Vlaanderen
is zorgzaam en
gezond samenleven

EINDRAPPORT
VLAAMSE HEALTH DATA SPACE PROJECT

DEPARTEMENT
ZORG

departementzorg.be

COLOFON

Verantwoordelijke uitgever
Karine Moykens
Secretaris-generaal
Departement Zorg
Simon Bolivarlaan 17
1000 Brussel

Samenstelling
Departement Zorg
Center for IT and IP Law – KU Leuven (CiTiP)
Imec

Projectsponsor
Koenraad Jacob (Departement Zorg)

Center for IT and IP Law – KU Leuven (CiTiP)
Lotte Cools
Daniela Spajic

Departement Zorg
Katrien Levrie
Pieterjan Uytterhoeven
Kurt Vanbrabant
Kristof Vandenbroeck
Pieter Van Beek

Imec
Gabriele Bozzi
Matthias Degeyter
Xueying Deng
Sofie De Lancker
Dorien Goubert
Konstantin Kostov
Thomas Kusmirczak
Bart Matthys
Nell Van hansewyck

Productcoördinatie en vormgeving
Afdeling Communicatie en IT - Team Communicatie

Depotnummer
D/2025/3241/056

Uitgave
Januari 2025

INHOUD

LIJST VAN FIGUREN

EXECUTIVE ABSTRACT

Het Vlaamse Health Data Space R&D project had als doel de randvoorwaarden op business, governance, juridisch en technisch vlak te onderzoeken voor de implementatie van de Vlaamse health data space. Dit tweejarig innovatieproject vond plaats tussen 2023 en 2024 ter voorbereiding van de European Health Data Space regulering.

Bij aanvang van het project werden enkele onderzoeksvragen opgesteld. Gaandeweg was het echter nodig om bepaalde onderzoeksvragen bij te sturen gezien de pioniersrol die dit project opnam binnen het huidige data space landschap. Gedurende het project is onder meer gebleken dat het niet evident is om het stakeholderlandschap mee op de kar te krijgen. Daardoor kwam de vooropgezette pragmatische aanpak om met echte gezondheidsdata te werken onder druk te staan. Nochtans kwam uit gesprekken met stakeholders naar voren dat er meer en meer vraag is naar een decentrale manier van datadelen.

Met dit onderzoeksproject werd vanuit Departement Zorg, imec en CiTiP momentum gecreëerd waardoor het toekomstige proces om tot nieuwe manieren van datadeling te komen, vergemakkelijkt zal worden. Dit eindrapport kan hieraan een grote bijdrage leveren, aangezien tijdens het project duidelijk is geworden dat vele actoren binnen het gezondheidszorglandschap met vragen zitten over de nakende EHDS-regulering. Het is pas tijdens de laatste maanden van het onderzoeksproject dat de EHDS-regulering concreter is geworden, al blijven er nog veel vraagtekens rond o.a. secure processing environments, rolverdeling, enz.

Dit project heeft gepoogd om de fundamenten te leggen die nodig zijn om vanuit Vlaanderen – en bij uitbreiding België – tegemoet te komen aan de EHDS-regulering. De minimale blauwdruk die in dit eindrapport wordt gelegd, kan als startbasis gebruikt worden voor de verdere uitwerking van de Vlaamse (en Belgische) health data space.

Dit eindrapport is tot stand gekomen vanuit een pioniersrol. Het spreekt voor zich dat bepaalde standpunten en conclusies uit dit eindrapport herbekeken zullen moeten worden naargelang het landschap en de invulling van de EHDS-regulering concreter en matuurder wordt. De ambities lagen bij aanvang van het project erg hoog, maar doorheen de looptijd van het project werd vastgesteld dat de lat te hoog gelegd werd omdat er nog te veel onduidelijkheden zijn op juridisch en technisch vlak. Ondanks de graduele bijstelling van deze lat, bleek uit contacten met andere landen dat Vlaanderen wel degelijk grote stappen heeft gezet en verder staat in het onderzoek naar health data spaces dan heel wat andere lidstaten van de Europese Unie. In dat opzicht mag de waarde van dit onderzoeksproject en het bijhorende eindrapport niet onderschat worden.

1 INTRODUCTIE

Het Departement Zorg onderzocht samen met de onderzoeksinstelling imec of het mogelijk is om met data space technologie aan de slag te gaan in het gezondheidszorglandschap. Het onderzoeksproject dat startte in 2023 duurde twee jaar. Het kadert in de Europese datastrategie waarmee Europa innovatie wil stimuleren door de uitwisseling van data tussen lidstaten te bevorderen zonder daarbij de Europese waarden, normen en wetgeving uit het oog te verliezen. Een hoeksteen van deze strategie is de in 2024 goedgekeurde Europese Gezondheidsdataruimte ofwel European Health Data Space (EHDS) regulering. Daarin staat dat lidstaten verplicht zijn om gezondheidsdata op grote schaal maar ook veilig beschikbaar te stellen.

In dit onderzoeksproject werd nagegaan welke randvoorwaarden vervuld moeten zijn om met een health data space aan de slag te kunnen gaan in Vlaanderen. Dat gebeurde met behulp van echte use cases en dit in samenwerking met stakeholders uit het gezondheidszorglandschap. Om dit gestructureerd aan te pakken, werd het project ingedeeld in drie luiken:

- een business luik
- een governance en juridisch luik
- een technisch luik

Deze luiken komen aan bod in de verschillende hoofdstukken beschreven in dit rapport.

Hoofdstuk 2 bespreekt de context en de gedetailleerde doelstellingen van het project.

Hoofdstuk 3 handelt over data spaces in het algemeen en het Vlaamse, Belgische en internationale speelveld rond data spaces.

Hoofdstuk 4 behandelt hoofdzakelijk het business luik van dit project waarbij nagegaan wordt wat de behoeften van een data space en de noden binnen het (inter)nationale speelveld zijn.

Hoofdstuk 5 licht toe hoe er te werk werd gegaan voor de identificatie en selectie van use cases, en geeft een overzicht van de verschillende onderzochte use cases.

Hoofdstuk 6 gaat dieper in op het juridische en ethische luik van dit project.

Hoofdstuk 7 behandelt het governance luik. Er wordt nagegaan hoe een health data space kan bestuurd worden in Vlaanderen en bij uitbreiding in België.

Hoofdstuk 8 behandelt het technische luik. Hierin wordt onderzocht wat de gewenste architectuur is met inbegrip van de verschillende componenten en mogelijke datastandaarden.

In hoofdstuk 9 wordt dieper ingegaan op de Data4PHM use case die als specifieke use case binnen het Proof of Concept (PoC) werd uitgevoerd.

Hoofdstuk 10 is een vervolg van het business luik waarbij vooral ingezoomd wordt op de business roadmap en de go-to-marketstrategie.

Hoofdstuk 11 maakt een conclusie van dit onderzoeksproject.

Hoofdstuk 12 geeft een overzicht van de verschillende onderzoeksdoelstellingen zoals vermeld in het Besluit van de Vlaamse Regering (BVR).

2 DOEL EN CONTEXT VAN HET PROJECT

2.1 CONTEXT

Het project kadert in de European Strategy for Data. Deze strategie heeft als doel een bloeiende **datagedreven** economie in de EU te creëren door veilige en efficiënte toegang tot en uitwisseling van data mogelijk te maken. Een kernonderdeel is de oprichting van data spaces of dataruimtes: sectoroverschrijdende, gemeenschappelijke data-ecosystemen waarin organisaties data kunnen delen en benutten binnen een duidelijke **juridische, technische** en **organisatorische** structuur.

De dataruimtes bevorderen innovatie, ondersteunen besluitvorming en respecteren Europese waarden zoals privacy, veiligheid en soevereiniteit. Door een gemeenschappelijk databeleid wil de EU data vrij laten circuleren, de concurrentiepositie versterken en bijdragen aan strategische autonomie in cruciale sectoren zoals gezondheidszorg, industrie en energie. Dit project onderzoekt de randvoorwaarden voor de oprichting van een Vlaamse health data space om tegemoet te komen aan deze Europese verordening binnen de gezondheidszorgsector.

Data spaces of data ruimtes zijn een oplossing om actief deel te nemen aan een groeiende data-economie en tegelijkertijd de Europese waarden hoog te houden. Door op een **decentrale** manier **veilige** en **gereguleerde** toegang te bieden tot uitgebreide gegevens van hoge kwaliteit, stellen data spaces Europese bedrijven, de academische wereld en de publieke sector in staat om hun innovatievermogen te vergroten.

In de afgelopen jaren zijn er talrijke door de EU gesponsorde initiatieven ontstaan die verschillende uitdagingen binnen het ecosysteem van data spaces aanpakken en waardevolle inzichten en oplossingen bieden. Als gevolg hiervan zijn er belangrijke stappen gezet met betrekking tot technische hindernissen door middel van technische proof of concepts. In hoofdstuk 3 Data spaces wordt in detail uitgelegd wat data spaces concreet zijn en hoe ze werken.

2.1.1 European Health Data Space regulering

De Europese Unie heeft in haar European Strategy for Data de gezondheidssector erkend als een belangrijk domein voor het implementeren van de principes van data spaces, waarbij het hergebruik van gegevens voor primaire en secundaire doeleinden wordt gestimuleerd. (Primair gebruik verwijst naar het gebruik van gezondheidsgegevens voor het verlenen van zorg; met secundair gebruik wordt het hergebruik van gezondheidsgegevens voor onderzoek, innovatie, beleidsvorming en regelgeving bedoeld.) Met dat doel voor ogen heeft de Europese Commissie in mei 2022 de European Health Data Space (EHDS) gelanceerd. De oprichting van deze data space zal burgers controle geven over hun gezondheidsdata en het gebruik ervan in hun thuisland en andere lidstaten.

De EHDS komt naar voren als een centraal initiatief dat uitdagingen op het gebied van toegang tot en delen van elektronische gezondheidsgegevens aanpakt. In lijn met de visie van een verenigde Europese gezondheidsunie, beoogt EHDS een veilig, interoperabel[1] en privacy-respecterend digitaal gezondheids-landschap tot stand te brengen door te streven naar:

> Verbeterde digitale **toegang** en **controle** over elektronische persoonlijke gezondheidsgegevens van burgers
> Ondersteuning van het gebruik van gezondheidsgegevens voor betere gezondheidszorgverlening, beter **onderzoek, innovatie** en **beleidsvorming**
> Optimale benutting van gezondheidsgegevens in de Europese Unie door veilige **uitwisseling, gebruik** en **hergebruik** mogelijk te maken.

[1] *Het uitwisselen van data zonder beperkingen.*

In hoofdstuk 6.2.6 EHDS-verordening wordt verder ingegaan op de EHDS-verordening vanuit een juridisch perspectief.

2.2 DOELSTELLING PROJECT

Met het health data space project van het Departement Zorg wil Vlaanderen een voortrekkersrol opnemen en tegemoetkomen aan het basisidee van de EHDS: het op een veilige, betrouwenswaardige en gereguleerde manier beschikbaar maken van gezondheidsdata aan alle geïnteresseerden, zoals overheden, zorgverleners, middenveldorganisaties, burgers en de industrie, om zo innovatie te stimuleren.

In deze **haalbaarheidsstudie** wilde de afdeling Beleidsinformatie en Data, in samenwerking met onderzoeksinstelling imec, onderzoeken wat de randvoorwaarden zijn op **technisch, legaal, governance en business** vlak om over te gaan tot de succesvolle implementatie van de Vlaamse – en bij uitbreiding Belgische – health data space. Hierbij was het belangrijk om eveneens aandacht te besteden aan de ontwikkeling van het partnernetwerk dat nodig is om een ecosysteem voor gezondheidsgegevens te creëren. De focus van het onderzoeksproject lag hierbij in de eerste plaats op secundair gebruik.
Door samen te werken en dit ecosysteem van vertrouwen op te bouwen, kunnen we waardevolle kansen ontsluiten en de voordelen realiseren van een bloeiend data-gestuurd gezondheidszorgsysteem.

Het doel van dit project was om algemene maturiteit van data spaces te onderzoeken en op basis van echte business use cases enkele technische proof of concepts (PoC's) uit te voeren om zo te onderzoeken of een health data space haalbaar is in Vlaanderen en België en hoe ze dan gebouwd en geïmplementeerd moet worden. De complexiteit van het zorglandschap en het juridische kluwen vormen hierbij de grootste uitdagingen. Tijdens het onderzoek moest ook rekening gehouden worden met de interoperabiliteit van de Vlaamse health data space met de health data spaces van andere Europese lidstaten. Dit onderzoek vertaalt zich naar het beantwoorden van een aantal **onderzoeksdoelstellingen** (zie hoofdstuk 12 Onderzoeksdoelstellingen).

Er werd gekozen om op een pragmatische en agile manier te werk te gaan door te starten vanuit enkele strategisch gekozen use cases en gradueel extra partners toe te voegen. Co-creatie met de betrokken stakeholders stond hierbij centraal om zo tijdig bekommernissen te identificeren en aan te pakken.
Het project beoogde niet alleen een uniforme architectuur en infrastructuur uit te werken, maar ook een duurzaam governance model om het succes van de health data space te garanderen.

3 DATA SPACES

Disclaimer: dit hoofdstuk handelt over data spaces in het algemeen.
Sectorale data spaces, zoals bijvoorbeeld een health data space, zullen hun eigen specificiteiten hebben.

3.1 WAT ZIJN DATA SPACES?

Een data space is een **gedecentraliseerde** infrastructuur
voor **betrouwbaar** delen en uitwisselen van gegevens in data-ecosystemen,
gebaseerd op gemeenschappelijk overeengekomen principes en bouwstenen.

In een data space worden gegevens niet eerst verzameld op een centraal platform voor ze kunnen opgevraagd worden maar blijven ze bij de data holder en is het dankzij gemeenschappelijke afspraken dat een afnemer deze gegevens kan opvragen. Zowel het decentrale als het vertrouwelijke karakter zijn basisbeginselen van een data space.

Data spaces zijn de nieuwste visie op hoe datatransacties kunnen gebeuren op een manier die kwalitatief, betrouwbaar en veilig is, en bovendien schaalbaar, economisch rendabel, maatschappelijk relevant en juridisch rechtvaardig.

Onze maatschappij en economie bouwen in toenemende mate op kennis en inkomsten die volgen uit het genereren, analyseren en delen van gigantische en diverse hoeveelheden data – de ene al waardevoller of gevoeliger dan de andere.

De grote droom van Europa is om met behulp van kennis uit data een beter en duurzamer beleid te kunnen voeren. Ook wil de EU op het vlak van datagedreven toepassingen een eerlijker speelveld creëren door de toegang tot data te democratiseren en een nieuwe balans te creëren in de bijhorende kosten en baten. Dit moet kleinere en opkomende databedrijven **dezelfde kansen** geven als gevestigde spelers om bestaande en nieuwe markten aan te boren – en op die manier ook meer innovatieve toepassingen en businessmodellen laten ontstaan.

Na een decennium waarin beleidsmakers om die redenen publieke open data hebben gepromoot, is duidelijk geworden dat – om tot impactvolle toepassingen te komen – er een noodzaak is om deze te combineren met private data. Dit heeft tot gevolg dat de nodige technische, juridische en economische afspraken moeten toelaten om zowel open als private data decentraal te beheren en toch een vlotte uitwisseling te verzekeren tussen de databron(nen) en de eindgebruiker(s). Denk aan het combineren van (open) data over luchtkwaliteit met (private) data van je navigatiesysteem of fitnessapp. Data spaces faciliteren exact dát.

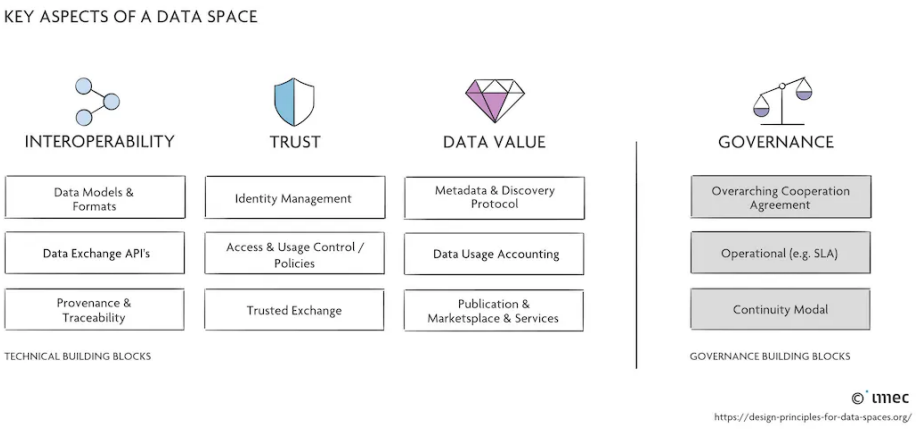
3.2 RANDVOORWAARDEN VOOR DATA SPACES

Tot op zekere hoogte is het delen van gegevens via data spaces vergelijkbaar met het delen van informatie over het internet. Daarbij worden websites over de hele wereld gehost en zijn ze dankzij de nodige standaarden en afspraken toch eenvoudig toegankelijk. Idem voor het delen van documenten via je eigen opslag, waarbij je dankzij de nodige standaarden en toegangsrechten kan beslissen wie er wel en niet bij kan, ook wel **datasoevereiniteit** genoemd.

