en kunnen personen in alle omstandigheden hun elektronische gezondheidsgegevens

of een deel ervan overdragen naar een zorgverlener van hun keuze. Daarnaast kunnen ze ook de toegang beperken van bepaalde zorgverleners tot hun elektronische gezondheidsgegevens of een deel ervan. Algemeen moeten ze ook een overzicht kunnen krijgen van wie er toegang tot hun gezondheidsgegevens heeft.

In het primair gebruik wordt er verder een **opt-out** procedure omschreven, waardoor bepaalde diensten de toegang tot de geregistreerde gezondheidsgegevens in het EPD kan ontzegd worden. Deze opt-out wordt lidstatelijk vastgelegd, en als het van toepassing is, dient het wel omkeerbaar te zijn (art. 10).

Verder omschrijft de regelgeving overwegingen en verplichtingen rond **wellnessapps**, die als een belangrijke leverancier van levensstijl- en welzijnsgegevens kunnen worden beschouwd (overweging 49, en art. 47, art. 48 en art. 49). Zo moeten personen geïnformeerd worden als dergelijke apps gekoppeld kunnen worden met een EPD-systeem. Het belang van interoperabiliteitsvereisten wordt aangehaald, anderzijds worden de wellnessapps als een databron beschouwd met een beperkte relevantie voor de gezondheidszorg, en wordt om die redenen afgezien van een verplichte certificering. Als alternatief wordt een vrijwillig label opgericht, en mogelijkheid tot registratie. Verdere aspecten rond het gebruik van wellnessapps worden aan de lidstaten zelf overgelaten (overweging 50). Voor medische hulpmiddelen wordt verwezen naar de bestaande regelgeving die dit verder vastlegt (overweging 51).

Hoewel de EHDS sinds maart 2025 is goedgekeurd, moeten nog veel implementatierichtlijnen volgen en is er ook een tijdspad opgesteld die enkele deadlines en mijlpalen weergeeft rond de implementaties[23]. Het eindpunt van de implementaties wordt in 2034 gelegd. Voor secundair gebruik van bepaalde categorieën, en onder meer ook de regels rond wellnessapps, ligt de deadline op 2031.

2.2.4.3 Secundair gebruik, governance en wellnessapps

Naast primair gebruik van data, definieert de EHDS ook **secundair gebruik**, met name ‘de verwerking van elektronische gezondheidsgegevens voor de in hoofdstuk IV van deze verordening vermelde doeleinden, anders dan de oorspronkelijke doeleinden waarvoor zij zijn verzameld of gegenereerd’. Deze definitie ligt meer in lijn met wat de AVG als een bijkomende verwerking beschouwt: verwerking voor een ander dan het oorspronkelijke doel van verwerking. De soorten doeleinden worden wel nauwer bepaald, en zijn vastgelegd in art. 53, onder meer algemeen belang, statistieken, beleidsvorming, onderwijs, en verbeteren van zorgverlening en optimaliseren behandelingen op basis van gegevens van andere natuurlijke personen. Ook wetenschappelijk onderzoek hoort bij de doeleinden, meer bepaald onderzoek dat een bijdrage levert aan de volksgezondheid of evaluatie van gezondheidstechnologie, of waarmee een hoog kwaliteits- en veiligheidsniveau wordt gewaarborgd ten opzichte van eindgebruikers (zowel patiënten als zorgverleners). Ontwikkeling en innovatie, en het trainen en testen van algoritmen horen hier eveneens bij. Bepaalde doeleinden zijn beperkt tot publieke instanties, of organisaties die in hun opdracht werken. Naast de toegelaten doelen, zijn er ook bepaalde verwerkingen voor secundair gebruik die verboden zijn (art. 54), met name onder meer besluiten op basis van elektronische gezondheidsgegevens die nadelig kunnen zijn voor de betrokken natuurlijke personen, discriminatie op basis van deze gegevens of nadelige voorwaarden/uitsluiting van verzekeringen, reclame of marketingactiviteiten, ontwikkelen van schadelijke producten, of activiteiten in strijd met ethische bepalingen vastgelegd in nationaal recht.

In Afdeling 2 wordt verder ingegaan op de **governance** van het secundair gebruik van gezondheidsgegevens. Hier worden voornamelijk specifieke taken bij de lidstaten gelegd, die instanties dienen in te richten die verantwoordelijk zijn voor de toegang tot gezondheidsgegevens (HDAB’s, of de ondersteunende Health Data Access Bodies), de instanties mogen geen belangenconflicten hebben met mogelijk andere taken die ze vervullen. Er kunnen per lidstaat meerdere instanties worden ingericht, en overkoepelend stemmen deze af met elkaar en de Europese Commissie. Indien er raakpunten zijn met kwesties van gegevensbescherming, stemmen ze ook af met die bevoegde autoriteiten. Nationaal recht kan een voorwaarde voorzien om in een ethische instantie te voorzien, in dat geval stellen de HDAB’s deskundigen ter beschikking. Daarnaast dienen de HDAB’s af te stemmen met vertegenwoordigers van belanghebbenden, met name de patiënten, de houders en gebruikers van gezondheidsgegevens. De Commissie voert in sommige situaties ook zelf de

[23] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_nl#wat-is-de-tijdlijn-voor-de-uitvoering-van-de-ehds-verordening

taken uit van de bevoegde instanties, in het geval de gegevenshouders instellingen van de Europese Unie zijn. Art. 57-59 omschrijft de verplichtingen en taken van deze instanties, die voornamelijk de toegang en verwerking tot toegang van deze gegevens betreft. Voor een veilige verwerking van elektronische gezondheidsgegevens dient er een beveiligde verwerkingsomgeving te worden voorzien (overweging 77). Verantwoordelijken hiervoor zijn ofwel de bevoegde instanties ofwel een betrouwbare houder van gezondheidsgegevens. Deze laatsten zijn datahouders die kunnen aantonen dat ze een beveiligde verwerkingsomgeving kunnen voorzien, de nodige expertise hebben om toegangsaanvragen te beoordelen en de nodige garanties kunnen bieden dat deze verordening wordt nageleefd (art. 72).

Als we kijken naar de **soorten gegevens** die relevant zijn voor verwerking voor secundair gebruik, zien we dat deze zeer ruim omschreven worden (art. 51). De reden is dat om tot waardevolle inzichten te komen rond gezondheid, zeker in het algemeen belang, het noodzakelijk is om verschillende facetten van gezondheid mee te nemen (overwegingen 53-55 en 56). Wel wordt meegegeven dat het ondanks de ruime interpretatie, wel steeds dient te gaan om gegevens waarvan geweten is dat ze een invloed hebben op de gezondheid. Daarnaast kunnen bestaande datasets verder wel verrijkt en aangevuld worden (overweging 57). Ondanks de ruime categorieën van gegevens, is er wel weer aandacht voor dataminimalisatie, en dat er voor secundair gebruik ook enkel toegang wordt gegeven naar de strikt noodzakelijke gegevens (overweging 72 en art. 66), en dat er verder voldoende gebruik wordt gemaakt van anonimisatie als het kan en pseudonimisatie als het gaat om een onderzoeksvraag.

Belangrijk om te komen tot waardevol secundair gebruik van gezondheidsgegevens is dat er voldoende kwalitatieve datasets zijn, en dat ook voldoende is gedocumenteerd waaruit een dataset bestaat (overweging 58 en Afdeling 5). Een **datakwaliteit**slabel kan door de datahouders voorzien worden, en is verplicht voor datasets die met steun van de Unie of nationale overheidsfinanciering werden verzameld of verwerkt. Hiervoor wordt het quantum health data quality label[24] ontwikkeld.

Wat betreft de **rechten van de betrokkenen** zijn er wat betreft secundair gebruik minder randvoorwaarden. Dit wordt aangegeven als een afweging tussen de noodzaak naar zo volledig en kwalitatief mogelijke datasets enerzijds, en de behoefte aan autonomie van personen over hun gezondheidsgegevens anderzijds. Vandaar wordt er wel voorzien in een opt-out mechanisme. Anders dan bij primair gebruik, waar de opt-out vrij te organiseren was door de lidstaten, dient het opt-out mechanisme voor secundair gebruik wel voorzien te worden (art. 71). Dit dient eenvoudig en toegankelijk te zijn, en personen dienen duidelijk geïnformeerd te worden over dit recht, met de voor- en nadelen. Dit recht is bovendien omkeerbaar, en hoeft niet nader verantwoord te worden. Er zijn uitzonderingen mogelijk op dit recht, lidstatelijk te bepalen én te verantwoorden (overweging 54).

Er is wel aandacht in de EHDS rond de noodzaak voor het verhogen van de digitale en gezondheidsgeletterdheid (overweging 89 en art. 83 en 84), zowel voor zorgverleners of medewerkers in de zorgsector als voor burgers en patiënten, een taak die expliciet bij de lidstaten wordt gelegd.

Ook bij secundair gebruik komen **wellnessapps** en medische hulpmiddelen aan bod. Zij worden eveneens beschouwd als mogelijke datahouders (overweging 56 en 59), met de verplichtingen die daarbij horen (art. 60) rond toegang tot data geven, het omschrijven van de dataset, enz. Wel zijn er uitzonderingen voor natuurlijke personen of micro-ondernemingen, die zijn vrijgesteld van de verplichtingen voor datahouders, dit is dus ook van toepassing op wellnessapps. Indien wellnessapps gebruik willen maken van elektronische gezondheidsgegevens voor secundair gebruik, dienen ze te voldoen aan de verplichtingen voor datahouders (art. 61).

2.2.4.4 Data-altruïsme

De EHDS vult het DGA-kader voor data-altruïsme aan, met name wat betreft de veiligheidseisen (art. 78). Wanneer erkende data-altruïsmeorganisaties (onder DGA) persoonlijke elektronische gezondheidsgegevens verwerken via een beveiligde verwerkingsomgeving (Secure Processing Environment, SPE) moet die omgeving voldoen aan de strenge

[24] https://quantumproject.eu/

beveiligings- en technische maatregelen van de EHDS. Zorggegevensinstanties moeten samenwerken met de bevoegde autoriteiten die toezicht houden op data-altruïsmeorganisaties (art. 78).

2.2.4.5 Trusted Health Data Holders (THDH)

Trusted Health Data Holders (THDH's) zijn een concept binnen het kader van het secundaire gebruik (Hoofdstuk IV) van de European Health Data Space (EHDS). Het primaire doel van het aanwijzen van THDH's is het verlichten van de administratieve last voor HDAB's bij het behandelen van aanvragen voor gegevenstoegang. Lidstaten mogen zorggevenshouders aanwijzen als THDH's, mits zij voldoen aan specifieke voorwaarden. Deze voorwaarden zijn dat zij:

- Toegang tot gezondheidsgegevens kunnen bieden via een beveiligde verwerkingsomgeving (Secure Processing Environment - SPE) die voldoet aan de vereisten van Artikel 73.
- De nodige deskundigheid bezitten om aanvragen voor gegevenstoegang te beoordelen.
- De noodzakelijke garanties bieden om de naleving van de EHDS-verordening te verzekeren.

Wanneer een aanvraag voor gegevenstoegang uitsluitend gegevens omvat die in bezit zijn van een aangewezen THDH, wordt een vereenvoudigde procedure toegepast. Binnen deze vereenvoudigde procedure beoordeelt de THDH de aanvraag op basis van de gestelde criteria en dient een aanbeveling in bij de HDAB over het verlenen of weigeren van een datavergunning. De HDAB behoudt te allen tijde de verantwoordelijkheid voor het verlenen van de definitieve datavergunning en is niet gebonden aan de aanbeveling van de THDH. THDH's worden vermeld in de datasetcatalogus van de HDAB's.