Meer nog dan in de context van informatie en activiteiten op het internet, is **vertrouwen** een essentieel begrip voor data spaces. Zoals niet zomaar elke app toegang kan krijgen tot je bankgegevens, moet er een universeel systeem komen om in de context van data spaces licenties uit te geven aan betrouwbare partners. En om deze ook weer afdwingbaar te kunnen intrekken bij eventueel misbruik.

Net zoals informatie op het internet enkel vindbaar is omdat er **standaarden** bestaan zoals HTML en **afspraken** zoals domeinnamen, hebben ook data spaces behoefte aan breed gedragen standaarden en afspraken. Die beginnen bij het kwalitatief organiseren, filteren en labelen van data, zodat geïnteresseerden er hun weg in kunnen vinden. Vervolgens zijn afspraken noodzakelijk die de vindbaarheid van data garanderen en hun toegankelijkheid regelen in functie van de eindgebruiker en het doel dat die ermee heeft.

Dit alles moet gepaard gaan met de nodige economische en juridische afspraken die bepalen wie eigenaar is van de data en hoe die kan bepalen aan wie ze gratis of betalend ter beschikking worden gesteld. Zodra die antwoorden duidelijker worden, zal de technische infrastructuur ook daarop voorzien moeten zijn. Doorheen dit alles speelt het vraagstuk wie hier welke rol in moet nemen: de overheid vanuit haar maatschappelijke opdracht versus het bedrijfsleven vanuit de economische vooruitzichten die data spaces openen.



Figuur 1: Technische en governance bouwstenen van een data space

Om aan deze en andere vragen een antwoord te bieden, zijn zowel in Vlaanderen als internationaal heel wat initiatieven hard aan het werk. Vaak vanuit duidelijk gedefinieerde use cases om focus en relevantie te garanderen.

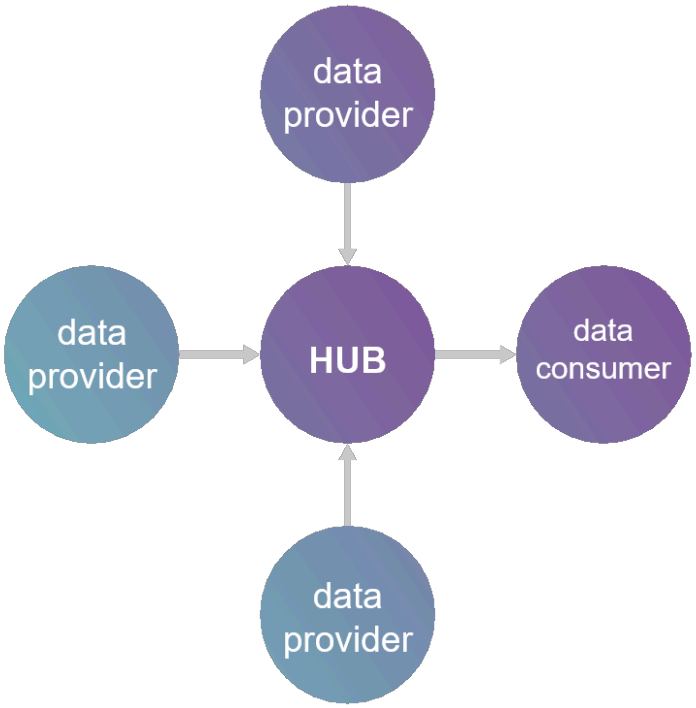
3.3 WAAROM DATA SPACES DE OPLOSSING ZIJN

Data delen bestaat al een tijdje dus men zou zich de vraag kunnen stellen waarom we nu plots nood hebben aan een data space.

Voor bilateraal data delen is geen data space nodig gezien de vereisten zoals de te gebruiken standaarden en de voorwaarden om data te delen kunnen gedefinieerd en gedocumenteerd worden in een contract tussen twee partijen.

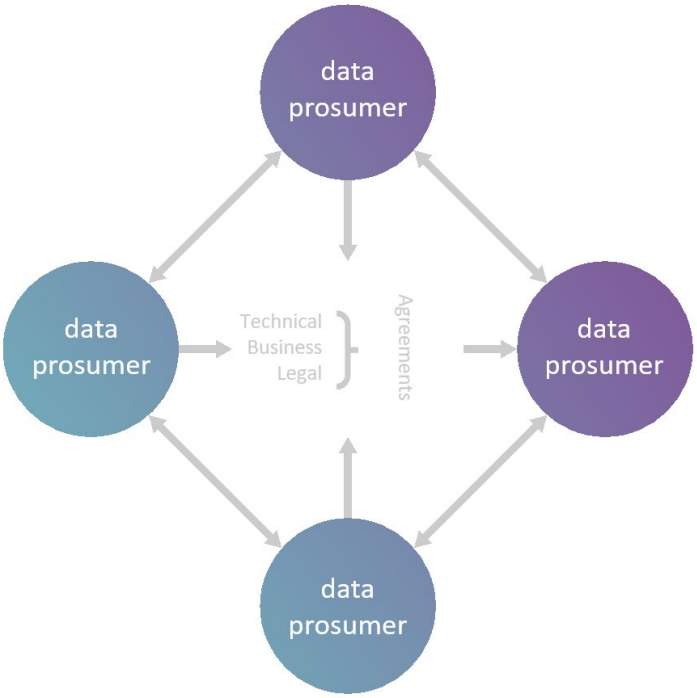
Figuur 2: Bilateraal communicatieschema

Het delen van data wordt een stuk complexer wanneer er meerdere partijen betrokken zijn die data aanbieden en data afnemen. Bilateraal data delen is hier niet meer aan de orde en dit wordt meestal opgelost door het voorzien van een centrale hub. In dit model sturen data aanbieders hun data eerst naar de hub die dienst doet als centrale opslagplaats. Data afnemers kunnen toegang krijgen tot data via deze hub zodat ze geen aparte afspraken moeten aangaan met elke data aanbieder.



Figuur 3: Datahub communicatieschema

Dit is een model dat werkt en ook vaak toegepast wordt. Het heeft echter ook zijn uitdagingen. In dit model wordt de relevante data vaak **gedupliceerd** en **gesynchroniseerd** op een centrale plek waarvoor de toegangsrechten dan voor de deelnemers worden gereguleerd. Dit is niet haalbaar en ook niet wenselijk als je gaat opschalen. Zo zou onnodig veel extra dataopslag nodig zijn, riskeer je **datamonopolies** (zoals je nu al hebt op het internet) en kunnen deze centrale bronnen een grootschalig doelwit vormen voor hackers. Data spaces vermijden al deze nadelen.



Figuur 4: Data space communicatieschema

In essentie zijn data spaces een omgeving waarop leveranciers en gebruikers van data onafhankelijk van elkaar kunnen inpluggen en met elkaar gegevens uitwisselen. Daarbij is het niet noodzakelijk dat ze (telkens) rechtstreeks met elkaar in interactie gaan. Dergelijke flexibiliteit en schaalbaarheid laat op termijn toe om een scala aan nieuwe impactvolle toepassingen te faciliteren die gebaseerd zijn op databronnen vanuit uiteenlopende sectoren. Om die redenen gebeuren momenteel heel wat inspanningen op technisch, juridisch en economisch vlak om data spaces te ontwikkelen en uit te rollen.

3.4 HET INTERNATIONALE, BELGISCHE EN VLAAMSE SPEELVELD ROND DATA SPACES

Uit ons onderzoek blijkt dat de term data space een modewoord is geworden dat te pas en te onpas toegepast wordt op dataplatformen. In realiteit blijkt echter dat een aantal Vlaamse en internationale initiatieven geen echte data spaces zijn zoals ze begrepen worden onder het IDSA framework zoals hieronder beschreven. In die zin zijn enkele premisses van het onderzoeksproject gaandeweg onder druk komen te staan, zoals de wens om optimaal bestaande Vlaamse bouwstenen te hergebruiken.

Heel wat Vlaamse actoren spelen diverse rollen in lokale en internationale initiatieven.
Zo is KU Leuven actief betrokken bij het *Data Spaces Support Centre* (DSSC – cf. infra), en hebben ook organisaties als Agoria programma's en activiteiten gericht op data spaces. Imec heeft, behalve technische inbreng, ook een verbindende rol om als neutrale partij kennis te ontwikkelen en te ontsluiten op Vlaams en internationaal niveau. Om data spaces succesvol te maken, is namelijk een goede orkestratie nodig tussen de verschillende aspecten en verschillende geografische niveaus.

3.4.1 Internationale speelveld

3.4.1.1 IDSA

De International Data Spaces Association[2] (IDSA) heeft een **referentiearchitectuur** en een formele standaard gedefinieerd die moet worden gebruikt voor het maken en beheren van data spaces.
De IDS-architectuur is gebaseerd op algemeen aanvaarde modellen voor gegevensbeheer die veilige uitwisseling en eenvoudige koppeling van gegevens binnen ecosystemen mogelijk maken.

De IDS-architectuur zorgt voor digitale soevereiniteit voor data holders die gegevens beschikbaar stellen voor de uitwisseling of het delen met anderen. Het vormt daarmee de basis voor het ontwikkelen en aanbieden van slimme diensten en voor het opzetten van innovatieve bedrijfsprocessen. Het is net zoals in een *Secure Processing Environment* (SPE) gericht op het creëren van een veilige en vertrouwde ruimte waarin bedrijven hun gegevens soeverein kunnen beheren. Waar een SPE vooral de focus legt op een afgebakende omgeving voor het verwerken van specifieke data ligt de focus hier op gezamenlijk datagebruik en het ontdekken van data.

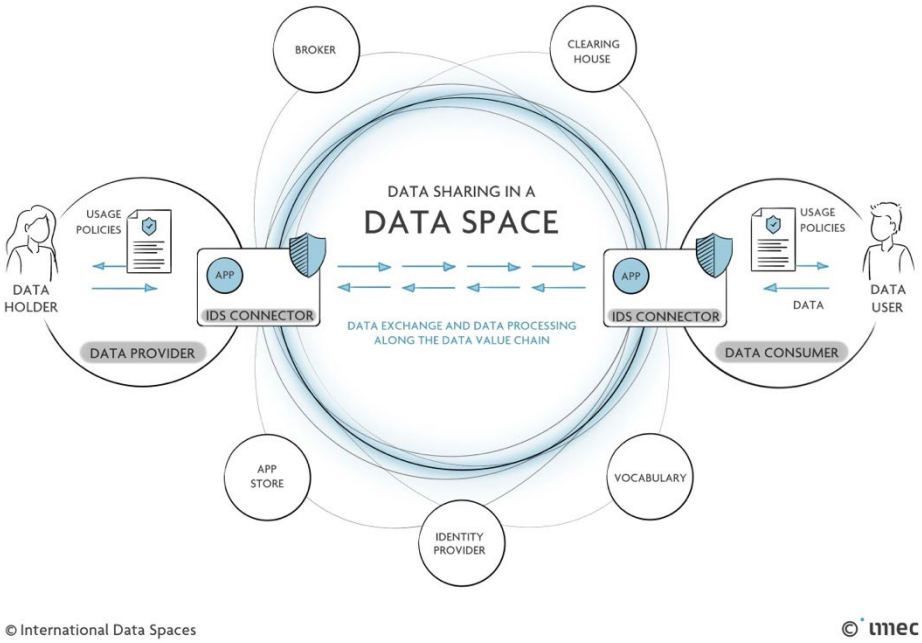
Het design en de implementatie van deze architectuur is op te delen in twee groepen: technische en governance bouwstenen.

3.4.1.2 Technische bouwstenen volgens IDSA

De bouwstenen die onder deze categorie vallen, maken de implementatie van de technische architectuur van een data space mogelijk. Ze omvatten netwerkprotocollen, middleware-componenten, (gestandaardiseerde) data uitwisselingsprocessen en meer, waardoor het delen van gegevens tussen verschillende partijen op een veilige en betrouwbare manier wordt vergemakkelijkt.

Deze componenten bieden een oplossing voor de meeste technische problemen die gepaard gaan met het creëren van data spaces die verband houden met **data-interoperabiliteit** (het uitwisselen van data zonder beperkingen), **datasoevereiniteit** (de controle over eigen data) en **datawaardecreatie** (het zoeken, vinden en effectief gebruiken van de data).

[2] *https://internationaldataspaces.org/*



Figuur 5: De belangrijkste actoren en componenten in een data space volgens IDSA

Door IDSA worden, zoals weergegeven in bovenstaande figuur, een aantal specifieke componenten vermeld die kenmerkend zijn voor een data space:

- **Broker**: Via de broker komt een data space participant te weten welke data er te vinden is, hoe die data er uit ziet en waar de data kan gevonden worden. De broker baseert zich hiervoor op de metadata van alle beschikbare data. Vergelijk het met de rol van een bibliothecaris die perfect weet welke boeken er aanwezig zijn in de bibliotheek.
- **Clearing house**: Een clearing house treedt op als onafhankelijke derde partij bij een datatransactie tussen een provider en consumer. Het heeft de mogelijkheid om een datatransactie al dan niet te laten doorgaan (clearen) op basis van de gemaakte afspraken. Vergelijk het met de rol van een notaris die contracten nakijkt en transacties valideert.
- **Vocabulary**: Opdat de data uitgewisseld door een data provider correct te begrijpen is door een data consumer is het nodig dat ze dezelfde taal spreken. Aan de hand van een vocabulary wordt een bepaalde dataset correct gedefinieerd.
- **Identity provider**: Om het mogelijk te maken aan te geven wie toegang heeft tot welke data is het nodig dat elke partij (provider, consumer) gekend is. Een identity provider biedt een scala aan diensten voor het maken, onderhouden, beheren en valideren van identiteitsinformatie van en voor alle IDS deelnemers en componenten. Vergelijk het met de rol van een politieagent die gaat controlere of elke data space participant wel is wie hij beweert te zijn.
- **Connector**: Een generiek stuk software dat zowel bij de data provider als de data consumer wordt geïnstalleerd en die verbinding kan maken met broker, clearing house en identity provider om data te vinden, te publiceren en data transacties te laten plaatsvinden. Via de connector maakt een stakeholder deel uit van het data space ecosysteem.
- **App store**: Een app store biedt data-apps aan. Dit zijn toepassingen die kunnen worden geïmplementeerd in IDS connectoren om taken zoals transformatie, aggregatie of analyse van de data uit te voeren.

3.4.1.3 Governance bouwstenen volgens IDSA

De bouwstenen die onder deze categorie vallen, hebben betrekking tot **zakelijke overeenkomsten** (voorwaarden die het delen en uitwisselen van gegevens tussen partijen regelen), **operationele overeenkomsten** (regelen het beleid tijdens de uitvoering van data space-operaties) of **organisatorische overeenkomsten** (procedures vastgesteld voor een data space). Deze afspraken worden afgedwongen via wettelijke kaders of via technische bouwstenen.

3.4.1.4 Gaia-X

Een van de belangrijkste data space-initiatieven op Europees vlak is Gaia-X[3]. Dit consortium uit industrie, beleid en onderzoek stelt zich als doel om tegen 2025 data spaces op substantiële schaal **operationeel** te hebben in Europa. Het onderhoudt nauwe banden met de International Data Spaces Association (IDSA), een wereldwijde organisatie van meer dan honderd bedrijven die onder andere verantwoordelijk is voor het bedenken en uitrollen van de International Data Spaces (IDS)-referentie-architectuur en andere afspraken rond vertrouwen en certificering.

Gaia-X is een initiatief dat is opgezet om een betrouwbaar en transparant data-ecosysteem in Europa te creëren. Het is ontworpen om de digitale soevereiniteit van Europa te bevorderen door een gefedereerde data-infrastructuur te bouwen die hoge normen voor gegevensbeveiliging, privacy, en interoperabiliteit naleeft.

Gaia-X faciliteert dit door een raamwerk te bieden voor de opslag en uitwisseling van data waarbij verschillende partijen zoals bedrijven, onderzoeksinstellingen en overheidsorganen betrokken zijn, zonder dat zij de controle over hun gegevens verliezen. Dit moet het mogelijk maken om data en diensten op een veilige, open en transparante manier met elkaar te verbinden, waarbij gebruik wordt gemaakt van bestaande cloudaanbieders en andere dataservices die zich aan de strikte Gaia-X normen houden.

Door middel van een aantal "**lighthouse**" projecten, zoals bijvoorbeeld Health-X dataLOFT (zie sectie 3.4.4.1 Health-X dataLOFT), worden in heel wat sectoren initiële businesscases geïmplementeerd met behulp van het Gaia-x raamwerk. Ze hebben als doel een platform voor gegevensuitwisseling te creëren dat is gebaseerd op transparantie, vertrouwen en openheid. Ze richten zich op meerdere industrieën en helpen om een samenhangend ecosysteem voor data-infrastructuur te creëren. Deze eerste businesscases zijn de koplopers bij de implementatie van het Gaia-X-raamwerk dat ook een uitgebreide pijplijn van toekomstige "lighthouse" projecten mogelijk zal maken.

Naast de "lighthouse" projecten zijn er ook data space projecten die Gaia-x conform willen zijn zoals bijvoorbeeld Dataspace4Health uit Luxemburg (zie sectie 3.4.4.2 Dataspace4Health).