2.2.4.6 Health data intermediation entities (HDIE)

De rol van een *health data intermediation entity* (HDIE) is specifiek gericht op het verminderen van de administratieve last voor bepaalde categorieën gegevenshouders bij het beschikbaar stellen van elektronische gezondheidsgegevens voor **secundair gebruik**. Een HDIE is een rechtspersoon die door lidstaten in hun nationale wetgeving kan worden aangewezen om de plichten van deze gegevenshouders te vervullen, waaronder het verwerken, registreren, beschikbaar stellen, de toegang beperken tot, en het uitwisselen van elektronische gezondheidsgegevens voor dit secundaire doel (overweging 59 en art. 50.3). Het is cruciaal dat, zelfs wanneer gegevens via een HDIE worden geleverd, deze **niettemin worden beschouwd als afkomstig van verschillende gegevenshouders**; HDIE's mogen hierdoor niet worden aangewezen als vertrouwde gezondheidsgegevenshouders (*trusted health data holders*) en de gegevens moeten altijd het **normale aanvraagproces** bij de Health Data Access Body (HDAB) doorlopen (overweging 76). Deze entiteiten voeren taken uit die verschillen van die van de data-intermediatiediensten zoals gedefinieerd in de Data Governance Act (DGA) (overweging 59).

2.2.5 Gap analyse en conclusies

Als we de Europese regelgeving bekijken, waar de AVG een startpunt en nog steeds referentie is als het gaat over persoonsgegevens, is er sterke aandacht voor de bescherming van deze gegevens, het is zelfs een Europees grondrecht. Ondanks dat de regelgeving niet alle problemen rond misbruik van persoonsgegevens heeft opgelost, heeft ze wel voor belangrijke evoluties gezorgd op dit vlak, met de eerste grote rechtszaken tegen misbruik door grote techspelers, en een sterker bewustzijn rond privacy en bescherming van persoonsgegevens. Daartegenover staat dat, hoewel er wettelijk telkens opties worden aangeboden om klacht in te dienen en informatie op te vragen, er nog veel van de betrokkene zelf wordt verwacht. Er zijn rechten, maar het uitoefenen van die rechten wordt niet echt gefaciliteerd. Verder spreekt de AVG zich maar beperkt uit over verdere verwerking van persoonsgegevens, voornamelijk rond de noodzaak van verenigbare doelen. Maar wat als je als persoon zelf gegevens wil gaan delen? Daar doet de AVG geen uitspraken over. Dit aspect, met de focus op bescherming van rechten, en minder op het makkelijk uitoefenen van die rechten, wordt ook aangekaart door bewegingen als MyData (zie ook 3.1.1).

De nieuwe regelgevingen die kaderen in de Europese datastrategie, de Data Act en Data Governance Act, houden al meer rekening met die beperking van de AVG. Zo verduidelijkt en concretiseert de Data Act het dataportabiliteitsrecht uit de AVG en de informatieplicht rond de verzamelde gegevens uit IoT-diensten. Het stelt ook uitdrukkelijk dat de gebruikers van deze diensten evenveel rechten hebben om te genieten van toegang tot de data en voordeel te

ondervinden die deze data kunnen leveren. Anderzijds worden de gebruikers van de producten die onder de Data Act gedefinieerd als personen die eigenaar zijn van het toestel, of er tijdelijke rechten op hebben gekregen. In veel gevallen zullen bij IoT-toestellen de eigenaars ook wel de gebruikers zijn waarover data worden gegenereerd, maar in een zorgcontext kan het toch wat complexer worden. Veel telemonitoring toestellen worden immers via het ziekenhuis uitgeleend aan hun patiënten. De eigenaar van het toestel is in dat geval dus niet de persoon waarover data wordt verzameld. Misschien valt de patiënt dan onder de definitie van een persoon die tijdelijke rechten heeft toegekend gekregen, maar in veel situaties zal dit niet duidelijk omschreven zijn, en de definitie en interpretatie van de Data Act is daar dan ook niet eenduidig in. Vraag is of het ietwat meer uitgebreide dataportabiliteitsprincipe van de Data Act ook gebruikt kan worden door personen die een toestel van een ziekenhuis, zorginstelling of zorgverlener, en indien niet, of de bijkomende rechten van patiënten rond hun gezondheidsdata deze manco voldoende dekt. In de situaties waar gebruikers toegang kunnen krijgen tot hun data volgens de bepalingen van de Data Act, benadrukt de Data Act bijkomend nog dat producten en diensten dienen ontworpen te worden zodat toegang tot de data gemakkelijk en toegankelijk is voor de gebruikers, en in een gemakkelijk bruikbaar dataformaat. Waar data niet onmiddellijk beschikbaar is, wordt deze eenvoudig beschikbaar gemaakt op verzoek van de gebruiker. Hier ligt ook wel een mogelijk pijnpunt van de Data Act: het zal in veel situaties weer een actieve stap vragen van de gebruiker, wat een mogelijke drempel kan zijn, ondanks de pleidooien, waaronder in de Data Act, om data geletterdheid te gaan verhogen.

In dat opzicht biedt de Data Governance Act bijkomende ondersteuning aan personen rond het gebruik en toegang tot hun data, met het definiëren van databemiddelingsdiensten (data deling bevorderen), data coöperaties (uitoefenen van rechten ondersteunen, onder meer geven van toestemming) en data altruïsme via bevoegde organisaties. Hier zien we wel de moeilijkheid dat een dataruimte een groeiend concept is, momenteel nog sterk gericht op industriële data, en met een nog ontwikkelend economisch model. De registers van databemiddelingsdiensten en data altruïsme organisaties bevatten nog maar weinig organisaties, en deze zijn ook nog niet erg bekend. Een deel van de verklaring kan liggen in het laat vastleggen door afzonderlijke lidstaten van de bevoegde instanties om de labels uit te vaardigen, maar daarnaast is het omwille van bovengenoemde redenen (dataruimte als nieuw concept, focus op industriedata, nog geen grote volumes van (persoonlijke) data) nog geen evidentie voor deze diensten om een werkbaar verdienmodel op te zetten. Pas als er voldoende volume van data in een dataruimte circuleert, zouden deze diensten kunnen gaan renderen, naast het uitbouwen van duidelijke use cases die de meerwaarde aantonen en de herkenbaarheid van deze diensten bij het grote publiek bevorderen.

De EHDS bouwt verder op al deze regelgevingen en verduidelijkt wat meer specifieke spelregels voor elektronische gezondheidsdata. De EHDS verwijst regelmatig op de complementariteit of uitbreiden op rechten in de AVG, anderzijds zijn de verwijzingen naar de Data Act en Data Governance Act (DGA) veel beperkter, hoewel deze als overkoepelende regelgeving gelden over dataruimtes heen. Neem bijvoorbeeld de DGA en de concepten van databemiddelingsdiensten. Deze worden eigenlijk niet vermeld in de EHDS, enkel om aan te geven dat de HDIE's niet dezelfde taken vervullen als de databemiddelingsdiensten uit de DGA. De mate waarin deze beide diensten van elkaar verschillen, wordt niet verduidelijkt. De enige duidelijk link met de DGA is een verwijzing naar data altruïsme, maar dit is niet hetzelfde als een databemiddelingsdienst. Toegang tot elektronische gezondheidsgegevens voor secundair gebruik zijn volledig vastgelegd in de EHDS en zullen door bevoegde instanties (HDAB's) worden opgevolgd. Een andere rol die binnen de EHDS wordt genoemd is de Trusted Health Data Holders (THDH) een entiteit die vergaande bevoegdheden heeft voor het beschikbaar stellen van gezondheidsdata. De THDH is nadrukkelijk in het leven geroepen om HDAB's te ontlasten. De mate waarin HDAB's gelijkenissen of verschillen vertonen met databemiddelingsdiensten wordt niet duidelijk gesteld, maar kan een interessante insteek opleveren om deze rollen te gaan vergelijken, en te bekijken of een HDAB of een THDH als een soort databemiddelingsdienst kan beschouwd worden. De EHDS stelt expliciet dat een THDH niet een THIE kan zijn, maar geeft anderzijds aan dat een THIE niet hetzelfde is als een databemiddelingsdienst. De vraag of een THDH dan wel een databemiddelingsdienst kan zijn, wordt niet beantwoord.

De EHDS is ook expliciet in welke organisaties niet verplicht zijn om gezondheidsdata ter beschikking te stellen. Micro-ondernemingen, die worden gedefinieerd als organisaties die minder dan 10 personen in dienst hebben en waarvan de jaaromzet niet meer dan 2 miljoen euro bedraagt. Voor deze organisaties, en mogelijke andere datahouders, voorziet de EHDS THIE's om hen te ondersteunen toch data voor secundair te ontsluiten. De THIE's worden wel expliciet onderscheiden van de databemiddelingsdiensten onder de DGA. De mate waarin deze THIE's verschillen van databemiddelingsdiensten wordt echter niet in detail gespecifieerd.

In de context van primair gebruik, zeker als het gaat over gezondheidsgegevens die buiten de EPD's en het primaire doel van gezondheidszorg vallen onder de definitie in EHDS, is het misschien wel mogelijk om de databemiddelings-diensten en data coöperaties een rol te laten spelen volgens de DGA definitie, zoals bijvoorbeeld in het geval van preventie via zelfmanagement door wellnessapps, omdat de EHDS zich er niet expliciet over uitspreekt en enkel regels oplegt aan deze apps indien er connectie wordt gemaakt met het EPD. Het is wel mogelijk dat nationale regelgeving rond dit soort apps wordt ingericht, waardoor de positie van de databemiddelingsdiensten en de rol van wellnessapps mogelijk verder wordt gecompliceerd.

Het ontbreken van duidelijkheid over de context van preventie en gezond leven is geen evidentie. EHDS definieert prioritaire categorieën van gezondheidsgegevens, maar levensstijl, welzijn en preventie worden hier niet genoemd, hoewel levensstijl een grote impact heeft op het ontwikkelen van chronische ziektes en deze (nog) niet systematisch worden gecapteerd worden in EPD's. Door de stijgende vergrijzing en stijging in chronische ziektes die vaak in combinatie voorkomen, is er een sterke druk op het gezondheidssysteem. Om dit op lange termijn werkbaar en betaalbaar te houden, is een shift in het gezondheidssysteem nodig van het puur curatieve naar preventie. Desondanks beschouwt de EHDS de wellnessapps en de info die ze verzamelen rond welzijn en levensstijl (nog) niet als belangrijke informatie voor het gezondheidssysteem.

Daarentegen zien we wel dat er over de verschillende regelgevingen heen, meer en meer aandacht is voor datakwaliteit, voldoende informatie over data en interoperabiliteit tussen systemen, en de creatie van labels en certificeringen in verschillende contexten (medische hulpmiddelen, wellnessapps, EPD-systemen en datakwaliteit). Deze richtlijnen opvolgen in de context van preventie kan het mogelijk maken dat dit soort data in een latere fase meer kunnen worden geïntegreerd in de systemen zoals MyHealth@EU en HealthData@EU.

Om te concluderen, als we kijken naar handvaten om mensen actief te laten meewerken aan hun gezondheid, zien we vanuit de regelgeving volgende vaststellingen en open vragen:

- Er zijn steeds meer rechten en stilaan ook wat meer manieren om geholpen te worden deze rechten ook uit te oefenen. Wel is het van belang dat er voldoende incentives zijn voor betrouwbare databemiddelingsdiensten en andere ondersteunende systemen.
- Als het gaat om gezondheidszorg in primaire zin onder EHDS hebben personen veel zeggenschap in wie hun gegevens wel en niet mogen zien. Verder is er de kans om gegevens toe te voegen en te (laten) corrigeren. Er wordt toegang voorzien tot de data via portalen. Deze zijn wel in eerste instantie gericht op de prioritaire categorieën van elektronische gezondheidsgegevens aangeleverd vanuit de EPD's, en preventieve gegevens of gegevens door een persoon gegenereerd via een wellnessapp of andere toepassing vallen hier (nog) niet onder. De open vraag blijft of er naast het wettelijk kader complementaire methodes te vinden zijn die deze werelden toch meer kunnen gaan verbinden.
- Na lange discussies rond de rol van toestemming in de EHDS, is er gekozen voor een opt-out mechanisme. Er is een beschikbaar voor primair en secundair gebruik. Daarnaast wordt er een rapporteringsplicht opgelegd, en is er aandacht voor data en gezondheidsgeletterdheid, maar is dit voldoende om de betrokkenheid van personen over de meerwaarde van secundair gebruik te gaan verhogen, en het vertrouwen rond secundair gebruik op te bouwen?
- Er is de laatste jaren meer aandacht voor de ondersteuning van personen in het uitvoeren van hun rechten. Wat betreft primair gebruik kan een persoon iemand aanstellen om mee zijn rechten te gaan opvolgen, en voor het delen van gegevens of het uitoefenen van rechten zijn er de databemiddelingsdiensten in de DGA. Dit kan best nog verder getrokken worden, en dat er in het kader van gezondheids- en datageletterdheid ook voldoende aandacht is voor de verschillende manieren waarop er op een proactieve manier steun kan geboden worden aan personen. Een voorbeeld kan zijn de datacoöperaties die in naam van de betrokkenen toestemming kunnen regelen: dit neemt de last weg van de personen om dit zelf te gaan opvolgen, en de problemen rond consent die daaraan gekoppeld zijn (zie ook 3.2.4).

3. Naar een grensoverschrijdend burgergedreven governancemodel

3.1 Databemiddelaars als middel voor democratisch beheer van data

Er zijn verschillende redenen waarom burgers meer zeggenschap over gezondheidsdata zouden moeten krijgen. Burgers en patiënten hebben in tegenstelling tot ziekenhuizen, huisartsen en wellnessapps toegang tot verschillende databronnen. WellData faciliteert dat de burger deze toegang op één plek kan organiseren. Gecombineerde data van meerdere burgers of patiënten zou in theorie ook een grotere waarden hebben. Dergelijke data kunnen bijdragen aan het **lerend zorgsysteem**, in het geval van WellData ook grensoverschrijdend. Een andere reden is dat burgers tegenmacht kunnen organiseren richting tech-bedrijven en instituties, en de scheefgetrokken machtsverhouding meer in balans kunnen brengen. Als laatste reden kunnen burgers door het doneren van gezondheidsdata meer betrokken worden bij onderzoek en het maken van gezondheidsbeleid[25].

3.1.1 Collectief databeheer d.m.v. data commons / databemiddelaars

Waar de DGA een formele definitie geeft van databemiddelingsdiensten en waaraan die volgens de regelgeving dienen te voldoen om erkend te worden, bestaat het concept van databemiddelaars al langer. Databemiddelaars of data commons zijn een middel om data collectief te beheren. Een databemiddelaar regelt bijvoorbeeld wie data kunnen benaderen en wie data kunnen en mogen gebruiken. Met andere woorden, data commons zijn digitale gegevens die collectief beheerd en bestuurd worden door een gemeenschap. Gemeenschappelijk beheer van data kan op verschillende manieren worden georganiseerd. Alek Tarkowski en Jan J. Zygmuntowski beschrijven verschillende vormen van data commons[26]. In Tabel 1 is een opsomming te zien van de verschillende vormen. Dit varieert van Open Access Commons waar datasets met behulp van een Creative Commons-licentie bruikbaar is. Hier wordt datagebruik over het algemeen niet actief gemonitord. De datacoöperatie is een organisatievorm waarbij de leden van de coöperatie digitale gegevens samen beheren terwijl in data trusts het beheer van data wordt toevertrouwd aan geautoriseerde beheerders die zelfstandig beslissingen over het beheer van data mogen nemen.

Open access commons	The least restricted repositories of easily shareable sets of data, where monitoring access is not necessary.
Data collaboratives	Voluntary public-private agreements to share data to achieve synergies along the lines of ‘data for good’.
Data cooperatives	Grassroots initiatives employing the democratic model of cooperativism and social entrepreneurship to govern data of its members.
Public data commons	Institutions such as agencies, banks and trusts established to provide systemic solution of data governance in the public interest.
Data trusts	Authorized third-party managers of data, bound by fiduciary obligations to act in the best of interest of beneficiaries.
Data unions	Collective bargaining institutions, distributing revenue for members and assisting them in data strike actions.
Common data spaces & Data access bodies	Connecting sectoral, interoperable frameworks of standards with designated authorities (as seen in the European Health Data Space proposal).

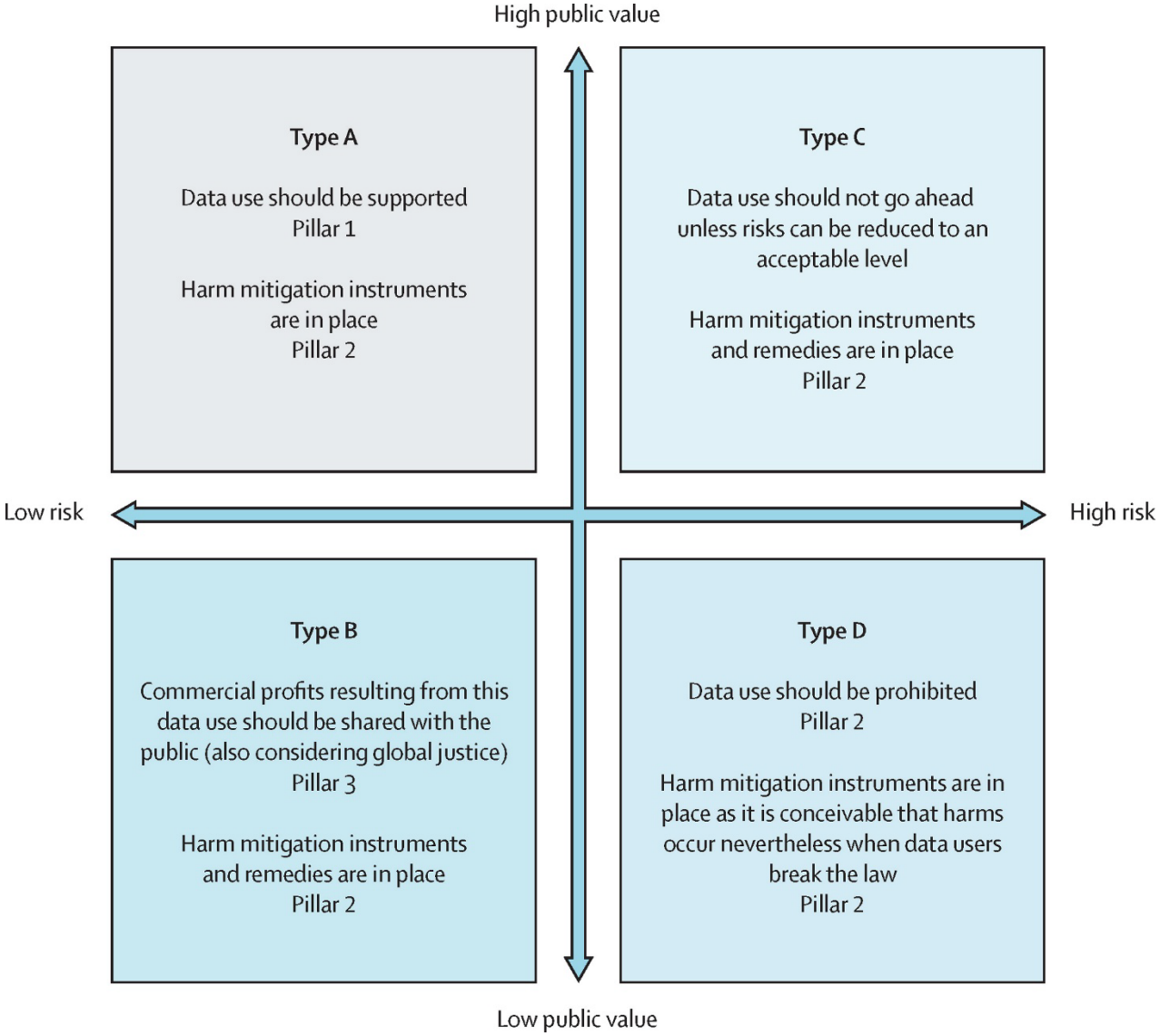
Tabel 1. Verschillende varianten van Data Commons - uit 'Data Commons Primer'.

[25] https://www.icthealth.nl/magazine/editie-03-2021/gegevens-als-brandstof-voor-gezondheidsonderzoek-en-innovatie

[26] https://openfuture.eu/wp-content/uploads/2022/07/220723data-commons-primer.pdf

3.1.2 Publieke waarde van gezondheidsdata

Barbara Prainsack noemt in een aantal artikelen[27,28,29] over data op solidariteit gebaseerde governance dat de aard van de data belangrijk zijn om een beslissing te maken op welke manier data worden beheerd. In Figuur 3 worden langs de as van laag tot hoog risico datasets en lage tot hoge publieke waardevolle data vier kwadranten geplot. Afhankelijk van het risico en de publieke waarde kunnen geschikte maatregelen in de governance worden opgenomen.



Figuur 3. Matrix voor de risicomitigatie voor het hergebruik van gezondheidsdata. Gezondheidsdata worden in vier types verdeeld aan de hand van het risico voor hergebruik van gezondheidsdata en de publieke waarde van deze data.

[27] https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00189-3/fulltext

[28] https://pubmed.ncbi.nlm.nih.gov/39313256/

[29] https://pubmed.ncbi.nlm.nih.gov/39789994/

3.2 Voorbeelden van burgergedreven governancemodellen

3.2.1 MyData

MyData[30] is een internationale non-profit organisatie die vertrekt vanuit de overtuiging dat het beheer van persoonsgegevens fundamenteel moet worden herzien in functie van individuele autonomie, transparantie en maatschappelijk verantwoord gebruik. MyData schuift zowel een normatief kader als een beleidsvisie naar voren die burgers zelf zeggenschap geeft over de verwerking en het gebruik van hun persoonlijke gegevens. In tegenstelling tot de huidige dominante praktijk, waarbij data voornamelijk worden verzameld en beheerd door private of publieke instellingen met beperkte inspraak van de betrokken datasubjecten, bepleit MyData een governancebenadering die vertrekt vanuit data met mensen, in plaats van data over mensen. Burgers dienen toegang te hebben tot hun gegevens, te kunnen bepalen wie toegang krijgt, voor welk doel en onder welke voorwaarden, en moeten ondersteund worden om hierin geïnformeerde keuzes te maken. Binnen dit kader krijgen burgers ook een structurele rol in de governance-structuur van dataplatformen. Dit kan onder meer via representatieve organen zoals gebruikersraden, participatieve besluitvormingsmechanismen, of via transparante auditstructuren die toezien op het datagebruik. Burgers worden zo niet enkel beschouwd als individuele datasubjecten, maar als collectieve stakeholders met rechten en verantwoordelijkheden binnen het bredere datasysteem.