3.4.1.5 Data Spaces Support Center (DSSC)

Sinds eind 2022 is er – met financiële steun van de Europese Commissie – ook een Data Spaces Support Center[4] (DSSC). Dit neemt een coördinerende rol op om de behoeftes vanuit de verschillende sectoren in kaart te brengen en bestaande initiatieven op elkaar af te stemmen. De organisatie draagt – mede dankzij een door hen ontwikkelde '**starterskit'** – ook bij aan de kennisdeling over data spaces en heeft ook een sleutelrol in de ontwikkeling van het Europees beleid en regelgeving.

[3] https://gaia-x.eu/

[4] https://dssc.eu/

Het Data Spaces Support Center (DSSC) werkt verschillende hulpmiddelen uit om de implementatie en het beheer van data space-oplossingen te vergemakkelijken. Enkele van deze hulpmiddelen omvatten:

> **Technische richtlijnen en standaarden**: het DSSC ontwikkelt gedetailleerde technische richtlijnen die beschrijven hoe data spaces moeten worden opgezet, beheerd en geïntegreerd. Dit omvat specificaties voor interoperabiliteit, data-uitwisselingsprotocollen, en beveiligingsmaatregelen.
> **Best practices en case studies**: door het verzamelen en delen van best practices en succesvolle case studies helpt het DSSC organisaties om te leren van bestaande implementaties. Dit kan organisaties helpen om veelvoorkomende valkuilen te vermijden en sneller effectieve data space-oplossingen te ontwikkelen.
> **Trainingsmateriaal en workshops**: de DSSC biedt educatief materiaal en organiseert workshops om stakeholders te trainen in de vaardigheden die nodig zijn voor het ontwikkelen en beheren van data spaces. Deze trainingen kunnen variëren van technische diepgaande sessies tot algemene inleidingen in het concept van data spaces.
> **Tools voor data governance**: om te waarborgen dat data binnen data space-oplossingen op een ethische en conforme manier wordt beheerd, ontwikkelt het DSSC tools en frameworks voor data governance. Dit omvat hulpmiddelen voor het beheren van data-toegang, data-auditing en naleving van wetgeving.
> **Samenwerkingsplatformen**: het DSSC stelt platformen beschikbaar die samenwerking en kennisuitwisseling tussen verschillende data space-gebruikers en -aanbieders vergemakkelijken. Deze platformen kunnen forums, online communities of gezamenlijke werkruimtes omvatten.

Het centrum onderhoudt ook een Data Spaces Radar[5] die een overzicht biedt van bestaande data space initiatieven in verschillende sectoren en stadia van ontwikkeling.

3.4.1.6 SIMPL-project

Als belangrijk element bij de uitvoering van haar datastrategie wil de Europese Commissie een Smart middleware-platform (bijgenaamd SIMPL[6]) ontwikkelen. Zo'n middleware zou cloud-to-edge-federaties mogelijk moeten maken en grote door de Europese Commissie gefinancierde data-initiatieven ondersteunen, zoals de Europese data spaces. Na een openbare aanbesteding werd de ontwikkeling van dit platform toegekend aan een consortium bestaande uit Eviden Belgium, Aruba (IT), Capgemini Nederland (NL), Engineering International Belgium (BE), IONOS (DE), and COSMOTE Global Solutions (BE).

De bedoeling is dat dit consortium de **basiscomponenten** voor een data space infrastructuur ontwikkelt. Tegen de zomer van 2024 had een eerste proof of concept voltooid moeten zijn. Vermoedelijk liep het project vertraging op. De ontwikkelingsstatus kan op de projectwebsite[7] opgevolgd worden.

Voor dit project kwam de ontwikkeling van deze bouwstenen te laat. Volgens de richtlijnen van de Europese Commissie zouden de SIMPL-componenten interoperabel moeten zijn met de meest gangbare data space componenten op de markt.

[5] *https://www.dataspaces-radar.org/radar/*

[6] *https://simpl-programme.ec.europa.eu/*

[7] *https://simpl-programme.ec.europa.eu/dashboard/development*

3.4.1.7 Catena-X

Catena-X[8] is het eerste collaboratieve en open data-ecosysteem voor de auto-industrie van de toekomst. Het is bovendien de eerste geoperationaliseerde data space binnen Europa. De toegevoegde waarde is dat alle partners in de waardeketen kunnen samenwerken en tegelijkertijd de volledige soevereiniteit over hun eigen gegevens behouden. Elke partner krijgt een digitale sleutel tot de gegevens die voor die partner relevant zijn.

Voorheen gebruikten veel partners veel op zichzelf staande situaties in deze context, terwijl Catena-X een gedeelde oplossing creëert voor alle belanghebbenden, of het nu gaat om automotive, IT of onderzoek. Ontwikkelingskosten worden verdeeld over de partijen en de open source-structuur maakt het mogelijk om op elk moment software-elementen toe te voegen.

De leden zijn onder meer BMW, Mercedes-Benz, Volkswagen-Bosch, BASF en SAP, evenals grote bedrijven uit de VS, China en Japan.

3.4.2 Belgische speelveld

3.4.2.1 HDA

Het Belgisch Gezondheids(zorg)Data-Agentschap[9] (GDA) of ook wel Health Data Agency (HDA) genoemd, streeft naar een kwaliteitsvol, datagedreven gezondheidszorgsysteem, waar gezondheids(zorg)gegevens en gezondheids(zorg)gerelateerde gegevens, op een uniforme, transparante en veilige manier beschikbaar zijn voor secundair gebruik. Hierbij richt de HDA zich op volgende doelstellingen:

- Het **faciliteren** van de **beschikbaarheid** van de gezondheids(zorg) gegevens en gezondheids(zorg) gerelateerde gegevens;
- Het **ontwikkelen** van veilige en betrouwbare **methodes** om persoonlijke gezondheidsgegevens uit te wisselen, met aandacht voor cybersecurity;
- Het **ontwikkelen** en het implementeren van een **beleidsstrategie** met betrekking tot gezondheids(zorg)gegevens en gezondheids(zorg) gerelateerde gegevens;
- Het **stimuleren** van **innovatie**, wetenschappelijk **onderzoek** en beleidsondersteunend onderzoek die kunnen bijdragen tot een hogere kwaliteit, betaalbare, preventieve en doelgerichte gezondheidszorg.
- Het **vertrouwen** van burgers en patiënten wordt gewaarborgd door de nadruk te leggen op transparantie en veiligheid rond het hergebruik van gezondheidsgegevens, waarbij de rechten en plichten van de betrokken partijen worden gerespecteerd.

In het evoluerende digitale landschap kan de HDA een belangrijke rol spelen voor België. Het operationele kader van de HDA is bewust ontworpen om te voldoen aan de EHDS en toekomstige initiatieven, en Europese wettelijke vereisten. Vanuit een interfederaal standpunt werkt de HDA samen met het Belgische gezondheids(zorg)ecosysteem om grensoverschrijdende samenwerking te bevorderen.

Het verlenen van controle aan individuen over hun elektronische gezondheidsgegevens komt overeen met het streven van de HDA naar privacy. Door betrouwbaar en veilig gegevensgebruik voor onderzoekers, innovators en beleidsmakers te faciliteren, dragen zowel EHDS als de HDA significant bij aan de visie van een samenhangend en geavanceerd Europees gezondheidsecosysteem.

[8] https://catena-x.net/en/
[9] https://www.hda.belgium.be/nl

De HDA stelt een aantal diensten ter beschikking om deze doelstellingen te realiseren:

> **Gegevencataloog**[10]: De gegevenscataloog is een gecentraliseerde inventaris die metagegevens en informatie over Belgische gezondheidsdatasets opslaat. Het stelt gebruikers in staat om relevante datasets te ontdekken, begrijpen en mogelijk toegang te krijgen. De gegevenscataloog bevordert het delen, vinden en combineren van gezondheidsgegevens.
> **Gegevensaanvraag**[11]**:** Indien een gewenste dataset gevonden werd in de gevenscataloog kan hier toegang tot gevraagd worden.
> **Projectfinanciering**[12]**:** Ook andere projecten die op een innovatieve manier bijdragen aan het hergebruik van gezondheidsdata kunnen beroep doen op de HDA.

3.4.3 Vlaamse speelveld

3.4.3.1 Athumi

Op Vlaams niveau is een belangrijke rol weggelegd voor het recent opgerichte Datanutsbedrijf Athumi[13]. Deze organisatie heeft als wettelijke opdracht om persoonsgegevens en gevoelige bedrijfsdata slim en veilig te verwerken, met behoud van volledige **controle** en **transparantie** voor wie data via de diensten van Athumi en haar partners deelt. Hiervoor ontwikkelt Athumi ecosystemen en bouwt het dataplatformen. Vergelijk het met de aanleg en onderhoud van (snel)wegen voor personen- en vrachtvervoer.
Voor Athumi lijkt dan ook een belangrijke rol weggelegd te zijn in de context van sectorale data spaces.

Aangezien Athumi ook actief is in de health sector, werd eind 2023 voorgenomen om een gemeenschappelijke technische roadmap op te stellen voor de PoC's in het kader van dit onderzoeksproject. Zeker wat betreft de clearing house component leek Athumi een goede partner te zijn aangezien zij al over een clearing house (gebouwd door Eviden) beschikten.

Om te voldoen aan de voorwaarden voor een clearing house component, bruikbaar binnen dit project, was het nodig dat een minimaal aantal clearing acties, zoals beschreven door IDSA, werden ondersteund:

> Het verifiëren van contract of overeenkomst vooraleer de transactie plaatsvindt
> Het monitoren en loggen tijdens een transactie
> Het delen van gegevens na het plaatsvinden van de transactie.

Dit wil onrechtstreeks ook zeggen dat een clearing house component zoals beschreven door IDSA de beslissing kan maken om een transactie al dan niet te laten plaatsvinden op basis van de bestaande voorwaarden.

Uit nadere analyse bleek echter dat dit clearing house van Athumi vooral een facturatiesysteem is en dus in zijn huidige vorm niet inzetbaar is voor een health data space. Op korte termijn heeft Athumi ook niet de ambitie om zijn clearing house uit te breiden met de functionaliteiten van een clearing house zoals beschreven door de IDSA.

[10] https://catalog.hda.belgium.be/

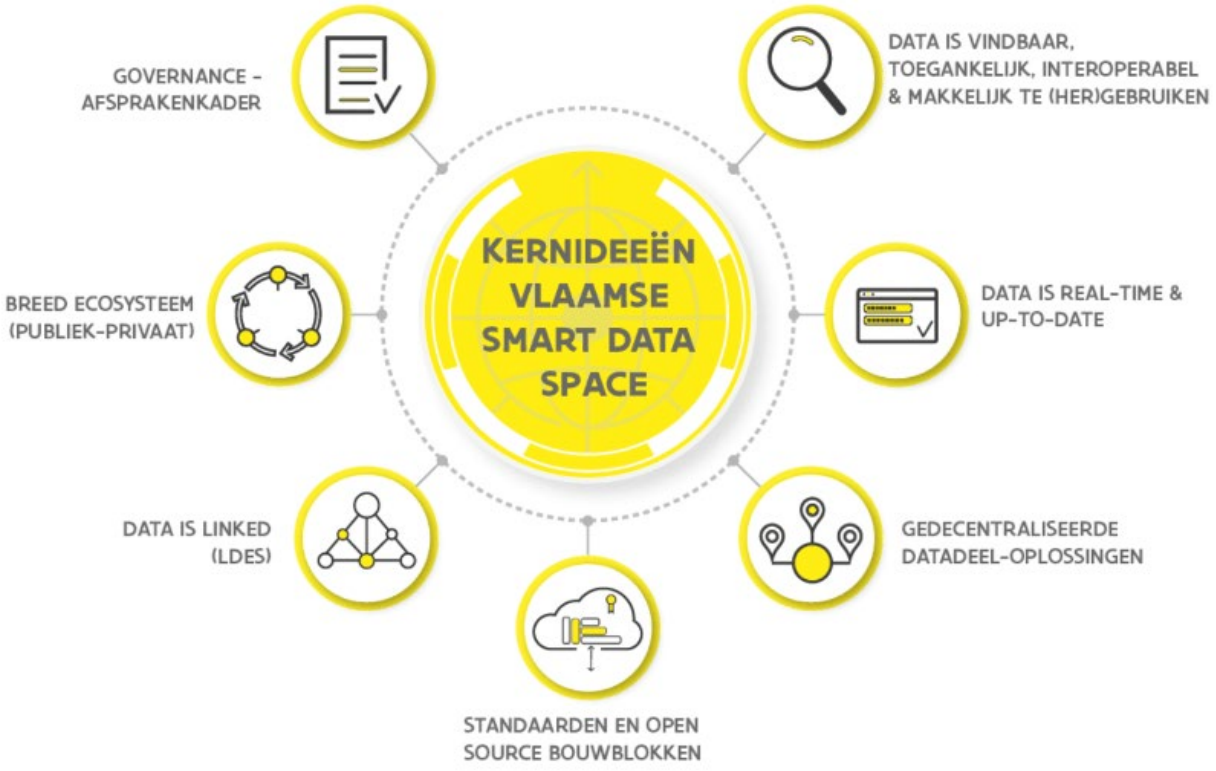
[11] https://www.hda.belgium.be/nl/data_request

[12] https://www.hda.belgium.be/nl/diensten/financiering-van-innovatieprojecten

[13] https://athumi.be/

3.4.3.2 Digitaal Vlaanderen en de Vlaamse Smart Data Space

Daarnaast is er de Vlaamse Smart Data Space[14] (VSDS), een door Vlaanderen opgezet initiatief om alle **bouwstenen** te creëren die toelaten om Vlaamse (open) basisdata en (publieke of private) data op een gestandaardiseerde manier en volgens de principes van data spaces te publiceren en te gebruiken.
In de kern bestaat het VSDS-consortium uit vier partijen: Digitaal Vlaanderen, imec en de bedrijven DXC.technology en Cegeka. De VSDS beoogt compatibel te zijn met het IDSA-model voor data spaces.



Figuur 6: Kernideeën VSDS

De Vlaamse Smart Data Space zet in op het vindbaar, toegankelijk en makkelijk (her)bruikbaar maken van data, kortom duurzaam datadelen. Dit door technische standaarden en bouwblokken te ontwerpen, en daar een afsprakenkader rond te voorzien dat het vertrouwen tussen de partijen bevordert.

De Vlaamse Smart Data Space zorgt zo voor een standaardisering van de data-integratie. Dat wil zeggen dat ernaar gestreefd wordt om het maatwerk dat bij data-uitwisseling komt kijken, zo veel mogelijk te beperken. Zo kan elke partij in het ecosysteem zich op zijn kerntaken (datakwaliteit, inzichten halen uit de data, nieuwe toepassingen ...) focussen bij het uitwisselen van data. Op basis van goeie afspraken en de principes van Linked Data kan eenzelfde databron ingezet worden voor meerdere use cases of meerdere doeleinden. Zo genereert de data de best mogelijke inzichten voor elke partij.

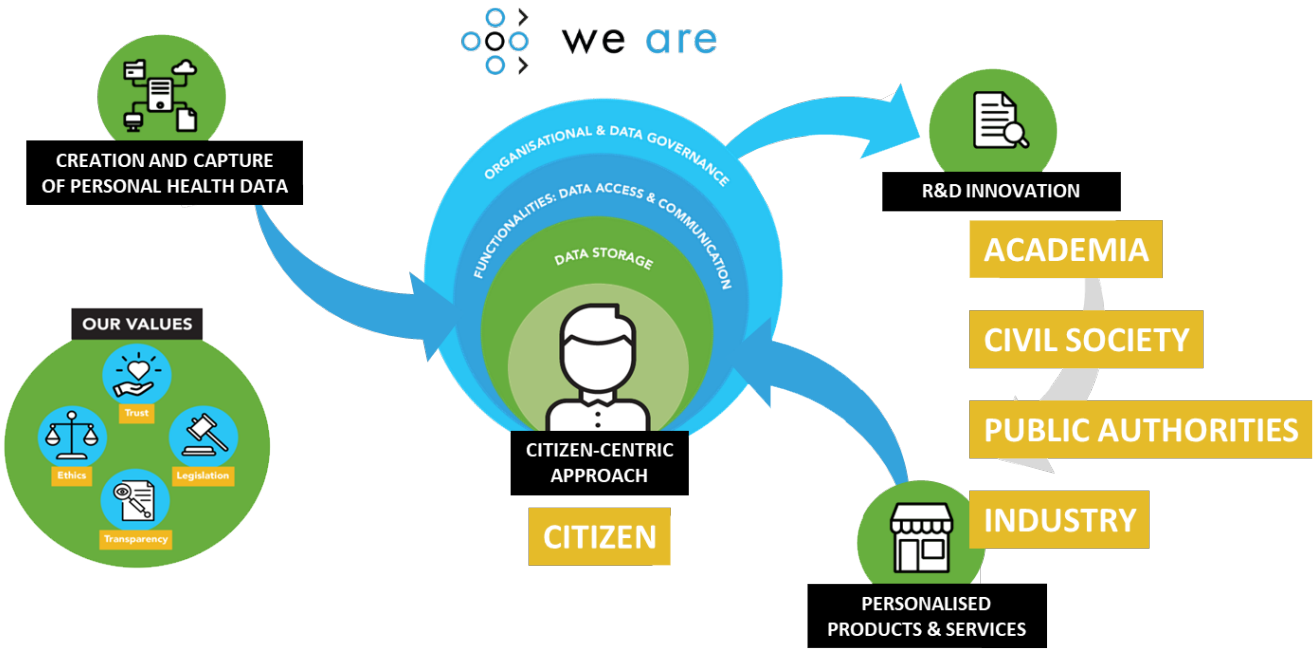
Voor deze data standaardisatie wordt gebruik gemaakt van de LDES technologie. LDES staat voor Linked Data Event Streams en zorgt naast standaardisatie voor een efficiëntere replicatie en synchronisatie van databronnen. Dit impliceert dat om gebruik te kunnen maken van de VSDS-bouwblokken een databron eerst dient omgezet te worden naar het LDES formaat.