De fundamentele waarden die MyData richting geven zijn menselijke waardigheid, keuzevrijheid, inclusie, rechtvaardigheid en wederzijdse verantwoording. Deze waarden worden niet alleen ethisch geformuleerd, maar ook vertaald naar concrete structurele vereisten voor systemen en processen. Zo moeten burgers ondersteund worden door begrijpelijke communicatie, toegankelijke technologie, en waar nodig betrouwbare tussenpersonen. MyData pleit tot slot voor een evenwicht tussen individuele datacontrole en maatschappelijk belang. Het delen van gegevens moet in die zin geen verplichting zijn, maar wel worden aangemoedigd via duidelijke garanties over privacybescherming en publieke meerwaarde. Eén van de kernelementen van MyData gaat met name over wat ze ‘actionable rights’ noemen. Dit wordt tegenover de GDPR-rechten geplaatst, die waardevol zijn, maar passief door mensen wordt ondergaan en sterk gericht zijn op bescherming. MyData wil een shift realiseren door mensen centraal te stellen in datadeling, en een kader creëren waar de ethische keuze ook een economisch zinvolle keuze is. Het model streeft zo naar een duurzame datasamenleving, waarin het gebruik van persoonsgegevens gebeurt binnen een kader van wederzijds vertrouwen, transparantie en collectieve verantwoordelijkheid. MyData is dus geen operationeel platform maar eerder een internationaal netwerk van individuen en organisaties die dit normatief kader onderschrijven en actief uitdragen.

Daarnaast zijn er ook ‘MyData operators’[31], organisaties en bedrijven (profit of non-profit), die de MyData principes onderschrijven en die werken aan het interoperabel maken van systemen die het delen van persoonlijke data mogelijk maken, om op termijn te komen tot een persoon-centrische persoonlijke data-infrastructuur. De kernelementen van MyData operators draaien rond identiteitsmanagement, toestemmingsmanagement, dienstmanagement, waardeuitwisseling, data model management, persoonlijke datatransfer, en persoonlijke dataopslag. Niet elk element is noodzakelijk bij elke operator aanwezig, maar het gaat over gemeenschappelijke, veel voorkomende functionaliteiten die de kern uitmaken van het MyData operator-model. MyData doet geen keuzes naar technische infrastructuur waarrond de MyData operators kunnen werken, maar stelt interoperabiliteitsvereisten. Daarnaast is er ook een overkoepelend governancekader, aangezien de operatoren niet in isolatie werken, maar zich in een groter ecosysteem bevinden. Daarom interageren de MyData operatoren met zowel het legale kader als de bredere maatschappelijke en economische context. Enkel het legale kader zal niet volstaan om vertrouwen te gaan creëren, en het governance framework legt de rollen en verantwoordelijkheden vast om de machtsbalans in het datadelingssysteem te gaan herstellen. Binnen MyData is er nog geen vastgelegd governance kader uitgewerkt, ze benadrukken vooral het opvolgen van de MyData principes, en de verschillende verantwoordelijkheden die operatoren hebben ten opzichte van personen afhankelijk van hun interacties met mensen (direct of indirect, publiek of privé, collectief of individueel). Recent bracht MyData naar

[30] https://mydata.org/

[31] https://mydata.org/wp-content/uploads/2020/04/Understanding-Mydata-Operators.pdf

aanleiding van hun 10-jarig bestaan een nieuwe white paper[32] uit met reflecties over de recente evoluties in AI en geautomatiseerde beslissingen, de plaats van de rechten die mensen hierin hebben, het risico dat technologie totalitaire regimes ondersteunt, en de balans tussen privacy en gemeenschappelijk belang. Ze tonen aan dat de MyData principes actueel blijven in het kader van de nieuwe legale, technologische en maatschappelijke ontwikkelingen, maar dat er implementatiedrempels zijn om dit te gaan realiseren. Een reflectieoefening over het versterken van MyData, de principes en de meerwaarde is opgestart om deze uitdagingen verder aan te gaan.

3.2.2 MIDATA

MIDATA[33] is een praktijkvoorbeeld van burgergerichte datagovernance dat vertrekt vanuit het principe dat gezondheidsdata niet enkel persoonlijke eigendom zijn, maar ook collectieve waarde kunnen genereren. Het model werd in Zwitserland ontwikkeld en vormt een coöperatieve structuur waarin burgers actief deelnemen aan het beheer van hun eigen gezondheidsdata, en meebepalen hoe en onder welke voorwaarden deze data gedeeld worden voor onderzoek en innovatie. In de MIDATA-structuur kunnen burgers zich aansluiten als lid van de coöperatie. Zij behouden het individuele beslissingsrecht over hun persoonlijke gegevens, maar engageren zich tegelijkertijd om collectief te waken over het ethische gebruik ervan. De coöperatie fungeert als vertrouwensorganisatie die instaat voor het platformbeheer, dataveiligheid, ondersteuning van leden, en de onderhandelingen met externe datagebruikers (zoals onderzoeksinstellingen of zorgaanbieders).

Een belangrijk kenmerk van het MIDATA-model is de nadruk op democratische controle. Leden van de coöperatie kunnen deelnemen aan de besluitvorming via stemrecht (waarbij elk lid van de coöperatie één stem kan uitbrengen), zetelen in bestuursorganen, en betrokken zijn bij een ethisch comité dat voorstellen tot datatoegang beoordeelt. Deze structuur garandeert dat de inzet van persoonlijke data steeds getoetst wordt aan gedeelde waarden, maatschappelijke relevantie en het respect voor individuele voorkeuren. MIDATA biedt burgers bovendien een beveiligde digitale infrastructuur (een “persoonlijke datakluis”) waarin zij hun gezondheidsdata centraal kunnen beheren. Dit verhoogt niet alleen de autonomie van het individu, maar maakt ook interoperabiliteit mogelijk tussen verschillende bronnen van gezondheidsdata, zoals ziekenhuizen, apps, wearables of onderzoeksinstellingen.

Het model sluit aan bij principes van solidariteit, maatschappelijke meerwaarde en data-ethiek. MIDATA ziet het delen van data niet als een louter transactioneel gegeven, maar als een vorm van datadonatie, waarbij burgers bijdragen aan het algemeen belang, bijvoorbeeld door innovatie te stimuleren of betere preventie. Tegelijkertijd wordt de vrijwillige aard van deelname benadrukt: leden behouden altijd de mogelijkheid om toegang te weigeren of in te trekken, en het gebruik van hun data wordt nooit gecommercialiseerd zonder hun expliciete toestemming.

Samengevat biedt MIDATA een kader waarin burgers zelf eigenaar en beheerder zijn van hun gezondheidsdata, democratisch meebeslissen over datagebruik en governance, en de maatschappelijke inzet van data ondersteunen, binnen duidelijke ethische en juridische kaders.

3.2.3 Gezond Akkoord

Gezond Akkoord[34] is afsprakenstelsel ontwikkelt door gezondheidsdatacoöperatie ‘mijn data onze gezondheid (MDOG)’ die tot doel heeft om burgers beter te beschermen als het komt op het delen van hun gegevens, en anderzijds een bijdrage kan leveren aan de gezondheidseconomie door verantwoord delen van gezondheidsgegevens. De coöperatie wil burgers ontzorgen in het omgaan met vragen tot het delen van hun data voor onderzoek. Om deze ontzorging mogelijk te maken, zijn er richtlijnen ontwikkeld rondom onder meer procedures voor de ethische toetsing van dataverzoeken. Verder kunnen leden van de coöperatie hun voorkeuren aangeven rond voorwaarden voor datadeling,

[32] https://mydata.org/wp-content/uploads/2025/05/MyData-in-Motion-Evolving-Empowerment-for-2025-and-beyond-layout-v4-1.pdf

[33] https://www.midata.coop/en/home/

[34] https://mdog.nl/wp-content/uploads/2021/11/1-GA-Position-paper-Gezond-AKKOORD.pdf

een vorm van consentprofiel (zie ook 3.2.4.2). Gezond Akkoord is een Nederlands initiatief, dat voortbouwt op de stijgende rechten van Nederlandse burgers rond toegang toe en zeggenschap over hun gezondheidsgegevens. In Nederland wordt dit specifiek vertaald in een zogenaamde Persoonlijke Gezondheidsomgeving (PGO). In een PGO kan een burger zijn verzamelde gezondheidsgegevens opslaan en delen met andere zorgverleners. Daarnaast kan de burger in veel PGO's hun data rond levensstijl en welzijn opslaan, en kunnen daarom een interessante bron zijn van gegevens voor onderzoek, maar dat hoort niet tot de doelstellingen van de PGO en is nog niet geborgd in het onderliggende afsprakenstelsel Medmij.

Via Gezond Akkoord wil men deze en ook andere gezondheidsgegevens beter gaan ontsluiten voor niet enkel primair maar ook secundair gebruik, en dit met aandacht voor de blijvende toegankelijkheid van zorg, de privacy van de burger, de zeggenschap van deze burger en het waarborgen dat dit niet gepaard gaat met nadelen voor de burger. Belangrijk hierin is ook de aandacht voor de rol van de burger in de data-economie en de dataruimten daarrond, waar een individu vaak in een zwakkere positie staat ten opzichte van de andere spelers in het ecosysteem. Van daaruit wordt het concept uitgewerkt om vanuit een coöperatie te gaan werken om burgers hierin te ondersteunen.

De coöperatie werkt rond een aantal kernwaarden:

1. Jij beheert de sleutel tot jouw data.
2. De leden van de coöperatie bepalen de koers van de coöperatie.
3. De coöperatie zorgt ervoor dat je alleen dataverzoeken ontvangt die bij je passen.
4. De coöperatie stimuleert een gezondheidseconomie: een economie die belang heeft bij jouw gezondheid in plaats van je ziekte.
5. De werkwijze van de coöperatie is controleerbaar en transparant.
6. De coöperatie controleert of alle dataverzoeken aan wettelijke en ethische eisen voldoen.

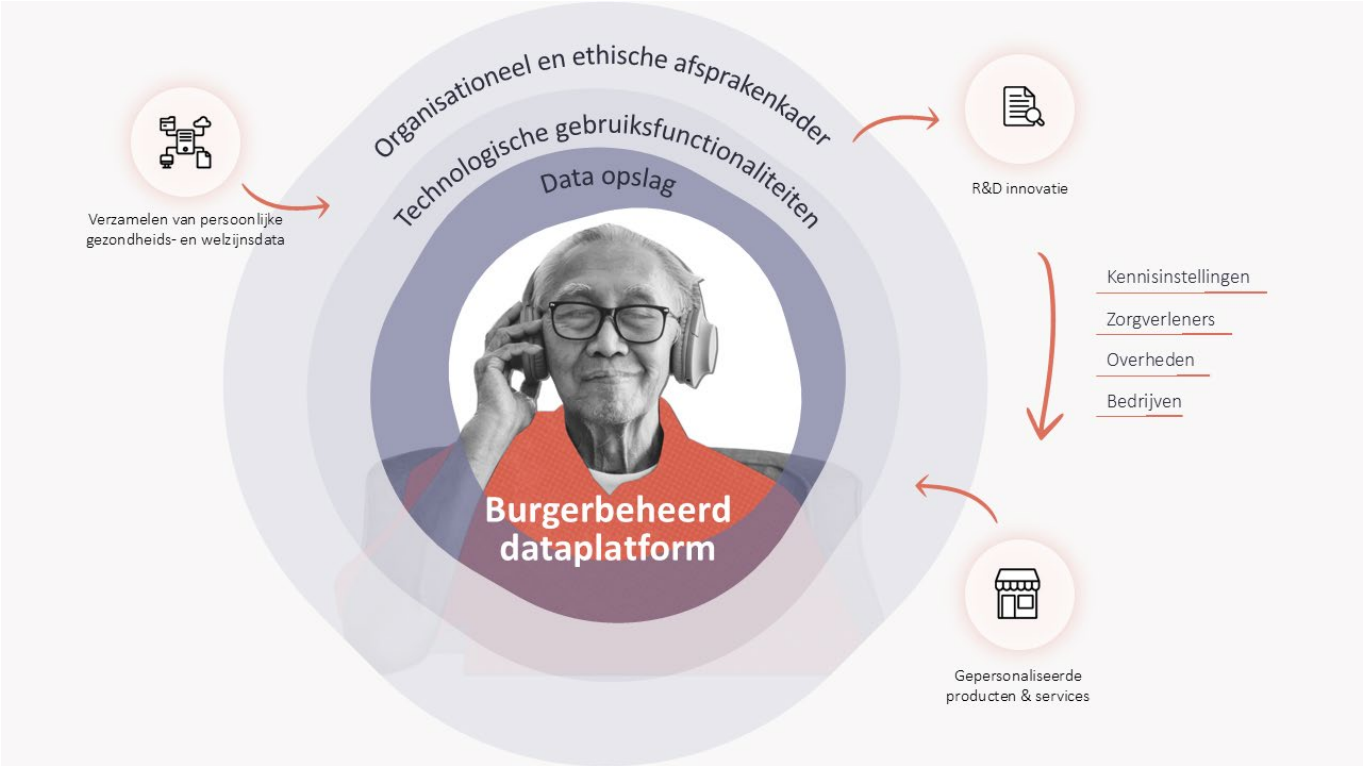
Daarnaast stelt de coöperatie met inspraak van de leden een aantal richtlijnen op om de praktische werking te regelen, onder meer over hoe lid te worden van de coöperatie, hoe een voorkeurenfilter op te stellen (om enkel dataverzoeken binnen het interessegebied te ontvangen) en het verlenen van toestemming, naast richtlijnen rond de werking van de Beoordelingscommissie Ethisch Datagebruik (toetsing AVG principes en aanvullende ethische principes opgesteld door de leden van de coöperatie) en het afhandelen van dataverzoeken.

Wat betreft de toestemmingen, werkt de coöperatie in eerste instantie met actieve toestemming van de leden. Wel wijst het op de onwenselijke effecten van te vaak toestemming vragen (zie ook 3.2.4.2), en de noodzaak om te kijken naar aspecten als consentprofielen en gedelegeerd consent. De coöperatie zorgt verder voor een overzicht van de verleende en openstaande toestemmingen.

3.2.4 We Are

We Are[35] is een innovatief data-ecosysteem dat tot doel heeft burgers terug aan het stuur te zetten van hun persoonlijke gezondheidsgegevens. Het project vertrekt vanuit het principe dat gezondheidsdata niet alleen correct beheerd en veilig opgeslagen moeten worden, maar ook ingezet kunnen worden om zowel individuele gezondheidsdoelstellingen als maatschappelijke meerwaarde te realiseren. Centraal in de visie van We Are staat het idee van zelfbeschikking in solidariteit. Burgers krijgen via een persoonlijke datapod de mogelijkheid om hun gezondheidsdata veilig op te slaan, te beheren en, indien gewenst, te delen met zorgverleners, overheden, onderzoekers of bedrijven. Die datadeling gebeurt op basis van transparante toestemmings-mechanismen en onder voorwaarden die door de burger zelf bepaald kunnen worden.

[35] https://we-are-health.be



Figuur 5. De verschillende lagen van het We Are-platform. Centraal staat een burgercentrale data-opslag, met daarrond een laag die zorgt dat de data in de persoonlijke datakluisjes kan ontsloten worden naar derde partijen. Een participatieve governancelaag zorgt voor ethische en legale screening, en worden burgers betrokken in het beheer van het platform.

Maar We Are gaat verder dan individuele zeggenschap geven aan de burger. Het project kiest bewust voor een governancebenadering waarin burgers ook collectief betrokken zijn bij het bestuur van het ecosysteem. Zo wordt gewerkt aan een ethisch comité dat volledig uit burgers zal bestaan (mogelijks met ondersteuning van experts op specifieke gezondheidstoepassingen) en dat zal bepalen welke toepassingen toegang zullen krijgen tot het We Are ecosysteem. Ook het bepalen van wat als “algemeen belang” geldt in datagebruik, wordt niet opgelegd, maar in dialoog met burgers afgetoetst.

De governancestructuur van We Are is ontworpen op basis van vier kernprincipes:

- Zelfbeschikking en solidariteit – burgers kiezen wat met hun data gebeurt, maar worden ook uitgenodigd om bij te dragen aan maatschappelijke doelstellingen.
- Kwaliteit en efficiëntie – het platform streeft naar een optimale integratie van betrouwbare gezondheidsdata, gebaseerd op FAIR-principes.
- Zorgzaamheid en gelijkwaardigheid – digitale en gezondheidsvaardigheden worden actief ondersteund, met bijzondere aandacht voor kwetsbare groepen.
- Privacy en veiligheid – er wordt strikt voldaan aan wetgeving zoals de GDPR en de Data Governance Act, en databeveiliging is fundamenteel ingebed in het ontwerp.

Burgers worden in deze context niet alleen beschouwd als dataleveranciers, maar als co-eigenaars van een collectieve infrastructuur. De governance is daarom opgevat als een gedeeld sturingsmodel waarin verschillende stakeholders (waaronder zorgorganisaties, overheden, technologiepartners en burgers) samenwerken op basis van gelijkwaardigheid en gedeelde waarden. Door in te zetten op participatief beleid, transparantie, en ethische toetsing van datagebruik, wil We Are bijdragen aan een vertrouwensvol en inclusief datalandschap. Niet via marktlogica of top-down regulering, maar via een maatschappelijk contract waarin burgers mee vorm geven aan de regels die gelden voor het gebruik van hun meest persoonlijke gegevens.

3.3 De burger en zijn (gezondheids)data

3.3.1 Visies op datadeling

Hoewel wetgevingen zoals de AVG en de EHDS inzetten op het versterken van burgerrechten en het bevorderen van datadeling ten behoeve van onderzoek en innovatie, blijkt uit onderzoek dat veel burgers onvoldoende bewust zijn van het feit dat hun gezondheidsdata worden verzameld, opgeslagen en secundair gebruikt (Aitken et al., 2016; Skovgaard et al., 2019; Stockdale et al., 2019; Simpson et al., 2021). Er bestaat dus een discrepantie tussen het beleidsmatige discours over datageletterde, actieve burgers en de realiteit waarin burgers vaak onvoldoende bewust zijn over hoe en waarvoor hun data wordt ingezet.

Onderzoek toont aan dat wanneer burgers voldoende geïnformeerd zijn, zij een positieve attitude hebben ten aanzien van het delen van gezondheidsdata, op voorwaarde dat het gebruik kadert binnen het publieke belang (Aitken et al., 2016; Howe et al., 2018). De bereidheid tot datadeling wordt daarbij sterk beïnvloed door het doel van gebruik. Burgers maken een duidelijk onderscheid tussen datagebruik voor publieke doeleinden, zoals wetenschappelijk onderzoek of beleid, en het gebruik door commerciële partijen, waarvoor aanzienlijk meer terughoudendheid bestaat (Hutchings et al., 2020; Street et al., 2022; Kassam et al., 2023).

Het idee van “publiek belang” kan in dit verband gezien worden als een legitimatiegrond voor datadeling. Hoewel het begrip vaak vaag blijft, vormt het voor veel burgers een noodzakelijke voorwaarde (Shabani et al., 2014; Waind, 2020). Tegelijkertijd worden persoonlijke en publieke voordelen niet als tegengesteld ervaren, maar eerder als wederzijds versterkend (Budimir et al., 2011; Kalkman et al., 2022). Toch blijven burgers waakzaam voor onevenredige verhoudingen waarbij commerciële actoren zouden profiteren van publiek gegenereerde data zonder dat daar evenredige maatschappelijk voordelen tegenover staan (Street et al., 2022).

De vraag naar transparantie, zeggenschap en verantwoording voor datagebruik weerspiegelt een bredere wens van burgers om op een betekenisvolle manier betrokken te worden bij de governance van hun gezondheidsdata (Aitken et al., 2016; Skovgaard et al., 2019).

3.3.2 De burger en zijn gezondheidsdata: geletterdheid en vertrouwen

De mate waarin burgers effectief kunnen participeren in de governance van gezondheidsdata hangt samen met hun digitale en gezondheidsgeletterdheid. Verschillen in deze vaardigheden hangen nauw samen met sociodemografische factoren, zoals sociaaleconomische status, opleidingsniveau, leeftijd, en etniciteit (Hutchings et al., 2021; Damen et al., 2022). Om deze ongelijkheid te verminderen en inclusieve participatie te bevorderen, is het essentieel om te investeren in toegankelijke informatie, transparante communicatie en educatie die burgers in staat stellen hun rechten te begrijpen en betekenisvol deel te nemen aan governance (Househ et al., 2018; Cumyn et al., 2023).

Vertrouwen speelt daarnaast een sleutelrol in de bereidheid van burgers om hun gezondheidsdata te delen. Burgers blijken doorgaans meer vertrouwen te hebben in publieke instellingen, zoals ziekenhuizen en universiteiten, dan in private of commerciële actoren (Husedzinovic et al., 2015; Hutchings et al., 2020; Naeem et al., 2022). Vertrouwen fungeert daarbij als een soort hefboom. Waar vertrouwen hoog is, zijn burgers sneller geneigd hun data te delen, zelfs als de mogelijkheden tot zeggenschap beperkt zijn. Omgekeerd leidt een laag vertrouwen tot een grotere vraag naar zeggenschap en expliciete toestemming (Clayton et al., 2018; Moorthie et al., 2022).

Een gebrek aan vertrouwen en een gebrek aan vaardigheden kunnen elkaar versterken, waardoor burgers zowel de motivatie missen als de middelen om zich actief in te zetten in governanceprocessen. Daarom is het belangrijk dat beleid en praktijk niet alleen inzetten op bewustmaking en informatievoorziening, maar ook op het verlagen van structurele drempels voor participatie, met specifieke aandacht voor kwetsbare of ondervertegenwoordigde groepen (Hutchings et al., 2021; Damen et al., 2022).

3.3.3 De burger en participatieve governance

Ondanks toenemende aandacht voor participatie in regelgeving zoals de EHDS, blijft het in de praktijk onduidelijk wat burgerparticipatie in de governance van gezondheidsdata precies kan inhouden. Algemeen gezien kan participatie in governance verschillende vormen aannemen, gaande van transparantie en geïnformeerd worden, tot effectieve zeggenschap door middel van inspraak in besluitvorming (Aitken et al., 2016). Daarbij wordt de wens naar zeggenschap vooral ingegeven door een behoefte aan autonomie en bescherming tegen misbruik, en minder door een expliciete ambitie om zelf dagelijks databeheer op zich te nemen (Simpson et al., 2021).