[14] *https://www.vlaanderen.be/digitaal-vlaanderen/onze-oplossingen/vlaamse-smart-data-space*

3.4.3.3 We Are

Het We Are-project[15] is een samenwerking tussen Domus Medica, Koning Boudewijnstichting, VITO, Vlaams patiëntenplatform VZW en Zorgnet Icuro. We Are wil burgers eigenaarschap geven over hun eigen gezondheidsdata via een ecosysteem van **persoonlijke datakluizen**. Hiervoor wordt gebruikgemaakt van de Solidkluizen van Athumi. De burger kan zelf kiezen welke gegevens uit de pod gebruikt mogen worden en door wie. Het doel van We Are is om het vertrouwen van burgers in datadeling te vergroten, waardoor ze hun gezondheidsdata niet alleen delen met dienstverleners, maar deze ook ter beschikking stellen voor secundair gebruik (onderzoek).

Hoewel het We Are-ecosysteem elementen bevat die overeenkomen met de principes van data spaces, zoals data-soevereiniteit en beveiliging, is het niet opgezet als een open, federatief netwerk voor data-uitwisseling tussen meerdere organisaties, zoals gedefinieerd door de IDSA. Het We Are dataplatform is dus geen data space, maar heeft wel gelijkaardige ambities in het toegankelijker maken van data voor innovatie en onderzoek.



Figuur 7: We Are-ecosyteem

3.4.4 Data spaces in het domein van de gezondheidszorg

3.4.4.1 Health-X dataLOFT

Health-X dataLOFT[16] heeft als doel een gelegitimeerd, open gefinancierd platform te implementeren, gebaseerd op Gaia-x normen die gezondheidsgegevens van burgers bevat en deze kan toegankelijk maken volgens de voorwaarden zoals door de burgers zelf zijn opgelegd of met andere woorden datasoevereiniteit implementeert.

In tegenstelling tot bestaande diensten zal de Health-X dataLOFT dataruimte dus **burgergericht** zijn: burgers zullen toegang hebben tot en controle hebben over hun persoonlijke gezondheidsgegevens, ongeacht de oorsprong ervan. Op deze manier kunnen deze gegevens beschikbaar worden gesteld voor

[15] https://we-are-health.be/nl

[16] https://www.health-x.org/home

persoonlijke gezondheidsproblemen, medische zorg en onderzoek op basis van de rechten die burgers/patiënten hiervoor zelf toekennen.

Als aanvulling op het bestaande klassieke aanbod in leveranciersgebonden silo's, wordt een leveranciersonafhankelijk platform ontwikkeld om toegang tot en integratie van gegevens uit de eerste en tweede zorgmarkt mogelijk te maken. Dit platform maakt nieuwe gebruiksbenaderingen en bedrijfsmodellen mogelijk voor fabrikanten van hulpmiddelen, serviceproviders en klinische aanbieders. Dit nieuwe ecosysteem is open, gefedereerd en gebaseerd op de standaarden die zijn ontwikkeld in het kader van het Gaia-X-project.

Concreet baseert het Health-x project zich eveneens op de EHDS regulatie en hebben ze een model uitgewerkt dat de EHDS mapt op de Duitse gezondheidssector via een eigen Health-x ecosysteem. Verder is het project aan de slag gegaan op basis van vier verschillende use cases waaronder een use case rond borstkanker en endometriose. Binnen deze use cases is eveneens aan de slag gegaan met data space connectoren en werd een prototype ontwikkeld voor een consent manager.

Health-x dataLOFT is een project gefinancierd door de Duitse overheid voor economische aangelegenheden en klimaatbescherming. Het bestaat uit 9 werkpakketten[17] die verbonden zijn aan 14 mijlpalen[18].
Het project loopt van Q2 2022 tot Q2 2025.

3.4.4.2 Dataspace4Health

Dataspace4Health[19] (DS4H) is een samenwerking tussen NTT DATA, Hôpitaux Robert Schuman, het Luxembourg Institute of Health, de Universiteit van Luxemburg, Agence eSanté en de Luxemburgse nationale datadienst. Het project heeft tot doel een gezondheids data space op te bouwen door verschillende belanghebbenden uit het **zorgecosysteem** met elkaar te verbinden.

Door het creëren van een veilige gezondheidsdata space met Gaia-X-conforme diensten, wil het project nieuwe zorgdiensten mogelijk maken en de patiëntresultaten verbeteren, door veilige gezondheidsgegevens aan onderzoekers aan te bieden met behoud van gegevenseigendom en privacy. DS4H is gebaseerd op de EU Strategy for Data en het Gaia-X initiatief voor een gefedereerde en veilige data-infrastructuur.
Het project zal meerdere aspecten op verschillende niveaus aanpakken, waaronder zakelijke, juridische en technische aspecten. Dit initiatief is een innovatieve stap in de richting van de digitale transformatie van de zorgsector in Luxemburg en Europa.

Het project is ingegeven door de behoefte aan een nieuwe aanpak voor het delen van gezondheidsgegevens die de GDPR en de rechten van patiënten respecteert. Momenteel zijn gezondheidsgegevens vaak in silo's, gefragmenteerd en onderbenut, wat het potentieel voor innovatie en onderzoek beperkt. Het project zal onderzoeken hoe Gaia-X kan worden gebruikt als een Europees raamwerk voor dataruimtes dat gegevensbescherming, -beveiliging en -interoperabiliteit waarborgt. Dataspace4Health zal ook de voordelen van datagestuurde innovatie en AI voor gezondheidszorg en onderzoek demonstreren, zoals het verbeteren van diagnose, behandeling en preventie van ziekten, het verbeteren van patiëntresultaten en kwaliteit van leven, en het bevorderen van wetenschappelijke kennis en ontdekkingen.

Dataspace4Health is een project gefinancierd door de Luxemburgse ministerie voor economie. Het project loopt van maart 2024 tot maart 2026.

[17] https://www.health-x.org/arbeitspakete

[18] https://www.health-x.org/meilensteine

[19] https://www.dataspace4health.lu/

4 BEHOEFTEANALYSE VLAAMSE HEALTH DATA SPACE (BUSINESS CONTEXT)

4.1 BEHOEFTEANALYSE TEMPLATE EN TOPIC GUIDE

4.1.1 Stakeholder identificatie

In dit eerste deel van de behoefteanalyse hebben we de verschillende stakeholders geïdentificeerd die ons informatie en feedback hebben verstrekt over de opzet en het gebruik van de Health Data Space.
De meeste, zo niet alle, resultaten van deze behoefteanalyse zijn gebaseerd op interviews en interacties met deze stakeholders. Deze stakeholders zijn niet alleen geselecteerd voor de behoefteanalyse, maar hebben ons ook waardevolle informatie geleverd voor een positioneringsoefening en dienden als basis voor het opstellen van de 'go-to-market' analyse.

4.1.1.1 Identificatie plan

Bij het identificeren van stakeholders zijn we niet blind te werk gegaan. Ons doel was om een brede waaier van organisaties binnen het gezondheidszorglandschap van België te bestrijken. Het is belangrijk op te merken dat de potentiële stakeholders voor dit onderzoek vrijwel oneindig zijn. Niet alleen stakeholders binnen de gezondheidszorg kunnen waarde toevoegen aan het project, maar ook stakeholders uit andere sectoren, zoals milieu, verkeer en overheid, kunnen van belang zijn. Tijdens het onderzoek hebben we ons aanvankelijk gefocust op stakeholders binnen de gezondheidszorg, en later zijn we meer naar stakeholders buiten deze sector gaan kijken. Uiteraard blijft het mogelijk om in de toekomst nog meer stakeholders uit verschillende sectoren te betrekken.

Aangezien het governance- en technische onderzoek eerder is gestart dan het business-onderzoek (zie hoofdstuk 7 Governance en hoofdstuk 8 Architectuur), hoefden we niet vanaf nul te beginnen.
We konden gebruikmaken van de reeds geïdentificeerde stakeholders en de meest relevante selecteren voor deze analyse. Waar er leemtes waren en geen stakeholders konden worden geïdentificeerd, zijn we actief op zoek gegaan naar nieuwe stakeholders binnen het veld.
Hier hebben we een lijst van stakeholders die we bevraagd hebben omtrent de behoefteanalyse:

- eHealth
- FarmaFlux
- Statbel
- RIZIV-INAMI
- Sciensano – Healthdata.be

De lijst met potentiële stakeholders is natuurlijk veel te lang om hier op te lijsten. Daarom geven we vier verschillende categorieën van zorgactoren waarin we het landschap kunnen onder verdelen. Deze kunnen later verder betrokken worden in een vervolgtraject.

> Industrie
  - Gericht op farmacie
> Software- en hardware gericht (bv. Corilus)
> Overheid (focus op gezondheid en datadeling)
  - Federaal
  - Vlaams
  - Brussel
  - Waals

> Algemene actoren gezondheidszorg
> Onderzoek
    - Laboratoria
    - Universiteiten

4.1.2 Behoeften bevragen

In deze stap hebben we informatie, verwachtingen en meningen verzameld over de implementatie en operationalisering van een Health Data Space binnen de Belgische grenzen. We hebben ons gebaseerd op de stakeholdermatrix uit de identificatiestap. De informatie is verzameld via individuele interviews met verschillende stakeholders. In sommige gevallen werd dit vervangen door een reeks kleinere vergaderingen vanwege andere afhankelijkheden die gelijktijdige communicatie vereisten.

De manier waarop we de verzameling van de behoeften hebben aangepakt, is onderverdeeld in drie fasen. In dit hoofdstuk bespreken we alle drie de fasen, hun input en output, en de uitvoering. We moeten wel vermelden dat deze fase aanzienlijke overlap vertoont met het governance-traject. Vanuit governance-perspectief zijn veel interviews gehouden met verschillende organisaties. De resultaten van deze interviews waren ook waardevol voor de behoefteanalyse, of ze nu vanuit een business- of governance-perspectief plaatsvonden.

4.1.2.1 Contacteren en informeren

Door de combinatie van technische complexiteit en strategische planning hebben we bij het contacteren van de geselecteerde organisaties de focus gelegd op het zoeken van de juiste contactpersoon.
Ter voorbereiding van het interview stuurden we eerst een korte introductie presentatie.
Deze presentatie bood een basis van informatie over de volgende onderwerpen:

> Wat is een data space? (business en technisch)
> Voor- en nadelen van een data space
> European Health Data Space ecosysteem
> Ons project
> Wat betekent dit voor jou? (en jouw organisatie)

Voor de intropresentatie van de behoefteanalyse-interviews zie bijlage 4.A

4.1.2.2 Bevragen en verduidelijken

Tijdens het interview gingen we over naar de tweede fase. In deze fase controleerden we of de geïnterviewde alle informatie uit de introductiepresentatie had begrepen. Als dat het geval was, konden we ons meteen richten op het stellen van vragen in plaats van het uitleggen van bepaalde onderwerpen.
Alle vragen waren opgesteld door het onderzoeksteam en samengevoegd in een topicgids. Deze gids was gebaseerd op de governance-topicgids (zie bijlage 7.B), maar richtte zich meer op business, positionering en participatie.

Het sjabloon bestond uit drie delen:

> Gegevensbeheer en het delen van gegevens
> Mening over data spaces
> Wat als jouw organisatie deel uitmaakt van de data space?

Voor de topicgids met vragen voor de behoefteanalyse interviews zie bijlage 4.B

In sommige gevallen was de organisatie zeer uniek wat betreft haar positie en/of activiteiten binnen de gezondheidszorgsector, zoals in het geval van eHealth. Deze interviews vereisten een meer op maat gemaakte vragenlijst. Als de geïnterviewden niet alles uit de introductiepresentatie hadden begrepen of aanvullende vragen hadden, gingen we dieper in op de informatie uit de presentatie. Meestal veranderde dit de opzet van het interview. In plaats van de vragen te volgen volgens de volgorde van de topicgids, legden we de presentatie uit en stelden we vragen tijdens het verduidelijkingsproces. Als sommige vragen niet beantwoord konden worden, vroegen we de geïnterviewde ons door te verwijzen naar een collega die wel over de benodigde informatie beschikte. Last but not least, tijdens de interviews keken we niet alleen naar de verbale respons, maar ook naar hoe gemotiveerd en enthousiast de geïnterviewde en de organisatie waren ten aanzien van health data spaces.

4.1.2.3 Samenvatten en opvolgen

Na het gesprek stuurden we altijd een follow-up e-mail waarin we vroegen om feedback over verschillende onderwerpen, zoals:

> De vorm van het interview
> De overdracht van informatie
> Eventuele vragen die er nog restten bij de geïnterviewde
> ...

Daarnaast gaven we aan het einde van het interview informatie over mogelijke vervolgstappen. Dit kon betrekking hebben op vervolgafspraken of de transcriptie van het vorige interview. Het recap- en follow-upgedeelte was niet verplicht. Als organisaties ervoor kozen om niet te reageren op deze communicatie, stuurden we geen herinneringen en drongen we niet aan op een antwoord.

4.2 HUIDIGE EN IDEALE (TOEKOMSTIGE) SITUATIE

4.2.1 Intro

In deze stap werden de behoeften voor de Health Data Space geanalyseerd en gedocumenteerd.
Op basis van de informatie die tijdens de interviews was verzameld, werd een lijst met behoeften opgesteld (zie 4.3.1 Gap analyse). Dit document onthult de essentiële vereisten die nodig zijn om een waardevolle Health Data Space te creëren.
De combinatie van de resultaten van de positioneringsoefening, de visieverklaring en de go-to-marketstrategie kan dienen als startpunt voor de zakelijke kant van het implementatieproject.

4.2.2 Strategie

De strategie die we hebben gebruikt, is de gap-analyse. Dit type analyse bestaat uit drie delen.
Eerst werd de huidige situatie blootgelegd en beschreven. Dit kon op basis van verschillende onderwerpen, zoals gegevensuitwisseling, huidige technische architecturen en huidig gebruik van gegevens.

Na de huidige situatie werd de toekomstige situatie beschreven. Deze werd gevormd door de verwachtingen en behoeften van stakeholders te verzamelen. De verwachtingen waren gericht op processen op bedrijfsniveau, zodat ze niet beperkt zouden worden door technische of architecturale beperkingen, tenzij de verwachting specifiek van technische of architecturale aard was. In dat geval moest de verwachting gekoppeld worden aan aspecten van gegevensverzameling of -uitwisseling om de waarde voor het project te waarborgen.

De volgende stap was het analyseren van de kloof. Hierbij combineerden we de huidige en toekomstige situatie om grote verschillen te identificeren. Deze verschillen konden worden omgezet in officiële vereisten voor de Health Data Space.

Om de behoefteanalyse af te ronden, hebben we een extra rubriek toegevoegd met een aantal aanvullende behoeften. Deze kunnen in de toekomst worden toegevoegd om de waarde van de Health Data Space verder te verhogen, maar zijn niet essentieel voor het functioneren van de data space.

4.2.3 Huidige staat

Op het moment van de behoefteanalyse is er nog geen Health Data Space actief. Er zijn echter wel enkele onderwerpen die we nader kunnen onderzoeken om beter inzicht te krijgen in hoe gegevens momenteel worden gebruikt en gedeeld.

4.2.3.1 Gegevens delen

De manier waarop gegevens momenteel worden gedeeld, is zeer gefragmenteerd. Ten eerste zijn er meerdere structuren voor gegevensoverdracht: de twee meest voorkomende zijn bilaterale communicatie en communicatie via een gecentraliseerde hub. Meer informatie hierover vind je in hoofdstuk 3.3 Waarom data spaces de oplossing zijn.

Bij bilateraal delen beperk je jezelf tot één consument met wie je wil communiceren. Als je dezelfde data met verschillende consumenten wilt delen, moet je voor elk van hen een volledig nieuw proces opstarten; dit geldt zowel op technisch, governance- als businessniveau. Kies je voor het hub-spoke model, dan vereist dit veel inspanning, vertrouwen en financiële middelen om een veilige en gecentraliseerde hub te creëren en te onderhouden.

Wanneer we dit alles combineren met het feit dat we werken met gevoelige medische gegevens, ontstaat er een complex, gefragmenteerd landschap van gezondheidsdata, met veel vragen, wantrouwen en risico's op het gebied van beveiliging. Bij de gemiddelde speler in de gezondheidszorg zien we dat gebruik wordt gemaakt van een combinatie van meerdere structuren voor gegevensoverdracht binnen de organisatie.

Naast de verschillende manieren om data te delen, moeten we ook rekening houden met data analytics [20] en de combinatie van verschillende datasets om nieuwe inzichten te ontdekken. Momenteel is de enige mogelijkheid een opstelling met een datahub, waarbij data centraal in bulk wordt gekopieerd naar één plek. Pas als alle data centraal is opgeslagen, kan er gekeken worden naar verschillende combinatiemogelijkheden. Het gevaar hierbij is dat er uiteindelijk veel data wordt gedeeld, maar slechts een fractie daarvan daadwerkelijk wordt gebruikt.

4.2.3.2 Technisch

Er zijn veel verschillende technische manieren om gegevens te delen, elk met hun eigen voor- en nadelen, zoals het gebruik van API's, SFTP, gegevensoverdracht in de cloud, enzovoort. Momenteel is het gebruik van deze technologieën gebaseerd op een afweging tussen efficiëntie en financiële middelen.

> Wat is de 'beste' of 'meest efficiënte' manier om gegevens te delen?
> Hoeveel financiële en technische middelen hebben we om deze gegevens te delen?

[20] *Qlik Data Sience vs Data Analytics https://www.qlik.com/us/data-analytics/data-science-vs-data-analytics [Laatst geraadpleegd op 16/12/2024]*

De combinatie van de antwoorden op deze vragen bepaalt hoe de gegevens worden gedeeld.
Dit denkproces is logisch: het is een afweging tussen het gebruik van de beste tool voor de taak en het minimaliseren van het aantal verschillende tools om de complexiteit laag te houden. Naast de verschillende technische manieren om gegevens te delen, zijn er ook de 'datastandaarden'. Er worden momenteel meer dan 70 verschillende datastandaarden (zie 8.5 Datastandaarden en Bijlage 8.C) gebruikt in het gezondheidsecosysteem om gegevens met elkaar te delen.

> *"Een datastandaard is een type standaard, die een overeengekomen benadering is om een consistente meting, kwalificatie of uitwisseling van een object, proces of eenheid van informatie mogelijk te maken." - Network of the National Library of Medicine*[21]

4.2.3.3 Governance

Binnen het huidige ecosysteem voor gezondheidsgegevens zijn vertrouwen en beveiliging zeer belangrijke begrippen. Om deze voorwaarden te waarborgen, worden governance aspecten toegepast bij het delen van gezondheidsgegevens. Zo zijn er verschillende organisaties die bepaalde governance aspecten coveren. Zo voorziet bijvoorbeeld het IVC entiteiten van een gegevens vergunning, E-health zorgt voor o.a. pseudonimisatie en healthdata.be heeft o.a. een SPE die gebruikt kan worden.

Naast de verschillende organisatie worden er contracten opgesteld tussen de verschillende partijen die gegevens delen. Deze contracten zijn echter niet ingebouwd in de technische kant van de gegevens-overdracht en zijn daarom moeilijk automatisch te controleren. Er is geen echt proces opgezet voor organisaties om contracten te formaliseren wanneer ze gegevens willen delen. Mocht er sprake zijn van contractbreuk, dan zou dat pas opgemerkt worden wanneer het gebruik of de stroom van gegevens afwijkt van wat in het contract is vastgelegd. Dit betekent meestal dat er al gegevens zijn vervuild of blootgesteld. Bij het hubmodel ligt het enigszins anders. Net zoals bij de gegevens kunnen contracten hier gecentraliseerd worden, en de hub-eigenaar kan het contractproces vergemakkelijken. Er kleven echter grotere risico's aan de hubvariant. Door de gecentraliseerde structuur vormt het een duidelijke bottleneck wanneer de doorvoer toeneemt, en het wordt een aantrekkelijk doelwit voor kwaadaardige aanvallen. Bovendien slaat de hub alle gegevens op zijn eigen servers op. Dit vereist een groot vertrouwen van de data holder om zijn waardevolle medische gegevens aan een externe organisatie toe te vertrouwen.

Governance maakt dus zeker een deel uit van het huidige gegevens deling proces. Alleen is er op dit moment geen uniformiteit tussen de vele data delingsprocessen die op dit moment lopen. Dat is te zien doordat er bijvoorbeeld geen eengemaakte data catalogus is binnen het health landschap.

Meer informatie over wat governance is, waaruit het is opgebouwd en hoe men in de toekomst aan good governance kan doen kan je vinden in hoofdstuk 7 Governance.

4.2.3.4 Invloeden van de overheid

Wat ook uniek is aan de manier waarop gezondheidsgegevens in België worden gedeeld, is het feit dat we een meertalig land zijn. België is onderverdeeld in drie hoofdregio's: Vlaams, Waals en het Brussels Hoofdstedelijk Gewest. Op dit moment zijn er organisaties die alle regio's bestrijken, evenals organisaties die alleen binnen een specifieke regio opereren. Deze laatste groep heeft meestal tegenhangers in de andere regio's. Het delen van gegevens tussen organisaties in meerdere regio's is vaak complex.
Er zijn geen strikte regels, behalve de basiswetten voor het delen van gegevens zoals bijvoorbeeld de GDPR. Regio-overschrijdend gegevens delen is voor veel organisaties geen vanzelfsprekendheid. Soms gebeurt het wel, maar soms hebben organisaties geen idee hoe hun tegenhangers in andere regio's opereren, waardoor ze niet weten of het delen van gegevens voordelen oplevert.

[21] *26/6/2024: Network of the national library of medicine. https://www.nichd.nih.gov/ [Laatst geraadpleegd op 10/12/2024]*

Daarnaast bestaat er een zekere aversie onder gezondheidsorganisaties ten opzichte van de overheid, wat voortkomt uit het gevoel onnodig gecontroleerd te worden. Bovendien heeft de Vlaamse bevolking over het algemeen weinig vertrouwen in de overheid. Uit een studie van Statistiek Vlaanderen bleek dat in 2024[22] minder dan 1 op de 5 Vlamingen vertrouwen heeft in de provinciale, Vlaamse, federale en Europese overheden. Alleen de lokale overheid scoorde beter, waarbij 3 op de 10 Vlamingen vertrouwen hebben in het lokale beleid. Dit illustreert het wantrouwen ten opzichte van de overheid, een factor waarmee rekening moet worden gehouden bij het delen van gezondheidsgegevens in België.

4.2.4 (Ideale) toekomstige staat

Als we naar de toekomst kijken, moeten we uitgaan van één ding: het gebruik van data space-technologie.

4.2.4.1 Gegevens bezoeken

Het benaderen van gegevens met behulp van een data space is veel minder gefragmenteerd, mits de technische realisatie generiek genoeg is om met meerdere data spaces tegelijk te communiceren.
Deze manier van communiceren maakt verschillende gedecentraliseerde combinaties mogelijk bij het combineren van gegevens:

- Eén-op-één
- Veel-naar-één
- Eén-naar-veel
- Veel-naar-veel

Al deze combinaties kunnen tegelijkertijd werken zonder dat de technische basisopstelling ingrijpend hoeft te worden aangepast. De gegevens van een organisatie blijven binnen de organisatie, en alleen de gevraagde gegevens worden naar de consument gestuurd. Dit hoeft niet de volledige dataset te zijn, maar kan een select aantal datavelden betreffen die opnieuw in kaart worden gebracht op een manier die bruikbaar is voor de consument. Dit biedt de mogelijkheid om veel gegevensbronnen te combineren en deze te gebruiken om eindgebruikers van de organisatie te helpen, informeren, ondersteunen en aantrekken.

Op basis van de voorgaande informatie lijkt het gebruik van datahubs (een gecentraliseerd systeem voor het verzamelen, opslaan en leveren van gegevens) achterhaald. Dit is echter niet helemaal waar, omdat dergelijke organisaties/systemen worden ingezet om de toegang tot de data space te vergemakkelijken. Vooral voor kleinere organisaties, die niet over de technische of financiële middelen beschikken om zich direct bij de data space aan te sluiten, bieden data intermediaries een oplossing. Een data intermediary is een tussenpartij die wél over de benodigde middelen en capaciteiten beschikt om deel te nemen aan de data space en allerhande (data) diensten aanbied. Hierdoor kunnen kleinere organisaties via de data intermediary hun gegevens beschikbaar stellen of ophalen uit de data space. Op deze manier kunnen ze hun gegevens sneller en efficiënter verspreiden door indirect gebruik te maken van de data space.

4.2.4.2 Technisch

Op technisch niveau zijn er enkele ontwikkelingen die we in de toekomst verwachten.
Allereerst is het belangrijk dat technische systemen die opgezet worden in staat zijn om met elkaar te communiceren. Het is niet zeker dat elke data space met dezelfde technologie wordt opgezet. Interoperabiliteit is dus van uiterst belang.

[22] *05/09/2024: Statistiek Vlaanderen. https://www.vlaanderen.be/statistiek-vlaanderen/relatie-overheid-en-burger/vertrouwen-in-de-overheid [Laatst geraadpleegd op 10/12/2024]*

Om meer te weten te komen over de technische opzet van een data space die in deze studie is gebruikt, zie secties 3.4.1.2 Technische bouwstenen volgens IDSA, 8.1 Analyse actuele data space componenten en 8.3 Design componenten.

Een belangrijk aspect voor een health data space is de aanwezigheid van een implementatiepartner. De implementatiepartner is verantwoordelijk voor het ontwikkelen, testen, bijwerken en onderhouden van de technische componenten die nodig zijn om de health data space operationeel te houden. Deze partner is verplicht om gezondheidsactoren en onderdelen van de health data space (zoals het clearing house) te ondersteunen bij het integreren van de technologie binnen hun organisatie-infrastructuur, op technisch niveau. Bovendien moet de implementatiepartner alle gezondheidsactoren binnen de data space live op de hoogte houden van technische kwesties, zoals hoge belasting van technische componenten en beveiligingsproblemen. Dit gebeurt op communicatief niveau.

Bij het delen van gegevens is technologie niet het enige technische onderwerp dat besproken moet worden. Datastandaarden zijn net zo belangrijk als het gaat om het efficiënt delen van gegevens. Wanneer er een beperkt aantal datastandaarden in gebruik is, is de kans groter dat gegevens zonder extra moeite gedeeld kunnen worden. Dit creëert ook een bepaalde mentaliteit binnen zorgorganisaties om na te denken over hoe ze hun gegevens structureren. Het aantal datastandaarden te veel beperken is echter ook geen goede oplossing. Dit kan namelijk betekenen dat sommige unieke soorten gezondheidsdata niet gedeeld kunnen worden, omdat de data space geen datastandaard ondersteunt die compatibel is.

4.2.4.3 Governance

Op bestuursniveau is de health data space samengesteld uit verschillende organen. Deze organen bestaan uit vertegenwoordigers van diverse actoren in de gezondheidssector binnen België. Sommigen zijn vertegenwoordigers van organisaties die al actief zijn binnen de health data space, terwijl anderen externen zijn die in eerste instantie misschien geen band hebben met de gezondheidssector. Deze leden vertegenwoordigen juridische, politieke en technische instanties. Het doel van deze verschillende bestuursorganen is het creëren, controleren en verbeteren van een niet-technisch ecosysteem rond de data space, waar organisaties zich veilig kunnen voelen om gegevens met anderen te delen. De processen omvatten, maar zijn niet beperkt tot:

- Toetreden tot de health data space.
- Het opstellen van contracten tussen alle partijen die betrokken zijn bij het delen van gegevens op de health data space.
- Wat gebeurt er als een gebruiker regels overtreedt?
- Wat gebeurt er als de health data space wordt aangevallen door kwaadwillende activiteiten?
- Wat is het algemene doel en de strategie van de health data space, en hoe moet deze zich ontwikkelen?

Meer informatie hierover kun je vinden in het hoofdstuk 7 Governance van het eindrapport.

4.2.4.4 Invloed vanuit de overheid

Op het niveau van de overheid is het moeilijker om een verwachte (ideale) situatie te creëren. Veel hiervan wordt bepaald door hoe gemotiveerd het huidige politieke landschap is als het gaat om health data spaces. In het ideale geval ziet het er als volgt uit.

Op een bepaald niveau binnen de overheid moeten beslissingen worden genomen over wat de schaal van de data space moet zijn en welke grondleggers de meest gunstige keuze vormen. Er moeten bestuursorganen en technische instanties worden aangesteld of opgezet. Als er nog geen voor de hand liggende organisaties bestaan, kan de overheid het juiste instrument zijn om bepaalde activiteiten te benoemen en te delegeren aan specifieke organisaties.

Een ander onderwerp waar de vertegenwoordigers van de overheid kunnen helpen is datastandaarden. Er moeten knopen doorgehakt worden over welke datastandaarden best gebruikt worden binnen het gezondheidsecosysteem. De overheid kan ondersteuning bieden door middel van het aanleveren van een soort handleiding met verschillende standaarden en waarvoor ze gebruikt worden.

Tot slot is het ecosysteem in België vooral gericht op het helpen van patiënten en het ondersteunen van de gezondheidszorg in het algemeen. Daarnaast is er ook veel aandacht voor onderzoek om de preventieve gezondheidszorg te verbeteren. Dit betekent dat winst, hoe noodzakelijk ook, niet altijd de belangrijkste focus is van organisaties. Het toetreden tot de health data space kan een technische en financiële inspanning vragen van de organisatie in kwestie, een inspanning die niet altijd mogelijk is wanneer we het hebben over non-profit gezondheidsorganisaties in België. Het is in deze gevallen dat de overheid een positieve invloed zou kunnen uitoefenen. Bijvoorbeeld door middel van subsidies of andere vormen van ondersteuning aan te bieden die de organisatie zou kunnen helpen om succesvol toe te treden tot de health data space. Op die manier zou de overheid zowel de health data space als de toetredende organisatie kunnen steunen.

4.3 BEHOEFTES HEALTH DATA SPACE

4.3.1 Gap analyse

In dit hoofdstuk hebben we de huidige situatie vergeleken met de verwachte (ideale) situatie om de kloof tussen beide toestanden te definiëren. Deze kloof is omgezet in verschillende behoeften. Deze behoeften zijn op hun beurt gebruikt om het implementatieproces voor de health data space op te zetten.

4.3.1.1 Gegevens bezoeken

Als het gaat om het delen van gegevens, is de kloof tussen de huidige en verwachte (ideale) situatie voornamelijk het gefragmenteerde gecentraliseerde ecosysteem versus de toekomstige, solide gedecentraliseerde aanpak waarbij men data bezoekt in plaats van datadeling. Bij deze laatste aanpak zal de data holder de gegevens binnen de organisatie houden in plaats van ze naar een datahub te sturen.

REQ001 - Als speler in de gezondheidszorg wil ik mijn verbindingen met verschillende technologische systemen beperken.

REQ002 - Als speler in de gezondheidszorg wil ik mijn gegevens binnen mijn eigen organisatiearchitectuur houden om het eigenaarschap en de veiligheid van de gegevens te garanderen.

REQ003 - Als speler in de health data space wil ik een veranderingsplan hebben dat datahubs en data intermediaries omvat om hun bestaan en waarde binnen het ecosysteem van de health data space te garanderen.

4.3.1.2 Technisch

Aan de technische kant verandert er veel als we de vergelijking maken.

> We gaan van meerdere manieren naar een beperkte/enkele manier om gegevens te delen.
> We richten ons veel meer op technische beveiliging door het gebruik van een technisch contractsysteem en vertrouwde derde partijen.
> We selecteren een implementatiepartner van de data space die toezicht houdt op de technische kant van de data space en die actoren binnen de data space ondersteunt.

> We selecteren bepaalde datastandaarden om het delen van gegevens minder complex te maken en een verandering te creëren in de manier waarop gegevens in de gegevensruimte worden gestructureerd.

REQ004 – Als speler in de gezondheidszorg wil ik de mogelijkheid hebben tot het verspreiden van mijn eigen organisatiegegevens en het ophalen van de nodige andere organisatie gegevens via een technologisch efficiënte en veilige oplossing.

REQ005 - Als speler in de gezondheidszorg wil ik er zeker van zijn dat als mijn data via een data space gedeeld wordt, er technische ingebouwde contracten zijn die nauwgezet worden opgevolgd door een neutrale, betrouwbare derde partij.

REQ006 - Als speler in de gezondheidszorg wil ik een geverifieerde technische partner die op technisch niveau zorg draagt voor de data space. Een partner die alles up-to-date houdt en actoren in de data space ondersteunt bij de implementatie van de nodige technische onderdelen.

REQ007 - Als speler in de gezondheidszorg wil ik een handleiding met alle noodzakelijke gegevensstandaarden die ik moet gebruiken om gegevens te delen. Er moet ook worden uitgelegd hoe ik ze moet gebruiken, zodat ik het gegevensbeleid binnen mijn organisatie proactief kan aanpassen om ervoor te zorgen dat toekomstige gegevens vanaf het begin goed worden gestructureerd.