De effectiviteit van participatie hangt sterk af van de mate waarin burgers hun rol als medebeslissers kunnen opnemen in een context van vertrouwen, transparantie en ondersteuning. In dit opzicht wordt het belang van tussenfiguren, zoals zorgprofessionals of community link workers, aangehaald (Aughterson et al., 2020; Hannes et al., 2024). Deze kunnen fungeren als een brug tussen burgers en complexe datasystemen, en helpen om drempels zoals beperkte digitale geletterdheid of wantrouwen te verlagen (Evans et al., 2014; Sabey et al., 2022).

Tenslotte blijkt dat burgers openstaan voor collectieve vormen van governance, zoals burgercommissies of datacomités, waarin zij samen met andere stakeholders kunnen waken over het ethisch en maatschappelijk verantwoord gebruik van data (Howe et al., 2018; Kalkman et al., 2022). Dergelijke modellen sluiten aan bij het idee van datasolidariteit, waarbij het belang van het collectief en de bescherming van kwetsbare groepen centraal staan (Prainsack en Kickbusch, 2024). Participatie wordt dan niet louter individueel opgevat, maar als een sociaal ingebedde praktijk met aandacht voor inclusiviteit en rechtvaardigheid (Tommel et al., 2023).

3.3.4 De burger en toestemming

3.3.4.1 Soorten consent: opt-in en opt-out

Vanuit de regelgeving wordt in grote lijnen het onderscheid gemaakt tussen opt-in, waar een persoon expliciet toestemming geeft voor deelname en opt-out, waar deelname en toestemming tot deelname een basisaanname is, en de persoon bij actieve kennisgeving zich aan deelname kan onttrekken.

Bij de AVG wordt het concept van de rechtsgrond toestemming als een opt-in geïnterpreteerd: er dient een duidelijk actieve handeling te worden gesteld, en daarenboven moet de toestemming vrijelijk gegeven zijn, specifiek, geïnformeerd en ondubbelzinnig (overweging 32 en art. 7). Daarnaast mag er geen wanverhouding zitten tussen de betrokkene en de verwerkingsverantwoordelijke, waar er vermoed kan worden dat de toestemming niet vrijelijk kan worden gegeven (overweging 43). Voorbeelden zijn bijvoorbeeld toestemming tussen werkgever en werknemer, of tussen een persoon en een overheidsinstantie.

De vraag tot toestemming en de info die men als betrokkene ontvangt over de verwerking dient verder ook helder en verstaanbaar te zijn. Daar loopt het in de toepassing van de AVG al vaak mis, aangezien privacyverklaringen vaak uitvoerig en omslachtig worden opgesteld, vooral met het oog op het voldoen aan de voorwaarden van de informatieplicht aan de AVG, en minder gericht op de verstaanbaarheid voor de betrokkene. Onderzoek toont dan ook aan dat mensen vaak toestemmingsformulieren of privacyverklaringen slecht begrijpen (Wisgella & Hasford, 2021; Korunovska, Kamleiter & Spiekermann, 2005; Geier, et al., 2021)[36,37,38] en de risico's slecht inschatten, wat de ethische basis voor consent deels ondergraaft, met name dat ervan uitgegaan wordt dat men geïnformeerde keuzes maakt. Ook sociodemografische factoren kunnen leiden tot slecht begrip van consentformulieren zoals taalbarrières, zeker als de formulieren vanuit een sterke legale invalshoek worden opgesteld.

[36] https://pubmed.ncbi.nlm.nih.gov/35246415/

[37] https://arxiv.org/pdf/2005.08967

[38] https://pubmed.ncbi.nlm.nih.gov/34029168/

Daarnaast worden mensen vaak overstelpt met toestemmingsvragen, zie ook het probleem van de cookie-consent: een uitgebreide lijst van vragen om toestemming, soms samengevat in ‘accept all’ of ‘refuse all’, en mensen die eerder voor de snelle opties gaan en minder voor de granulaire keuzes. Daarenboven kunnen mensen ook gemanipuleerd worden in het geven van een consent in een bepaalde richting: door de keuze van het accepteren van alle cookies te vergemakkelijken en drempels op te werpen om deze te gaan afwijzen (bv. groene kleur ‘accept all’, weigeren-optie extra laten doorklikken, enz.). Om deze reden heeft de European Data Protection Board (EDPB) richtlijnen uitgevaardigd over het correct bevragen van cookievoorkeuren[39], maar vooralsnog worden deze nog niet algemeen toegepast.

Ondanks richtlijnen van de EDPB rond cookieconsent en ook het correct bevragen van consent[40], blijft het een problematisch concept. Hoewel het de ultieme zeggenschap lijkt van een individu op zijn gegevens, legt het tevens ook alle verantwoordelijkheid bij het individu, en bovenstaande voorbeelden geven aan dat mensen vaak keuzes maken die tegen hun belangen of initiële intenties ingaan, door ofwel de omslachtige manier om geïnformeerd te geraken over toestemming, het niet begrijpen van het doel van de toestemming of manipulatie in het verkrijgen van consent. Dit kan leiden tot een vals gevoel van controle, waarbij toestemming formeel gegeven wordt, maar zonder echte geïnformeerde keuze. Bovendien miskent het systeem van individuele consent vaak dat persoonsgegevens ook een collectieve waarde kunnen hebben, bijvoorbeeld in het kader van wetenschappelijk onderzoek of publieke gezondheidszorg. Wanneer toegang tot data enkel via individuele toestemming wordt geregeld, bestaat het risico dat bepaalde groepen (zoals ouderen of mensen met beperkte digitale vaardigheden) worden uitgesloten, wat maatschappelijke ongelijkheid versterkt. Tot slot kan een te strikte focus op toestemming de morele verantwoordelijkheid van organisaties ondermijnen: zodra de handtekening van de burger binnen is, verdwijnt soms de zorg om rechtvaardigheid, transparantie of inclusie. Consent blijft belangrijk, maar moet steeds ingebed worden in een breder governancekader dat aandacht heeft voor collectieve waarden, begrijpelijke communicatie en structurele bescherming van burgers.

Om bovenstaande redenen is er in de EHDS niet gekozen voor toestemming voor secundair gebruik van gegevens, naast bezorgdheden rond mogelijke selectiebias (Kho et al., 2009; Kluge, 2004) [41,42]. Initieel werd er helemaal geen opt-in of opt-out gevraagd van de betrokkenen, maar door protest vanuit sommige lidstaten over het zo toch wel grote gebrek aan betrokkenheid en transparantie voor personen over hun gezondheidsgegevens en wat er mee gebeurt, is het opt-out concept geïntroduceerd. Er zijn wel wat randvoorwaarden en uitzonderingen ingebouwd, waar lidstaten het recht op opt-out kunnen beperken indien dit goed verantwoord wordt, in situaties van gewichtig belang. Ook de AVG had op het vlak van onderzoek wel uitzonderingen voorzien op het vlak van consent in de situatie van wetenschappelijk onderzoek of statistische doeleinden, in geval het moeilijk tot onmogelijk was om de betrokkenen te contacteren om toestemming te bevragen. Opt-out kan als risico hebben dat het de autonomie van het individu ondergraaft, zeker indien het moeilijk wordt gemaakt om de opt-out uit te oefenen, waardoor mensen zich mogelijk niet eens bewust zijn van de mogelijkheid tot opt-out. Opt-out kan ook gezien worden als het plaatsen van de verantwoordelijkheid op het individu, wat oneerlijk kan zijn in geval de opt-out moeilijk te vinden is, of de aanpassingen moeilijk te maken, en het houdt dezelfde risico’s in rond toegankelijkheid en verstaanbaarheid voor kwetsbare populaties. Indien het te weinig transparant is, kan het leiden tot een daling in het vertrouwen. Allicht om die reden bepaalt de EHDS dat het opt-out mechanisme voor secundair gebruik makkelijk en toegankelijk dient te zijn. Maar net als bij opt-in bestaat het risico bij opt-out dat het een last wordt, als er heel veel van deze opt-outs bestaan. Dat risico bestaat zeker indien de EHDS leidt tot een boost in het secundair gebruik van gegevens. Ook het gebruik van opt-out bij heel gevoelige datasets kan ethische uitdagingen bieden. In veel nationale regelgeving is het voor dit soort data wel vereist om een duidelijke opt-in te hanteren, en de EHDS handhaaft deze nationale regelgeving ook voor secundair gebruik (overweging 11).

Omwille van de veelvuldige risico’s die er rond consent bestaan, kan het lonen om te kijken naar alternatieven, ofwel voor de rechtsgrond van verwerking (AVG), of, indien consent wenselijk is, naar alternatieven voor de klassieke opt-in en opt-out om de risico’s op incorrect en onethisch gebruik van consent tegen te gaan.

---

39 https://www.edpb.europa.eu/system/files/202301/edpb_20230118_report_cookie_banner_taskforce_en.pdf

40 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

41 https://pmc.ncbi.nlm.nih.gov/articles/PMC2769263/

42 https://pubmed.ncbi.nlm.nih.gov/15360890/

3.3.4.2 Meer soorten consent: individueel en collectief consent

Als manier van zeggenschap wordt toestemming vaak genoemd als manier van controle over data. Vaak gaat het dan over individueel consent wat op verschillende manieren kan worden ingeregeld. De EHDS noemt voornamelijk eenvoudige opt-in/op-out mechanismen als manier voor individuen om zeggenschap over gezondheidsdata uit te oefenen. Andere vormen van consent zijn brede toestemming, dynamisch consent of granulaire toestemming. Deze vormen kunnen onderdeel zijn van gedelegeerd consent waarbij een individu iemand anders of een organisatie machtigt om namens hem/haar toestemming te geven. Een andere vorm van consent is endorsement consent, een vorm van collectief consent waarbij een collectief, bijvoorbeeld een gemeenschap (zie boven) besluit of bepaald of datagebruik acceptabel is. Endorsement consent is niet zozeer een juridische vorm van consent maar meer een governancevorm.

Consent – van individueel consent naar collectief consent

Consent (toestemming) in de context van medisch datagebruik betekent de uitdrukkelijke toestemming van een persoon om diens gezondheidsgegevens te mogen verzamelen, gebruiken of delen. Consent is geldig wanneer het:

1. **Vrij gegeven** is – dus er is geen druk of verplichting opgelegd.
2. **Specifiek** is – het is duidelijk waarvoor de data worden gebruikt.
3. **Geïnformeerd** is – de persoon begrijpt wat er met zijn gegevens gebeurt.
4. **Ondubbelzinnig** is – er is een duidelijke ja, meestal via een handtekening of een digitale bevestiging.
5. **Herroepbaar** is – een persoon mag op elk moment van gedachten veranderen.

Er bestaan verschillende vormen van consent zoals **breed consent**, een vorm van toestemming waarbij een persoon of deelnemer aan onderzoek, toestemming geeft voor een nog niet volledig gespecificeerde reeks van toekomstige onderzoeksdoeleinden. **Dynamisch consent**, een doorlopende aanpasbare toestemming vaak via een digitaal systeem, met maximale transparantie en controle. **Granulair consent** is een variant waarbij een patiënt of deelnemer kan aangeven welke categorieën van data wel of niet mogen worden gedeeld. **Opt-out** in de context van consent betekent dat iemand automatisch data deelt, tenzij de persoon actief aangeeft niet mee te willen doen. Bij **Opt-in** doet iemand pas mee als hij actief instemt.

Het vertrek punt van **gedelegeerd individueel consent** is dat een persoon een ander bijvoorbeeld een familie lid of een organisatie de machtiging geeft om namens hem/haar toestemming te geven. De vertegenwoordiger handelt daarbij namens het individu en in diens belang. Het vertrekpunt van **Endorsement consent** is dat een gemeenschap of collectieve vertegenwoordiger (bijvoorbeeld een patiëntenvereniging of een datacoöperatie, besluit of een bepaald datagebruik acceptabel is. De vertegenwoordiger spreekt namens de groep of organisatie en beslist op basis van vastgelegde waarden en afspreken. Belangrijk om te vermelden is dat endorsement consent niet een juridische vorm van consent maar een governance afspraak is.