4.3.1.3 Governance

Als we kijken naar de bestuurlijke kloof, zien we dat er in de huidige staat een duidelijk gebrek aan governance is. Daarom moeten we bepaalde structuren vanaf de grond opbouwen. Dit heeft voor- en nadelen. Aan de ene kant kunnen we met een "schone" lei beginnen, aan de andere kant zijn er veel onzekerheden, zoals wie initieel deel gaat nemen aan de health data space, welke organisaties operationele rollen gaan opnemen, enzovoort.

REQ008 - Als health data space moet er een algemeen governance-model worden opgezet om alle aspecten van de data space te reguleren en te controleren. Dit model moet bestaan uit meerdere bestuursorganen, elk met hun eigen taken en verantwoordelijkheden. De organen moeten vertegenwoordigers van elke actorengroep bevatten (overheid, gezondheidsactoren, ondersteunende organisaties, onderzoek en universiteiten).

REQ009 - Als speler in de gezondheidszorg wil ik er zeker van zijn dat mijn gegevens veilig zijn wanneer ze worden gedeeld, door middel van governancecontracten die nauwgezet worden opgevolgd door bestuursorganen. Deze contracten worden weerspiegeld in de technische contracten.

4.3.1.4 Overheid

Op het niveau van de overheid is het een mes dat aan twee kanten snijdt. De gezondheidszorgsector kijkt soms met wantrouwen naar de overheid omdat ze bang zijn voor onnodige controle en bestraffing van hun organisaties. Aan de andere kant kijken ze in een gefragmenteerd landschap naar de overheid om beslissingen te nemen over de grenzen en reikwijdte van de data space. Ook wanneer technische en bestuurlijke veranderingen nodig zijn, kijken ze naar de overheid voor ondersteuning en om de nodige systemen te creëren die door iedereen kunnen worden gebruikt.

REQ010 - Als speler in de gezondheidszorg verwacht ik dat de overheid beslissingen neemt over de omvang en grenzen van de data space, gegevensstandaarden, bestuursorganen en contractsystemen, terwijl de speler zijn vrijheid behoudt.

REQ011 - Als speler in de gezondheidszorg verwacht ik ondersteuning van de overheid als het gaat om financiële en technische middelen om toegang te krijgen tot de data space en mijn eigen gegevens beschikbaar te maken.

4.3.2 Vlaamse Health Data Space ten opzichte van de EHDS

Het resultaat toont aan dat er binnen Vlaanderen nood is aan een Vlaamse Health Data Space (VHDS). Naast de noden van het Vlaams ecosysteem omtrent datadeling is er natuurlijk ook nog de invloed op Europees niveau in de vorm van de European Health Data Space regulering (EHDS).

Tijdens het onderzoek hebben we geprobeerd antwoorden te vinden op diverse onderzoeksvragen. Eén van de belangrijkste vragen was hoe de optimale opzet van de Vlaamse Health Data Space (VHDS) eruit zou moeten zien en welke verwachtingen hieromtrent bestaan. De aanzet voor dit onderzoek kwam mede door de EHDS-verordening en de Europese ambitie om gezondheidsdata efficiënter en veiliger te delen binnen de EU.

Al snel werd duidelijk dat er verschillen zijn tussen wat de EHDS als wetgeving stipuleert en de potentiële missie, visie en scope van de VHDS.

> De **EHDS** is een wetsdocument dat een **processtructuur** beschrijft voor het delen van verschillende soorten gezondheidsdata. Daarnaast bepaalt het welke gezondheidsgegevens binnen de EU beschikbaar moeten worden gesteld en wat de gevolgen zijn wanneer lidstaten, datahouders of datagebruikers niet aan de voorwaarden voldoen.

> De **VHDS** richt zich op het daadwerkelijke delen en raadplegen van data bij datahouders door dataconsumenten. Het voorziet in een controlelaag op technisch, governance- en businessniveau die ervoor zorgt dat de data-uitwisseling veilig, gestructureerd en bewust plaatsvindt.

4.3.2.1 Belangrijke verschillen tussen EHDS en VHDS

> Doelstelling:
  - De VHDS kan in principe onafhankelijk van de EHDS bestaan en opereren. Het functioneert als een tool die de gezondheidssector ondersteunt bij het uitvoeren van specifieke acties:
    - Lokaliseren van relevante data binnen het gezondheidslandschap.
    - Faciliteren en monitoren van contracten op technisch niveau tussen datadelingspartners via trusted third parties.
    - Bijhouden van eerdere datatransacties.
  - De EHDS is daarentegen een wettelijke kader dat beschrijft:
    - Welke gezondheidsdata beschikbaar moet worden gesteld binnen Europa.
    - Hoe het proces voor het opvragen van data moet verlopen.
    - Welke consequenties gelden voor organisaties die niet aan de regelgeving voldoen.

> Relatie tussen VHDS en EHDS:
  - Het doel van de VHDS is om te voldoen aan de voorwaarden en verwachtingen die door de EHDS zijn gesteld. Hierdoor kan de VHDS fungeren als een tool binnen de EHDS om specifieke onderdelen van de beschreven processen te faciliteren, zoals de daadwerkelijke data-uitwisseling tussen datahouders en dataconsumenten.

> Onderdelen van de in de EHDS beschreven processen die de VHDS niet zal faciliteren zijn bijvoorbeeld het verwerken van data-aanvragen, het voorzien van secure processing environments, rapportering en publicatie naar andere lidstaten van de EU.

4.3.2.2 Conclusie

De VHDS richt zich initieel op de praktische, veilige en efficiënte uitwisseling van data binnen Vlaanderen met als langetermijnvisie uit te breiden naar België en Europa, terwijl de EHDS een breder Europees juridisch kader biedt dat regels en processen vastlegt. Samenwerking tussen beide is essentieel om te voldoen aan de Europese normen en tegelijkertijd een effectieve infrastructuur te bieden voor het delen van gezondheidsdata.

4.3.3 Het koppelen van data spaces

Het koppelen van data spaces is een onderwerp dat zeker nog aan bod moet komen in een vervolgproject. Het is een scenario waarvoor momenteel weinig praktische voorbeelden bestaan. Conceptueel roept het al snel vragen en onduidelijkheden op. Om in de toekomst een koppeling mogelijk te maken, moeten beide data spaces interoperabel zijn, zowel op technisch als op governancevlak.

4.3.3.1 Technische interoperabiliteit

Op technisch vlak betekent dit dat prosumers met één connector simultaan gebruik moeten kunnen maken van beide data spaces. Daarnaast moeten andere bouwblokken, zoals bv. de broker en het clearing house, compatibel zijn met elkaar.

4.3.3.2 Governance interoperabiliteit

Ook op governancevlak gelden vergelijkbare eisen. Beide governance-structuren en -frameworks moeten op elkaar afgestemd zijn om te garanderen dat de communicatie, efficiëntie en veiligheid aan de verwachtingen van beide data spaces voldoen.

De complexiteit neemt exponentieel toe wanneer men data spaces probeert te koppelen die verschillende sectoren vertegenwoordigen. Een voorbeeld hiervan is de koppeling tussen een gezondheidsdata space en een milieudata space. Deze bevatten zeer verschillende soorten data: gezondheidsdata zijn bijvoorbeeld van nature veel gevoeliger, waardoor de regelgeving voor deze data space veel strenger is dan voor een data space die zich richt op milieugegevens. Hoe hiermee omgegaan moet worden, is tot op heden een vraag die nog onbeantwoord blijft.

4.4 NODEN VAN DE VLAAMSE OVERHEID

4.4.1 Datadeling

Een algemene doelstelling van de Vlaamse overheid is een warme en zorgzame samenleving voor alle Vlamingen. Om dit te kunnen verwezenlijken zijn er verschillende onderwerpen waaraan gewerkt moet worden. Het delen van gezondheidsdata op een veilige, efficiënte en financieel voordelige manier is iets dat ondersteunend kan werken om op een correcte manier met deze uitdagingen aan de slag te gaan. Daarom wil de Vlaamse overheid met een data space het gezondheidslandschap ondersteunen om ervoor te zorgen dat alle dataleveranciers de mogelijkheid hebben om binnen het gezondheidslandschap hun data ter beschikking te stellen voor dataconsumenten.

4.4.2 De Vlaamse overheid als bibliothecaris

Ondersteuning bieden om gezondheidsdata beschikbaar te maken kan op verschillende manieren.
Eén van deze manieren is het zichtbaar maken van de verschillende databronnen in het gezondheidslandschap. Het is onmogelijk om een goed gezondheidsdatadelingsecosysteem op te zetten als men niet op de hoogte is van wie welke data ter beschikking heeft. Om hier meer duidelijkheid in te krijgen, is er behoefte aan een organisatie die enerzijds een overzicht creëert van alle gezondheidsdata en hun locatie. Anderzijds is het ook belangrijk dat deze informatie enkel beschikbaar is voor organisaties die met goede bedoelingen en belangen gezondheidsdata willen raadplegen. Daarom kan het een doel zijn van het Vlaams Departement Zorg om een exhaustief overzicht te creëren van alle data in het Vlaams zorg- en welzijnslandschap en dit overzicht beschikbaar te stellen voor iedereen die zich wil conformeren aan de vooropgestelde regels rond veiligheid en governance. Belangrijk hierbij is dat het gaat om een overzicht van welke data waar te vinden is en niet om de data zelf; deze blijft te allen tijde bij de dataleveranciers.

4.4.3 Vlaanderen als opstap voor België

We hebben vastgesteld dat innovatie omtrent het delen van data binnen het Vlaamse zorg- en welzijnslandschap niet gemakkelijk is. Het opzetten van een health data space in Vlaanderen plaatst de Vlaamse overheid in een unieke positie om met deze kennis en ervaring eenheid te brengen binnen België. Het vormt een startpunt om het toch wel gefragmenteerde gezondheidslandschap in België op het gebied van datadeling bij elkaar te brengen. Op die manier kan er mogelijk in de toekomst een veiligere en efficiëntere stroom van data zijn tussen Vlaanderen, Wallonië en het Brusselse hoofdstedelijk gewest en de federale overheid.

4.4.4 Preventieve gezondheidszorg

Datadeling binnen het Vlaams zorg- en welzijnslandschap is één ding, maar preventieve gezondheidszorg heeft meer te maken met alleen gezondheidsgegevens. Er komen ook niet-gezondheidsgegevens aan te pas, zoals milieu, wegen en verkeer, wonen, koopkracht, enzovoort. Deze gegevens in combinatie met gezondheidsgegevens kunnen leiden tot nieuwe interessante bevindingen die ervoor zorgen dat bepaalde preventieve maatregelen genomen kunnen worden om de gezondheid van de Vlaamse burger te verbeteren. In het regeerakkoord 2024 – 2029 wordt er dieper ingegaan op het inzetten op preventie.
Om deze verwachting te ondersteunen is er een nood aan samenwerking met andere sectoren en beleidsdomeinen.
Een data space zou deze combinatie oefening fundamenteel kunnen vergemakkelijken omdat men op een efficiënte en veilige manier specifieke stukken van data sets kan combineren.

4.4.5 Noden mappen op (inter)nationale context

Europa stimuleert de implementatie van health data spaces via de EHDS-verordening, maar de afstemming van nationale noden met Europese vereisten is complex door de snelle evolutie op business-, governance- en technisch vlak. Veel EU-lidstaten zoals Duitsland, Luxemburg en Nederland ontwikkelen al eigen initiatieven met specifieke doelen, wat benchmarking en kennisdeling tussen landen bevordert.
Daarnaast zijn er heel wat gedeelde behoeften tussen de verschillende lidstaten. Eén daarvan is het onderzoek naar zeldzame ziekten, waarbij samenwerking en data-uitwisseling essentieel zijn vanwege het beperkte aantal patiënten. Health data spaces kunnen veilige oplossingen bieden voor het delen van deze gevoelige gegevens, wat bijdraagt aan efficiëntie en innovatie binnen Europa. Op termijn kunnen Belgische of Vlaamse initiatieven optimaal in het Europese systeem geïntegreerd worden zodra de EU duidelijke verwachtingen formuleert.

5 USE CASES

5.1 PLAN VAN AANPAK

5.1.1 Toelichting plan van aanpak

In het kader van het bepalen van geschikte use cases voor dit project zijn via workshops verschillende **high-level onderwerpen** geïdentificeerd die kunnen uitmonden in impactvolle toepassingen of use cases. Hierbij werd een beroep gedaan op zowel interne als externe domeinexperten, projectpartners en de Vlaamse beleidsprioriteiten.

Enkele geïdentificeerde onderwerpen die uit deze workshops kwamen, waren:

- **Digitalisatie van de eerste 1000 dagen van een kind.** Door het samenbrengen van verschillende datastromen van een (ongeboren) kind tot de tweede verjaardag kunnen gerichte preventieve acties worden opgezet. Denk hierbij aan een digitaal kindboekje via een Solid Pod, remote monitoring, socio-economische gegevens van de ouders en data uit health-apps zoals *Baby Tracker* of *Oei, ik groei*.
- **Vroegdetectie van hartritmestoornissen**. Een tweede onderwerp richt zich op het verbeteren van de vroegdetectie van hartritmestoornissen. Dit wordt gerealiseerd door cardiovasculaire gegevens, bijvoorbeeld uit apps zoals *FibriCheck* of andere oplossingen (*CardioCare@home* van Byteflies), te verrijken met socio-demografische informatie. Deze gecombineerde data kunnen bijdragen aan vroegtijdige interventies en een betere gezondheidsuitkomst voor patiënten.
- **Verbeteren van de levenskwaliteit van kinderen met ADD**. Voor kinderen met Attention Deficit Disorders (ADD) wordt onderzocht hoe data uit wearables, gezondheidsapplicaties, omgevingsdata en elektronische patiëntendossiers (EPD) kunnen worden ingezet. Het doel is om methodologieën te ontwikkelen die kinderen helpen om met hun ADD om te gaan, hun unieke kwaliteiten te benutten en de impact van ADD op hun dagelijks leven te verminderen.
- **Verbeteren van de levenskwaliteit van werkende Vlamingen**. Het aanpakken van werkgerelateerde stress en burn-out vormt een andere opportuniteit. Door gegevens uit eerstelijnszorg, sociale media, publieke gezondheidsenquêtes, omgevingsfactoren en draagbare sensoren te combineren, kan een beter inzicht worden verkregen in de oorzaken van stress. Dit maakt gerichte interventies mogelijk om het welzijn van werkende Vlamingen te verbeteren.
- **Eenzaamheid bij ouderen opsporen**. Om eenzaamheid bij ouderen te bestrijden, wordt gekeken naar het gebruik van data uit eerstelijnszorg, zorginstellingen, wearables en omgevingsfactoren. Deze gegevens kunnen worden gebruikt voor vroegdetectie en om gepersonaliseerde behandelplannen op te stellen om ouderen beter te ondersteunen in hun sociale en mentale welzijn.
- **Regiogebonden preventieactieplan voor diabete**s. Voor de preventie en ondersteuning van mensen met diabetes wordt onderzocht hoe gegevens uit verschillende bronnen, zoals eerstelijnszorg, wearables, "Provincie in Cijfers", IMA, ziekenhuizen en apotheken, kunnen worden samengebracht. Deze data kunnen dienen als basis voor regiogebonden preventieactieplannen en gerichte interventies.
- **Stroomlijnen van labodata naar overheidsinstanties**. Een andere opportuniteit is het verbeteren van de datastroom van laboratoria naar overheidsinstanties zoals Sciensano. Dit kan bijdragen aan een snellere respons op acute situaties en het beter naleven van meldingsplichten.
- **Optimaliseren van datastromen tussen ziekenhuizen**. Hierdoor wordt het mogelijk om meer inzichten te verkrijgen in complexe en zeldzame aandoeningen en om benchmarking tussen ziekenhuizen te faciliteren.

Na de identificatie van deze onderwerpen werd een lijst opgesteld met belangrijke stakeholders in het gezondheidsecosysteem. Om de geschiktheid van de onderwerpen te bepalen, zijn daarnaast evaluatiecriteria ontwikkeld. Hierbij is gebruikgemaakt van de bouwstenen van de **Innovatrix** (zie Innovatrix) als **inspiratiebron**, een innovatiecanvas om assumpties van innovatieve ideeën te helpen structureren. Deze criteria hebben geholpen bij het selecteren van onderwerpen die het meest relevant en haalbaar zijn voor de beoogde doelstellingen van het project. De bovengenoemde onderwerpen werden geëvalueerd naar:

> Wat is de **haalbaarheid** van een **use case** omtrent dit onderwerp (bv. Wat is de doorlooptijd van een use case omtrent dit topic)?
> Wat is de **technische haalbaarheid** (bv. Wat is er architecturaal/infrastructureel nodig)?
> Wat is het niveau van interesse van de belangrijkste **stakeholders** voor dit onderwerp?
> Wat is de relevantie van de **beoogde doelgroep** voor de maatschappij (bv. Hoe groot is de populatie, welke druk oefent het probleem uit op de maatschappij)?
> Wat is de **meerwaarde** van een health data space voor dit probleem? (bv. Kan een health data space de huidige aanpak verbeteren?
> Welke onderwerpen bevatten near-real time data (bv via health apps)? Hoewel deze vraag een uiterst interessant item in een data space vormt, werd later beslist deze niet verder als criteria mee te nemen in het bepalen van een onderwerp om use cases rond te definiëren.

Vanuit de lijst met onderwerpen werden een aantal use cases voorgelegd en werden gesprekken opgezet met stakeholders voor identificatie van use cases omtrent deze (en nog andere) onderwerpen.

5.1.2 Verloop zoektocht naar use cases

In de eerste jaarhelft van 2023 deed imec een **vooronderzoek naar twee use cases** (zie sectie 5.4 Potentiële use cases, use cases De Vlaming leeft gezond en BMI monitor). Geen van beide use cases werd echter geschikt geacht door Departement Zorg. Vervolgens werden er intensief contacten gelegd, voornamelijk vanuit Departement Zorg en de projectsponsor, om mogelijke use cases te identificeren. Hieruit kwamen in de tweede jaarhelft van 2023 **drie potentiële kanshebbers**:

> De eerste use case richtte zich op ziekenhuizen uit het **FHIN-netwerk** die de OMOP-standaard en federated learning gebruiken om AI-modellen te verbeteren. De betrokken stakeholders in het FHIN-netwerk zijn: Radar, UZ Brussel, Imelda, UZA, ZOL, AZ Delta, CHU de Liège, AZ Klina, AZ Sint-Jan Brugge en UZ Gent.
> Een andere use case in samenwerking met het Data4PHM-consortium heeft tot doel population health management op lokaal niveau te vergemakkelijken door middel van federated analytics. Hierbij werd gekozen voor diabetes type 2. Het Data4PHM-consortium bestaat uit: Zorgzaam Leuven, Sciensano, IMA, FarmaFlux, UAntwerpen Faculteit Sociologie & Geneeskunde, Intego.
> De derde use case, bekend als **'Epilabo'**, maakt gebruik van het bestaande netwerk van peillaboratoria om het delen van gegevens over uitbraken van infectieziekten tussen de laboratoria, Sciensano en het Departement Zorg mogelijk te maken. Het Epilabonetwerk bestaat uit Sciensano, de peillaboratoria, en Healthdata.be.

Voor het FHIN-netwerk en Data4PHM werd in het najaar van 2023 een behoefteanalyse uitgevoerd. Uiteindelijk werd enkel voor Data4PHM daadwerkelijk een use case opgestart. Voor Epilabo zijn vanaf juni 2023 tot maart 2024 tal van gesprekken gevoerd met Sciensano en Healthdata.be met het oog op de opstart van de Epilabo use case. Uiteindelijk kregen we na enkele hoopvolle gesprekken begin 2024, in maart 2024 de melding dat Sciensano niet zou meewerken aan deze use case. (cf. bijlagen 5.C en 5.D voor meer details over FHIN en Epilabo)

In 2024 werd verder actief op zoek gegaan naar **andere mogelijke use cases**. Naar aanleiding van presentaties van de projectsponsor over het health data space project, kwamen er veel leads binnen voor mogelijke use cases. Het daadwerkelijk opstarten van use cases bleef echter moeilijk omwille van de redenen die hieronder zullen worden toegelicht in sectie 5.1.3 Bevindingen selectieproces. Uiteindelijk werd ook FAQIR bereid gevonden om een gemeenschappelijke use case op te zetten om de connectie van Solid Pods op een data space te onderzoeken. Aangezien deze use case zich ook focuste op diabetes type 2, was dit de ideale aanvulling op de reeds lopende Data4PHM use case. Verder werden ook belangrijke contacten gelegd met het Vlaams Ziekenhuisnetwerk dat zich ook bereid verklaarde om een gemeenschappelijke use case rond minimale ziekenhuisgegevens op te zetten. Helaas was de resterende tijd binnen het project onvoldoende om de FAQIR en VZN use cases gedegen op te starten. Beide use cases bevinden zich echter in een verder geëvolueerd stadium dan de andere potentiële use cases.

In wat volgt wordt daarom een onderscheid gemaakt tussen welke use cases werden weerhouden, welke use cases diepgaand voorbereid werden en welke use cases potentieel vertonen voor een vervolgtraject.

5.1.3 Bevindingen selectieproces

De zoektocht naar geschikte use cases en betrokken stakeholders bleek **uitdagend**.
De gezondheidssector lijkt momenteel niet volledig voorbereid op een innovatief onderzoeksproject van deze schaal. Potentieel interessante stakeholders gaven vaak aan niet te kunnen deelnemen vanwege een gebrek aan ruimte in hun planning, onvoldoende financiële ondersteuning voor de uitvoering van een use case, zorgen over het integreren van nieuwe technologische componenten in hun bestaande architectuur, of doordat zij al betrokken waren bij andere technologieprojecten (van de overheid of andere instanties). Daarnaast speelden onzekerheden over het vervolgtraject van dit project, zoals de implementatie van de health data space, een rol. Het gebrek aan subsidies voor deelname werd over het algemeen als een belangrijke belemmering ervaren. Tot slot wilden ook heel wat stakeholders afwachten wat de HDA zou doen.

Dit had als gevolg dat **het traject om use cases te selecteren voor de PoC erg lang heeft aangesleept**. Uiteindelijk is het volledige eerste onderzoeksjaar besteed aan deze zoektocht en kon er pas vanaf 2024 (Q1) gestart worden met de concrete uitwerking van de Data4PHM use case. In 2023 (en ook in 2024) werd er veel tijd besteed aan het identificeren van interessante stakeholders en aan gesprekken met deze stakeholders om het project en het concept health data space toe te lichten. Zo werden voor enkele potentiële use cases gesprekken gevoerd over een periode van meerdere maanden, om uiteindelijk toch van de stakeholders in kwestie te vernemen dat ze niet zouden deelnemen. Het belang van meerdere gesprekken om goed de context en de inhoud van het onderzoeksproject te kaderen, is niet te onderschatten. Stakeholders vinden data spaces over het algemeen geen evidente materie en moeten ook vaak gerustgesteld worden. Het feit dat dit een onderzoeksproject was (waarvan de resultaten niet in productie gingen), kon enerzijds helpen, maar anderzijds wilden geïnteresseerde stakeholders ook juist zekerheid dat er een verderzetting van het project in een implementatietraject zou volgen zodat de geïnvesteerde tijd geen weggesmeten tijd zou zijn. De onzekerheid over of er al dan niet budget zou toegewezen worden voor een vervolgproject, heeft het project dus helaas parten gespeeld.

5.2 UITGEVOERDE USE CASES

Gedurende de looptijd van dit project werden verschillende use cases onderzocht. Uiteindelijk werd slechts **één use case in detail uitgevoerd**, namelijk de Data4PHM use case. De gedetailleerde uitwerking hiervan is terug te vinden in hoofdstuk 9 Uitwerking Data4PHM use case.

5.2.1 Context van de Data4PHM use case

Het Data4PHM-consortium bestaat uit een aantal actoren uit het gezondheidslandschap die als missie hebben om middels **populatiegerichte gezondheidszorg**, gebaseerd op het **secundair gebruik van gezondheidsdata**, een krachtig en toekomstbestendig zorgsysteem te realiseren.

Drie van deze actoren (Intego, IMA en FarmaFlux) hebben vanuit die missie een specifieke use case voorgedragen rond **diabetes type 2**.

1. *Intego* is een Vlaams huisartsenregistratienetwerk dat medische gegevens verzamelt voor wetenschappelijk onderzoek en kwaliteitsverbetering in de zorg. Daardoor is het een belangrijk instrument voor het opvolgen van de volksgezondheid.
2. *IMA (Intermutualistisch Agentschap)* is een samenwerkingsverband tussen de Belgische ziekenfondsen dat gezondheidsdata over de terugbetaalde zorgen en geneesmiddelen in België verzamelt en analyseert. Daarnaast bezit IMA ook over verschillende socio-economische en demografische gegevens: aangezien aansluiting bij een mutualiteit verplicht is in België, bezit het IMA-gegevens van alle 11 miljoen burgers. Alle gegevens waarover IMA beschikt, worden op verschillende niveaus verwerkt, van nationaal tot regionaal niveau.
3. *FarmaFlux* is een overkoepelende organisatie van de Belgische apothekersverenigingen. Het beheert de gegevensuitwisseling van en naar apotheken, vooraleer deze in de centrale databank van het gedeeld farmaceutisch dossier terecht komen. Het gaat onder meer over afleveringsgegevens en data over het gebruik van terugbetaalde en niet-terugbetaalde medicatie en farmaceutische zorg. De datatransfers gebeuren real-time en zijn geautomatiseerd.

De drie partners zochten namelijk naar een manier om **geaggregeerde data uit verschillende bronnen efficiënt en veilig beschikbaar te stellen in een geïntegreerd dashboard**. Via een dergelijk dashboard kunnen population health managers, zorg- en welzijnsverleners namelijk verschillende zorgkwaliteits-indicatoren op lokaal niveau raadplegen en gebruiken, wat kan bijdragen de gewenste transitie van een reactieve naar een **preventieve gezondheidszorg**. Om zo'n dashboard te voeden met relevante **data**, moeten deze eerst (technisch) kunnen worden **samengebracht**. Dit laatste is echter nog een openliggend vraagstuk omwille van bestaande uitdagingen op vlak van interoperabiliteit, infrastructuur, wetgeving en governance.

Een use case rond **diabetes type 2** bleek naar voren te treden als logische eerste test case voor zo'n geïntegreerd dashboard. De prevalentie van diabetes is namelijk erg hoog in Vlaanderen: Sciensano schatte de prevalentie van diabetes in België in 2014 in op ongeveer 6,33% voor personen ouder dan 15 jaar. Dit cijfer betreft waarschijnlijk zelfs een onderschatting, aangezien een aanzienlijk deel van de populatie (nog) niet weet dat ze diabetes heeft. Bovendien legt diabetes type 2 een zware last op het gezondheids-systeem en de samenleving, zowel op vlak van menselijke als financiële kost. Het aanpakken van diabetes type 2, dat deels wordt ingegeven voor iemands (ongezonde) levensstijl, vraagt echter een brede, holistische aanpak, met betrokkenheid van een multidisciplinair team, en met steun van Vlaamse en federale programma's en zorgpaden. De nood aan zo'n proactieve en gecoördineerde aanpak wordt verder ondersteund door de expliciete vermelding van diabetes type 2 in de beleidsdoelstellingen als aandoening waarbij preventie essentieel is[23].

[23] https://www.zorg-en-gezondheid.be/sites/default/files/2022-11/Tussentijdsrapport_Gezonderlevenin2025_definitief.pdf

Tot slot is de diabetespopulatie een heel interessante use case omdat er reeds veel gezondheidsdata beschikbaar is van deze populatie. Zo worden niet alleen klinische data verzameld bij de verschillende bronnen, maar worden ook data over bepaalde risicofactoren zoals levensstijl, BMI, rookstatus, inkomen en andere geregistreerd. Een deel van deze gezondheidsdata kan bovendien via geautomatiseerde processen worden opgehaald, bijvoorbeeld via de diabetesbarometer van Intego of via het Gedeeld Farmaceutisch Dossier (GFD), wat hen interessante testgegevens maakt voor een PoC voor een health data space.

De grote kracht van dit consortium ligt onder andere in de **éénsgezindheid** die heerst bij de partners, en de duidelijke **hulpvraag** en nood (een dashboard voor population health managers op basis van databronnen die vandaag technisch moeilijk te combineren zijn). Dit maakt dat een technische PoC op korte termijn als haalbaar werd ingeschat. Finaal werd deze use case daarom weerhouden als referentie waaraan de technische PoC en de legal en governance scan moeten worden afgetoetst. Meer info over de specifieke invulling van de use case kan men terugvinden in hoofdstuk 9 Uitwerking Data4PHM use case.

Betrokken contactpersonen:

- Bert Vaes (Intego, KU Leuven)
- Gijs Van Pottelbergh (KU Leuven)
- Maarten Caspers (KU Leuven)
- Marie Van de Putte (KU Leuven, APB)
- Manon Buyl (FarmaFlux)
- Marc Buekens (FarmaFlux)
- Birgit Gielen (IMA)
- Sofie Vanassche (IMA)
- Johan Vanoverloop (IMA)
- Dirk De Kesel (IMA)
- Andreas De Bleser (IMA)
- Stijn Serry (SMALS, IMA)

5.3 USE CASES IN OPSTART

Tijdens het project werden **twee uses cases meer in detail voorbereid**:

> een use case rond Solid in samenwerking met **FAQIR**

> een use case rond minimale ziekenhuisgegevens (MZG) met het **Vlaams Ziekenhuisnetwerk** (VZN)

Door omstandigheden konden deze use cases gedurende de looptijd van dit project niet volledig uitgewerkt worden. Bij een vervolgproject worden idealiter deze use cases eerst opgepakt.

5.3.1 Solid use case i.s.m. FAQIR

5.3.1.1 Context

Tijdens het project werd contact gelegd met Filip Pattyn en Hans Constandt, de oprichters van **FAQIR Institute en FAQIR Foundation**. De FAQIR Foundation is een onafhankelijk onderzoeksinstituut dat zich richt op gezondheidszorginnovatie en -onderzoek. De foundation werkt aan diverse projecten, waaronder projecten rond persoonlijke datakluizen. Aan de andere kant is het FAQIR Institute een health tech bedrijf

dat klanten klaarstoomt voor datagedreven gezondheidszorg, waarbij de focus ligt op de FAIR principes en datakwaliteit (zie ook sectie 7.3.5.3 FAQIR en 9.3 Fair data en metadata).

Vanuit FAQIR was er ook interesse om een gemeenschappelijke **diabetes use case** uit te werken. Voor een oproep voor innovatieprojecten van de FOD Volksgezondheid werd begin 2024 door FAQIR een project rond diabetes voorgesteld. Het zou gaan om een samenwerking tussen vier ziekenhuizen in regio's Aalst en Gent, huisartsenpraktijken in dezelfde regio's en een diabetespraktijk. Het project had als doel om bottom-up voor de diabetespatiënt een dashboard te voorzien waarin een aantal parameters gecapteerd worden over de eigen diabetestrend. Zowel de patiënt als de huisarts en arts-specialist zouden parameters kunnen invoeren waardoor alle betrokkenen te allen tijde een goed overzicht hebben van de progressie van de patiënt. Hierbij worden alle partijen ontzorgd omdat informatie maar 1 keer ingegeven dient te worden. Voor dit project zou gebruikgemaakt worden van Solid datakluizen. Er werden echter geen projectmiddelen toegekend aan dit project.

Vanuit FAQIR werd beslist om het project toch op te starten, mits herscoping. Er zou in eerste instantie enkel gefocust worden op tweedelijnszorg in samenwerking met 2 ziekenhuizen. Voor dit project wordt gebruikgemaakt van **Solidtechnologie**, waarbij elke patiënt en elk ziekenhuis beschikt over een eigen datakluisje. Bij Solidtechnologie beslist de burger zelf aan wie hij toegang verleent tot zijn data. Eens deze toegang verleend is, komen de updates binnen in een zogenaamd aggregatorkluisje dat voorzien zal worden door FAQIR. Deze aggregatorkluis zou dan kunnen connecteren op de health data space.

Bovenstaande use case is complementair aan de diabetes use case met het Data4PHM-consortium omwille van vier overeenkomende indicatoren. Het biedt ook de mogelijkheid om te onderzoeken of een Solid Pod deel kan uitmaken van het health data space ecosysteem.