3.3.4.3 Consent uitbesteden: consentprofielen en gedelegeerd consent

De concepten opt-in of opt-out kunnen aangevuld of vervangen worden door nieuwe consentconcepten, vooral gericht op het bundelen van de keuzes die gemaakt worden, of het uitbesteden van deze keuzes aan vertrouwde partijen. Een uitgebreide oefening hierrond werd uitgevoerd door HealthRI in samenwerking met Gaston Remmers[43], waar dialogen met verschillende actoren en ook burgers werden opgezet om dieper in te gaan op de uitdagingen rond zeggenschap in brede zin (met onder meer ook vertrouwen en transparantie-uitdagingen), en dus ook toestemming als onderdeel hiervan, de moeilijkheden van een pure opt-in en opt-out, en de variërende noden rond zeggenschap en ook toestemming doorheen de levensloop. Het stelt een soort burgerreis voor, waarin rekening wordt gehouden met het soort zeggenschapsuitoefening, de nodige info, technische ondersteuning en randvoorwaarden. Daarnaast werden er ook een

[43] https://www.health-ri.nl/sites/healthri/files/2024-10/0924HRI_Rapp-Maatschappelijke%20Dialogen-v1.pdf

dialoog opgesteld rond ondersteuning van burgers in het maken van keuzes, en de informatie die ze daarbij wensen te krijgen, waar de kern ligt rond de aspecten vertrouwen, ondersteuning en organisatiemodel en hoe deze correct in te vullen om tot een goede ondersteuning te komen in het maken van keuzes.

Een consentprofiel bestaat uit een aantal vooraf bepaalde keuzes rond welke partijen onder welke omstandigheden toegang hebben tot bepaalde gegevens. Een voorbeeld kan zijn dat ziekenhuizen die toegang zoeken tot gezondheidsgegevens altijd toestemming krijgen zonder dit telkens opnieuw te bevragen. In België is er niet meteen iets als een consentprofiel ingesteld, maar in het eGezondheidslandschap is de toestemming die een burger geeft voor het delen van zijn elektronische gezondheidsgegevens in de zorg wel gekoppeld aan een toegangsmatrix, die per type zorgverlener gaat bepalen tot welke specifieke gegevens deze toegang heeft. In het model van Gezond Akkoord worden enkel de dataverzoeken die leden interesseren, voorgelegd voor toestemming. Een uitbreiding hierop kan zijn dat voor de interessante dataverzoeken de voorwaarden worden vastgelegd om ook automatisch deze toestemming te gaan toekennen.

Gedelegeerde toestemming is vooral gericht op het uitbesteden van de toestemmingsverzoeken aan betrouwbare partijen. In de zorg bestaan er machtigingen, om beslissingen rond de gezondheid uit te besteden aan vertrouwde derde partijen (bv. mantelzorger, ouder of voogd bij minderjarigen, enz.). Ook bestaat het concept ‘zorgvolmacht’, waar mensen kunnen aangeven wie voor hen beslissingen kan nemen als zij in de onmogelijkheid verkeren (bv. opvolgen bankzaken bij personen met dementie). Dit concept valt mogelijk ook uit te breiden naar digitale toestemmingen over het delen van gezondheidsgegevens. De DGA omschrijft bij de databemiddelingsdiensten de mogelijke functie om rechten, zoals toestemmingen, te laten beheren (meer bepaald bij de datacoöperatie).

Banken hanteren dergelijke principes in een andere vorm al wel. Zo kan een beleggersprofiel worden opgesteld, waar voorkeuren en soorten risico’s die een persoon wil nemen in kaart wordt gebracht, waarna de beleggingsportefeuille met inspraak van de klant verder wordt beheerd, zonder dat voor elke aparte keuze toestemming moet worden gevraagd, dit naast de optie dat een persoon ook helemaal alleen zijn eigen beleggingen beheerd en kan kiezen voor de mate van betrokkenheid. Dit is een voorbeeld van een combinatie van profielen opstellen en delegatie van diensten, en zou ook een bruikbaar model kunnen zijn om dit ook toe te passen in de zorg.

3.4 Aanbevelingen voor een burgergedreven governance model

3.4.1 Gaps en aanbevelingen

3.4.1.1 Burger en rol in data-ecosysteem

- Burgers hebben zelden zicht op wie hun gezondheidsdata gebruikt, met welk doel en met welke gevolgen, terwijl onderzoek aantoont dat ze dit erg belangrijk vinden. Dat is een eerste voorwaarde om vertrouwen te kunnen ontwikkelen. Transparantieverplichtingen zijn echter vaak beperkt tot abstracte privacyverklaringen.
  - **Aanbeveling 1**: ontwikkel een platform waarin burgers kunnen zien wie toegang heeft (gehad) tot hun data, en voor welk type gebruik (bv. via persoonlijke data dashboards).

- Hoewel gezondheidsdata vaak gebruikt worden voor onderzoek of beleidsontwikkeling in het “algemeen belang”, bestaat er geen kader waarin burgers mee bepalen wat als “algemeen belang” geldt.
  - **Aanbeveling 2**: Introduceer collectieve governancevormen, zoals coöperaties of data trusts, waarin burgers inspraak hebben in het vaststellen van maatschappelijke prioriteiten en voorwaarden voor datagebruik.

- Hoewel burgers bepaalde formele rechten hebben over hun data (bv correctie, dataportabiliteit, opt-out, enz.), is voor burgers vaak onduidelijk welke rechten ze precies hebben over hun gezondheidsdata, en hoe ze die in de praktijk kunnen uitoefenen.
  - **Aanbeveling 3**: Versterk het operationeel eigenaarschap van burgers via instrumenten zoals persoonlijke datakluizen, recht op dataportabiliteit, en ondersteuning bij het beheren van toegang en rechten (bv. datacoöperaties DGA).

- Juridisch gezien is het voornaamste instrument voor de burger de ‘informed consent’, maar deze is vaak niet echt geïnformeerd, begrijpelijk of aangepast aan de context van de gebruiker. Ook burgers zien zeggenschap niet per se als het continu opvolgen van hun data, maar hechten vooral belang aan aandacht voor autonomie en transparantie.
  - **Aanbeveling 4**: ontwikkel verschillende consent-opties (delegated consent, group consent enz.) die aangepast zijn aan de noden van verschillende gebruikers.

- De regelgeving kan eigenlijk maar adequaat inspelen op traag evoluerende datasystemen zoals de EPDs. Voor snel evoluerende domeinen zoals gezondheids- of wellnessapps zijn er grote onduidelijkheden.
  - **Aanbeveling 5**: er is nood aan een flexibel en adaptief governancekader op basis van technologie-neutrale en toekomstgerichte ethische toetsingskaders, die deliberatief (in onderling overleg met burgers) moeten toegepast worden.

- Ook de concepten en rollen in de huidige modellen rond dataruimten zijn niet goed aangepast aan de rol van de burger in het geheel, en de link met het regelgevend kader dat deze burger rechten toekent.
  - **Aanbeveling 6**: Ontwikkel een governancekader aangepast aan een persoonlijke dataruimte, met duidelijke richtlijnen rond de rol van de burger en hoe hij kan deelnemen aan het systeem via portalen of andere systemen van burgerparticipatie. Toon aan hoe dit kader in te passen valt in de definities en bestaande governanceaspecten van bestaande dataruimten, onder meer die van gezondheid (EHDS).

- Vertrouwen wordt als een kernelement gezien in de dataruimten, en ook in de bereidheid van de burger om data te gaan delen, maar er is vooralsnog geen magische formule die dit succesvol implementeert, met verschillende benaderingen vanuit regelgeving, dataruimtes en burgergedreven governancemodellen.
  - **Aanbeveling 7**: Maak werk van het opbouwen van vertrouwen in een burgerbetrokken dataruimte, door het inzetten op pro-actieve en duidelijke communicatie en transparantie, aandacht voor ethische randvoorwaarden, gebruik van betrouwbare actoren in gezondheid en meer inspraak in de datadeling van de eigen gegevens.

- Burgers krijgen vaak nog alle initiatief bij hen gelegd als het gaat over het uitoefenen van hun rechten (o.a. actief vragen naar dataportabiliteit, veelvuldige vragen rond consent zonder duidelijke info, zelf vragen indienen of correcties aanvragen, enz.), maar voelen zich vaak niet voldoende onderlegd of gemotiveerd om dit permanent op te volgen.
  - **Aanbeveling 8**: Ontwikkel een systeem waar burgers kunnen beroepen op tussenpersonen of vertrouwde tussenpartijen om hun rechten uit te oefenen (o.a. collectieve vormen van governance voor beheer en deling van persoonsgegevens).

3.4.1.2 Preventiedataruimte en data-ecosysteem

- Levensstijlfactoren hebben een sterke impact op de ontwikkeling van chronische ziekten, en preventie kan bijgevolg potentieel sterk wegen op de evolutie naar een duurzaam gezondheidssysteem. Toch wordt dit in regelgeving en dataruimte-modellen eerder stiefmoederlijk behandeld, met meer focus op curatieve aspecten en grote, klinische datasets.
  - **Aanbeveling 9**: ontwikkel standaarden en datamodellen rond levensstijl en welzijn in lijn/compatibel met de EHDS-aanbevelingen, zodat preventie structureel kan ingebed worden voor zowel primair als secundair gebruik.

- Preventie omvat voornamelijk gegevens die door burgers zelf worden aangeleverd of aangemaakt, en aanpassingen aan levensstijl kunnen ook buiten de klinische context plaatsvinden. De regelgeving en systemen rond EPD's voorzien nu nog geen of maar beperkte richtlijnen over hoe de burger kan participeren, en enkel door inbedding in de bestaande EPD's.
  - **Aanbeveling 10**: Ontwikkel systemen voor zelfmanagement van levensstijl en gezondheid voor de burger. Zorg dat deze systemen kunnen connecteren met EPD's of patiëntenportalen, en maximaliseer gebruiksgemak o.a. door hergebruik van datapunten mogelijk te maken.

- Veel levensstijlgegevens worden verzameld via wellnessapps, maar hun rol is onderontwikkeld in de huidige regelgeving, en het is onduidelijk hoe ze een betekenisvolle rol kunnen spelen in het grotere gezondheidssysteem.
  - **Aanbeveling 11**: Stimuleer wellnessapps om gebruik te maken van bestaande standaarden en richtlijnen rond dataruimtes. Ontwikkel een datacatalogus en evalueer datakwaliteit.

3.4.2 WellData-aanpak en -model

WellData is als project opgestart om beter te gaan gegevens uitwisselen rond preventie, en te komen tot een dataruimte, maar vanuit een meer burgergedreven aanpak omdat de kern van preventiegegevens voortkomen uit informatie die burgers zelf aanleveren. Daarnaast wil WellData een sluitend ELSA-kader opzetten, om te komen tot een burgergedreven, participatieve en ethische governancestructuur van deze dataruimte. Vanuit die optiek werd al een visie-missie gedefinieerd, en een set van principes met governance-aanbevelingen om deze principes in de werking van WellData te gaan verankeren. De principes zijn als volgt:

- Respect voor Personen en Individuele Autonomie
- Maatschappelijke Waarde
- Privacy en Veiligheid
- Datakwaliteit en Robuustheid
- Verantwoordingsplicht
- Duurzaamheid en Opschaalbaarheid

Deze principes, samen met dit rapport, worden verder afgetoetst in WP 4.3 met burgerpanels en in de fieldlabs. Meer bepaald worden de governance-suggesties van de principes en de aanbevelingen uit 3.3.1 voorgelegd en afgetoetst. Ook de huidige operationalisering van deze aanbevelingen worden bevraagd. Vanuit de feedback zullen de aanbevelingen onder 3.3.1 dan worden afgetoetst en aangepast, om tot een nieuwe versie van dit rapport te komen met

finale aanbevelingen en operationaliseringsaspecten voor het WellData-model, evenals andere systemen van gegevensdeling en gezondheidsbevordering rond preventie.

Momenteel operationaliseert WellData de aanbevelingen uit 3.3.1 al op de volgende manier:

1. Visualisatie van welke applicaties toegang hebben met mogelijkheid tot beheer van deze toegang (access managementapplicatie, AMA)
2. Co-creatie, burgerpanels en fieldlabs om burgers actief te betrekken, en verwerking van de governancestructuur van We Are en Gezond Akkoord in de WellData-governance-aanbevelingen.
3. Gebruik van Solid pods of persoonlijke datakluizen, stimuleren van hergebruik van data en zeggenschap via de AMA
4. Exploratie, aftoetsing en testing van nieuwe consentmechanismen (verder op te nemen in 4.3)
5. Vastleggen van WellData principes, en gebruik ethisch kader We Are bij livetests
6. Positionering WellData ten opzichte van bestaande systemen via dit rapport, verdere vergelijking nog meer uit te werken naar finale aanbevelingen toe (na acties 4.3)
7. Sterke betrekking van burgers in hele ontwikkelingsproces: aandacht voor maximale transparantie en communicatie
8. Exploratie van gedelegeerd consent en ondersteuning kwetsbare groepen in gezondheidsmanagement via field labs (4.3)
9. Ontwikkelen van een datamodel en gebruik van internationale standaarden (o.a. SOLID, FHIR, enz.)
10. Dashboard voor monitoring van gezondheidsparameters en gezondheidsaanbevelingen via actieplan. Link en koppeling met bestaande systemen nog te verkennen.
11. Richtlijnen voor ontwikkeling van datacatalogus en metadatagegevens rond datakwaliteit vanuit de standaardisatie- en datamodeloefening. Link met eventuele EHDS-aanbevelingen nog te implementeren.

3.4.3 Conclusies

De laatste jaren zagen heel wat evoluties in datadeling, ook in gezondheid, en zeker op Europees niveau is er veel aandacht voor. Europa wil een duidelijke rol gaan opnemen in de data-economie, en meer waarde halen uit het gebruik van data, zeker ook voor gebruik hiervan in AI-modellen. Daarnaast gaat dit ook gepaard met meer aandacht voor de rol van de burger in dit ecosysteem, al zien we dat de regelgeving geen perfect antwoord biedt. Naast de regelgeving zijn er bewegingen zoals MyData en andere burgergedreven initatieven om de lacunes mee op te vullen, en WellData wil op deze beide evoluties verder bouwen. Zo zijn de WellData-principes ontwikkeld op bestaande kaders, en zijn er in het project al heel wat operationaliseringen gebeurd naar concretisering van die principes toe en verankering in de governance. Eveneens zijn heel wat van de aanbevelingen in dit rapport, over dataruimtes, regelgeving en andere initiatieven en de bestaande lacunes, al deels of volledig geïmplementeerd in WellData. Belangrijk zal zijn om in de toetsing vanuit taak 4.3 in het WellData-project dit verder te gaan concretiseren, en te vertalen naar een helder voorstel voor een governancekader. Dit rapport zal bijgevolg door deze input zich tot een nieuwe versie ontwikkelen om tot een finaal overzicht te komen aan het einde van het Welldata-project.

In dit finale rapport dient er nog bijkomende aandacht te zijn voor de EHDS en de evoluties hierin, en hoe de aanbevelingen vanuit WellData een antwoord kunnen bieden op de grijze zones en onduidelijke rol van preventie, zodat WellData ook duidelijke beleidsaanbevelingen kan doen, bijvoorbeeld richting de lokale HDAB's. Immers, de rol van wellnessapps valt nog verder nationaal te bepalen. Doordat WellData specifiek naar de rol en meerwaarde van deze apps kijkt in het bredere preventiekader, en bovendien grensoverschrijdend, kan dit waardevolle aanbevelingen opleveren om te vermijden dat er wat betreft de rol van wellnessapps een te grote versnippering zou optreden (silo's tussen landen). Uiteindelijk zal dit rapport worden verwerkt richting een peer-reviewed paper in een internationaal tijdschrift.

4. Referenties

1. Aitken M, de St Jorre J, Pagliari C, et al. (2016) Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. BMC Medical Ethics 17(1): 73.
2. Aughterson H, Baxter L and Fancourt D (2020) Social prescribing for individuals with mental health problems: a qualitative study of barriers and enablers experienced by general practitioners. BMC Family Practice 21: 1-17.
3. Budimir D, Polašek O, Marušić A, Kolčić I, Zemunik T, et al. (2011). Ethical aspects of human biobanks: a systematic review. Croatian medical journal, 52(3), 262-279.
4. Clayton EW, Halverson CM, Sathe NA, Malin BA. (2018). A systematic literature review of individuals' perspectives on privacy and genetic information in the United States. PLoS ONE. 2018;13(10)
5. Cumyn A, Ménard JF, Barton A, Dault R, Lévesque F, & Ethier JF (2023). Patients' and members of the public's wishes regarding transparency in the context of secondary use of health data: scoping review. Journal of Medical Internet Research, 25(1), e45002.
6. Damen DJ, Schoonman GG, Maat B, Habibović M, Krahmer E, & Pauws S (2022). Patients managing their medical data in personal electronic health records: scoping review. Journal of Medical Internet Research, 24(12), e37783.
7. El-Sayed S, Kickbusch I, Prainsack B (2025) Data solidarity: Operationalising public value through a digital tool. Glob Public Health 20(1):2450403.
8. Evans C, Nalubega S, McLuskey J, et al. (2014) The views and experiences of nurses and midwives in the provision and management of routine (provider initiated) HIV testing: protocol for a systematic review of qualitative evidence. JBI evidence synthesis 12(2): 103-113.
9. Geier C, Adams RB, Mitchell KM, Holtz BE (2021) Informed Consent for Online Research-Is Anybody Reading?: Assessing Comprehension and Individual Differences in Readings of Digital Consent Forms. Journal of Empirical Research on Human Research Ethics 16(3): 154-164.
10. Hannes K, Thyssen P, Bengough T, et al. (2024) Inclusive Crisis Communication in a Pandemic Context: A Rapid Review. International journal of environmental research and public health 21(9): 1216.
11. Howe N, Giles E, Newbury-Birch D, & McColl E (2018). Systematic review of participants' attitudes towards data sharing: a thematic synthesis. Journal of health services research & policy, 23(2), 123–133. https://doi.org/10.1177/1355819617751555
12. Househ M, Grainger R, Petersen C, Bamidis P, & Merolli M (2018). Balancing between privacy and patient needs for health information in the age of participatory health and social media: a scoping review. Yearbook of medical informatics, 27(01), 029-036.
13. Hutchings E, Loomes M, Butow P, & Boyle FM (2020). A systematic literature review of health consumer attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on privacy, trust, and transparency. Systematic reviews, 9(1), 235. https://doi.org/10.1186/s13643-020-01481-9
14. Hutchings E, Loomes M, Butow P, & Boyle FM (2021). A systematic literature review of attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on consent. Systematic Reviews, 10, 1-44.
15. Husedzinovic A, Ose D, Schickhardt C, Frohling S, Winkler EC (2015). Stakeholders' perspectives on biobank-based genomic research: Systematic review of the literature. Eur J Hum Genet., 23(12):1607-1614.
16. Kalkman S, Van Delden J, Banerjee A, Tyl B, Mostert M, & Van Thiel G. (2022). Patients' and public views and attitudes towards the sharing of health data for research: a narrative review of the empirical evidence. Journal of medical ethics, 48(1), 3-13.
17. Kassam I, Ilkina D, Kemp J, Roble H, Carter-Langford A, & Shen N (2023). Patient perspectives and preferences for consent in the digital health context: state-of-the-art literature review. Journal of medical Internet research, 25, e42507.
18. Kho ME, Duffet M, Willison DJ, Cook DJ, Brouwers MC. (2009). Written informed consent and selection bias in observational studies using medical records: systematic review. BMJ, 338:b866.
19. Kluge EHW. (2024). Informed consent to the secondary use of EHRs: informatic rights and their limitations. Studies in Health Technologies & Informatics, 107(1): 635-638.
20. Korunovska J, Kamleitner B, Spiekermann S. Korunovska, Jana and Kamleitner, Bernadette and Spiekermann, Sarah (2020). The Challenges and Impact of Privacy Policy Comprehension. ECIS 2020, available at SSRN: https://ssrn.com/abstract=3604171

21. Moorthie S, Bartsota M, Wolfe I, et al. (2022). Rapid systematic review to identify key barriers to access, linkage, and use of local authority administrative data for population health research, practice, and policy in the United Kingdom. BMC Public Health. 22(1):1263.
22. Naeem I, van der Wal CC, Aarts JW, van Dongen JJM, van Halteren AT (2022). Factors Associated With Willingness to Share Health Information: Rapid Review. JMIR Hum Factors. 9(1)
23. Prainsack B, El-Sayed S, Forgo N, Szoszkiewicz L, Baumer P. (2022) Data solidarity: a blueprint for governing health futures. The Lancet 4(11): e773-e774
24. Prainsack B and Kickbusch I (2024) A new public health approach to data: why we need data solidarity. British Medical Journal Publishing Group.
25. Sabey A (2022) An evidence review of social prescribing and physical activity.
26. Shabani M, Bezuidenhout L and Borry P (2014) Attitudes of research participants and the general public towards genomic data sharing: A systematic literature review. Expert Review of Molecular Diagnostics 14(8): 1053-1065.
27. Simpson E, Brown R, Sillence E, et al. (2021) Understanding the Barriers and Facilitators to Sharing Patient-Generated Health Data Using Digital Technology for People Living With Long-Term Health Conditions: A Narrative Review. Frontiers in Public Health 9.
28. Skovgaard LL, Wadmann S and Hoeyer K (2019) A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. Health Policy 123(6): 564-571.
29. Stockdale J, Cassell J and Ford E (2019) “Giving something back”: A systematic review and ethical enquiry into public views on the use of patient data for research in the United Kingdom and the Republic of Ireland [version 2; referees: 2 approved]. Wellcome open research 3.
30. Street J, Carter S, Fabrianesi B, Bosward R, Carolan L, & Braunack-Mayer A. (2022). Public attitudes to sharing government data with private industry: a systematic scoping review. medRxiv, 2022-06.
31. Tommel J, Kenis D, Lambrechts N, et al. (2023) Personal genomes in practice: exploring citizen and healthcare professionals’ perspectives on personalized genomic medicine and personal health data spaces using a mixed-methods design. Genes 14(4): 786.
32. Waind, E. (2020). Trust, security and public interest: striking the balance A narrative review of previous literature on public attitudes towards the sharing, linking and use of administrative data for research. International journal of population data science, 5(3), 1368.
33. Wisgella A, Hasford J. (2022). Four reasons why too many informed consents to clinical research are invalid: a critical analysis of current practices. BMJ Open, 12(3): e050543.