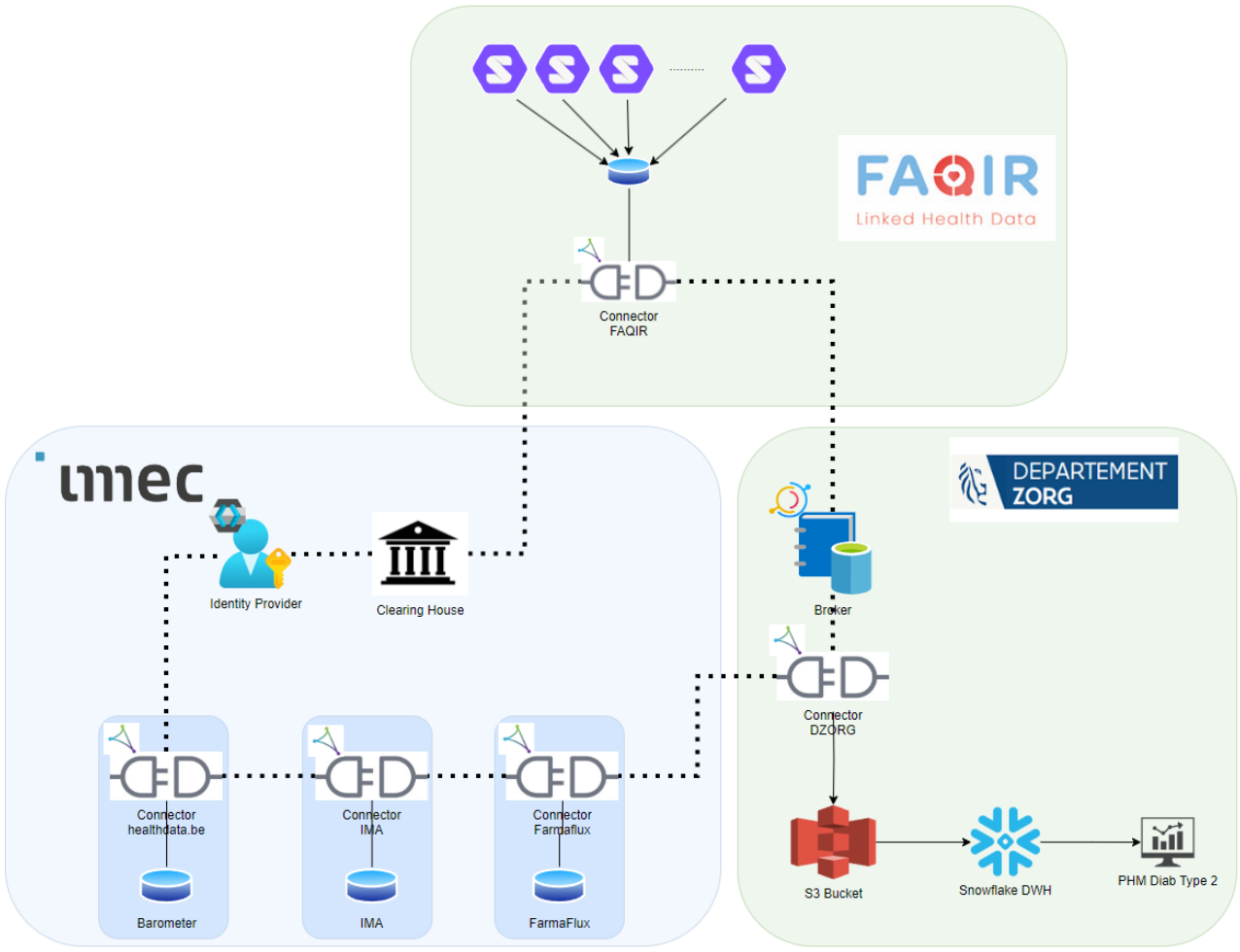
5.3.1.2 Uitwerking use case

Voor de uitwerking van deze use case werd door FAQIR een **simulatieomgeving voor gezondheidsdatakluizen** ontwikkeld die kan geconfigureerd worden voor verschillende indicaties en situaties. Hiermee is het mogelijk om profielen van individuen met diabetes te genereren waarbij volgens statistische modellen parameters en gebeurtenissen toegekend worden zoals: geslacht, leeftijd, aandoeningen, lengte, gewicht, medicatieschema …

Daarnaast kunnen ook eerstelijns- en tweedelijnszorgverstrekkers geconfigureerd worden. Dit resulteert in een kleinschalig netwerk van een aantal honderden virtuele patiënten en zorgverstrekkers. Via eenvoudige functies kunnen gebruikers van de omgeving gebeurtenissen toevoegen (meting, inname medicatie …) in de datakluis van één of meerdere patiënten. Een gebruiker kan ook dashboards genereren voor specifieke individuen of voor specifieke gezondheidsprofessionals (huisartsen of endocrinologen). Die laatste zijn overzichten van de patiëntenpopulatie van zo'n professional.

Er kan ook gesimuleerd worden wie specifiek zijn/haar data wil delen met een professional voor primair gebruik in de zorg zelf. Daarnaast kan ook ingesteld worden welke individuen bereid zijn om data te delen voor secundair gebruik (hergebruik) binnen en/of buiten de directe zorg. Voor secundair gebruik kan enkel geaggregeerde data beschikbaar gesteld worden. Gebruikers van de simulatieomgeving kunnen een wetenschappelijke vraag formuleren die vervolgens omgezet wordt in een query voor een aggregatordatakluis.

Zo'n **aggregatordatakluis** wordt geconfigureerd en extraheert de relevante data vanuit alle kluizen waar deling voor secundair gebruik is ingesteld. Binnen de datakluis wordt het aggregaat gegenereerd en is dit beschikbaar voor download samen met een metadatabestand dat de DCAT-specificaties volgt.
Dit geaggregeerde databestand kan vervolgens gepubliceerd worden in een data space connector die onderdeel uitmaakt van de Vlaamse health data space. Op die manier kan aangetoond worden dat een persooncentrisch datakluisnetwerk van primaire gegevensuitwisseling in de zorg direct gekoppeld kan worden aan een data space netwerk voor secundair gebruik van gezondheidszorgdata.



Figuur 8: FAQIR use case. Geplande technische opzet.

Betrokken contactpersonen:

- Filip Pattyn (FAQIR)
- Hans Constandt (FAQIR)

5.3.2 Minimale ziekenhuisgegevens use case i.s.m. het Vlaams Ziekenhuisnetwerk

5.3.2.1 Context

Binnen dit project werd vanaf de start in het achterhoofd gehouden dat **Minimale Ziekenhuis Gegevens (MZG-data**) een interessante use case zouden kunnen vormen om de waarde van een health data space te illustreren. MZG-data wordt gebruikt voor de financiering van ziekenhuizen, voor beleidsondersteuning en voor wetenschappelijk onderzoek. Het probleem met de Minimale Ziekenhuisgegevens (MZG) in België ligt vooral in de timing en de gedetailleerdheid van de feedback. Ook andere instanties behalve de federale overheid hebben nood aan deze gegevens (vb. Departement Zorg, VIKZ). Het zou daarom efficiënter zijn als de MZG-datasets beschikbaar zouden worden gesteld via de health data space. Dit zou alle betrokken partijen in staat stellen om de MZG-gegevens te raadplegen zodra de dataset beschikbaar is.
Bovendien zouden andere zorgactoren, als ze op de health data space zijn aangesloten, rechtstreeks specifieke data kunnen opvragen bij de ziekenhuizen en hen van persoonlijke feedback kunnen voorzien. Ziekenhuizen dienen tot slot hun MZG-data slechts éénmalig ter beschikking te stellen via de data space.

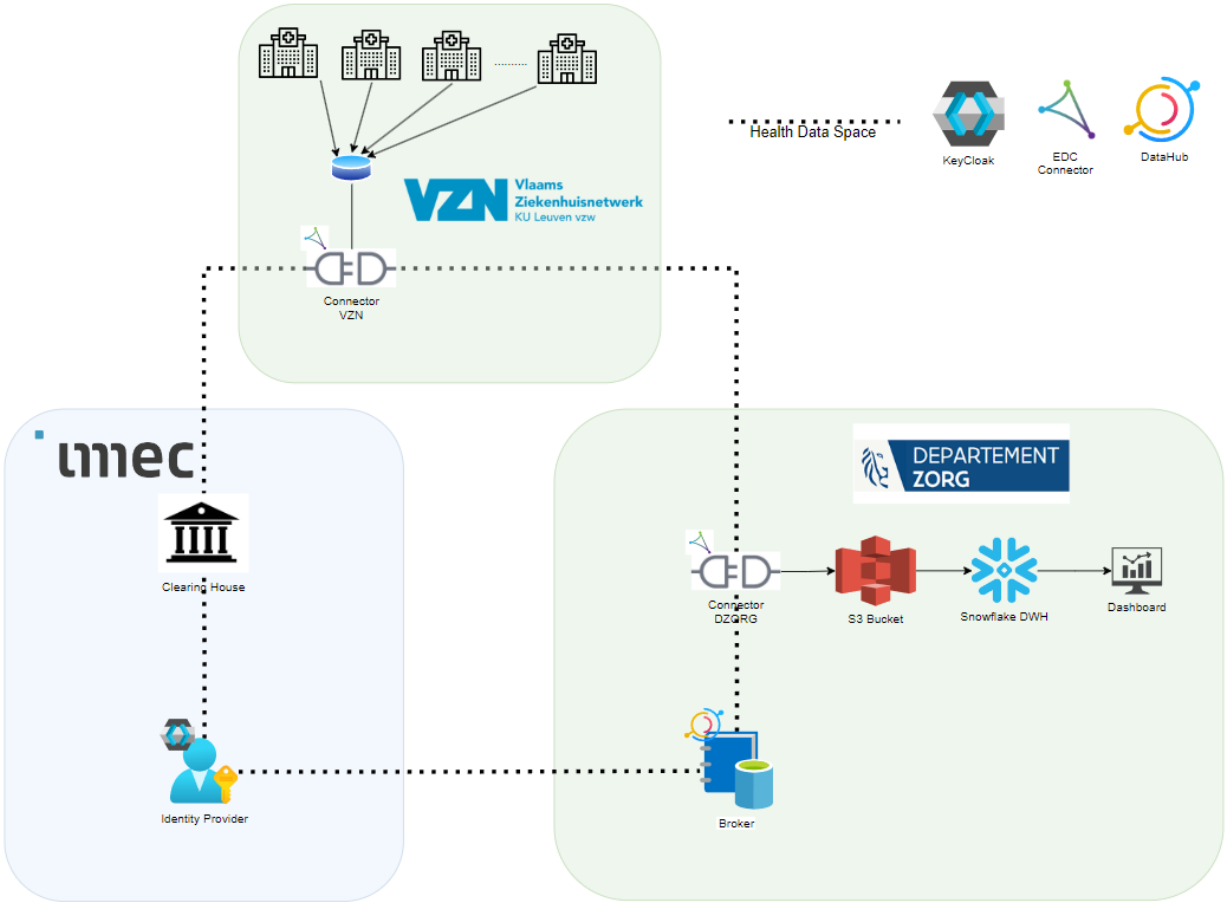
In februari 2024 zat het projectteam samen met dhr. Dirk De Wachter van het Vlaams Instituut voor Kwaliteit van Zorg (VIKZ) om het health data space project toe te lichten. Voor VIKZ is de health data space een zeer interessant initiatief, aangezien zij momenteel met secundaire datasets werken. Dit betekent dat ze met de resultaten van hun analyses niet kunnen terugkoppelen naar de betrokken ziekenhuizen, waardoor deze ziekenhuizen dus ook geen remediërende acties kunnen ondernemen. Voor VIKZ zou het dus heel interessant zijn om deel uit te maken van de health data space en data uit eerste hand van de ziekenhuizen te ontvangen zodat er ook terugkoppeling mogelijk is op basis waarvan gerichte acties genomen kunnen worden.

In juni 2024 werden **gesprekken opgestart met het Vlaams Ziekenhuisnetwerk (VZN)**, meer bepaald met dhr. Dirk De Ridder, directeur kwaliteit. Vanuit VZN was er grote interesse om binnen het huidige onderzoeksproject een use case rond Minimale Ziekenhuis Gegevens (MZG) op te zetten.

5.3.2.2 Uitwerking use case

Voor de specifieke use case met VZN zal in eerste instantie gekeken worden naar **MZG-data rond doorligwonden**. Door de decubitus ulcera te plotten op een dashboard kunnen bepaalde onderzoeksvragen beantwoorden worden, zoals bijvoorbeeld: Wat is de relatie tussen decubitus ulcera en de verblijfsduur in een ziekenhuis? Wat is het verschil met patiënten die geen decubitus ulcera hebben? Voor deze use case zal een stapsgewijze aanpak gebruikt worden. In eerste instantie zal enkel een connector geïnstalleerd worden bij VZN. Vervolgens zal VZN een geaggregeerde MZG-dataset creëren en delen met Departement Zorg via de health data space. Op basis hiervan zal een doorligwondendashboard gecreëerd worden.
Tot slot zal ook een governance structuur uitgewerkt worden. Deze eerste fase van de use case was helaas niet meer haalbaar binnen het huidige R&D-project, aangezien VZN pas in begin 2025 beroep kan doen op de benodigde mankracht voor de installatie van een connector.

In een volgende fase is **uitbreiding van deze use case mogelijk** door partners en datasets toe te voegen, zoals individuele VZN-ziekenhuizen, IMA, FarmaFlux en VIKZ. Bijkomende partners en datasets leiden tot bijkomende inzichten over doorligwonden. En de onboarding van het Vlaams Instituut voor Kwaliteit van Zorg op de health data space kan ervoor zorgen dat het VIKZ rechtstreeks MZG-data kan ophalen bij de ziekenhuizen en op deze manier ook sneller en op een meer gepersonaliseerde manier feedback kan geven aan de ziekenhuizen. (Noot: de vermelde partners moeten nog bevraagd worden over hun mogelijke interesse in deze specifieke use case.)



Figuur 9: VZN use case. Geplande technische opzet.

Betrokken contactpersonen:

- Dirk De Ridder (VZN)
- Marga Lavaerts (VZN)
- Caroline Weltens (VZN)
- Dirk De Wachter (VIKZ)

5.4 POTENTIËLE USE CASES

Verschillende **andere use cases** werden onderzocht. Elk daarvan had een duidelijke link met population health management.

Hoewel er veel interesse was bij de verschillende stakeholders en er heel wat potentieel zat in elke use case, werd in de vroege verkenningsfase of tijdens of na de haalbaarheidsanalyse besloten die niet te weerhouden voor de huidige PoC. Onder andere de complexiteit van de use case, beperkte of onbestaande middelen om tot een projectuitwerking te komen, te weinig buy-in bij de stakeholders ... maakten de use cases minder interessant voor een PoC.

De meeste use cases zijn echter van dien aard dat ze **potentieel interessant** blijven om **in een latere fase** onderdeel uit te maken van de Vlaamse Health Data Space. Voor een beschrijving van de potentiële use cases, verwijzen we naar addenda 5.A-5.Q.

- De Vlaming leeft gezond use case (vooronderzoek)
- BMI-monitor use case (vooronderzoek)
- FHIN use case
- Epilabo & Epilabo Benelux use case
- CM use case
- Janssen Pharmaceutica use case
- VIPA Benelux use case
- Telemonitoring use case
- Sportdata use case
- Diabetes use case met HDA
- HPV use case
- Vitalink Telemonitoring use case
- Genoomdata use case
- Athumi diploma use case
- Ventrical hernia surgery

5.5 MEMORANDUM OF UNDERSTANDING

In het najaar van 2023 werd een **memorandum of understanding (MOU) opgesteld** en voorgelegd aan de stakeholders van de weerhouden en opgestarte use cases (zie bijlagen 5.R-5.V). Dit document had als bedoeling de **verwachtingen van alle betrokken actoren gelijk te zetten**. De MOU licht toe wat het opzet van dit R&D project was en welke use cases het project op dat moment op het oog had, met name Data4PHM, FHIN en Epilabo. Tot slot werden ook de principes opgelijst waaraan het project zich wenste te houden. Hierbij werd voornamelijk onderstreept dat er geen budget voorzien werd voor de use cases. Dat aspect was echter vaak een struikelblok voor stakeholders: ofwel toonden ze interesse in een gezamenlijke use case, maar lieten ze gaandeweg weten dat hun roadmap te vol zat om technische implementaties te doen; ofwel lieten ze bij aanvang al weten dat ze niet in een use case konden stappen zonder dat hier financiële middelen tegenover stonden.

Na opstelling van de MOU in 2023 waren er twee van de drie use cases redelijk zeker: de diabetes use case met **Data4PHM** en een use case met het ziekenhuisnetwerk **FHIN**. De MOU werd in oktober ondertekend door Intego, UAntwerpen, Sciensano en Zorgzaam Leuven, en het Ziekenhuis Oost-Limburg. AZ Delta (FHIN use case) gaf aan de MOU te zullen ondertekenen, maar dit is uiteindelijk niet gebeurd. Van IMA en Farmaflux (Data4PHM use case) kreeg het projectteam te horen dat ondertekening van de MOU moeilijk was zonder meer details over de concrete invulling van de use case. Begin 2024 werd daarom een addendum opgesteld waarin het opzet van de diabetes use case meer in detail werd toegelicht evenals de specifieke verwachtingen die er vanuit het project waren naar IMA en FarmaFlux (vb. deelname aan behoefteanalyse-interviews, installatie connector ...). Bij beide spelers moest de MOU intern passeren langs heel wat beslissingsorganen. De MOU van IMA werd uiteindelijk pas ondertekend eind juni 2024; die van Farmaflux in oktober 2024. De laattijdige ondertekening door FarmaFlux had ook als gevolg dat we van hun kant enkel mock-up data kregen.

Voor **VZN** werd in augustus 2024 een gelijkaardige MOU, met addendum waarin de use case in detail toegelicht werd, uitgewerkt. Als vzw zijn de budgetten van VZN eerder beperkt. Daarom werd eerst de vraag gesteld om een technische werklastinschatting te maken, om te bepalen of VZN deze kost zelf zou kunnen dragen. Uit de werklastinschatting bleek dat de installatie van de connector ten vroegste in het eerste kwartaal van 2025 kon plaatsvinden. De MOU werd tot op heden nog niet ondertekend.

Ook voor **FAQIR** werd een MOU opgesteld (inclusief addendum) in oktober 2024. Deze MOU werd ondertekend in november 2024.

6 JURIDISCHE EN ETHISCHE PRINCIPES

Hoofdstuk 6 over de juridische en ethische principes is onderverdeeld in drie secties, waaronder een overzicht van contractuele kaders die relevant zijn voor het Health Data Space-project, een analyse van het toepasselijke regelgevingskader en, tot slot, een overzicht van relevante ethische principes ter bevordering van het ethisch gebruik en delen van persoonlijke en niet-persoonlijke gegevens.

Het eerste deel van dit juridische hoofdstuk, zijnde sectie 6.1 Contractueel kader, behandelt het gebruik van contractuele afspraken in de context van de Health Data Space. Het gaat dieper in op de afspraken die tussen de betrokken partners gemaakt zouden kunnen of zelfs moeten worden. Deze sectie bevat een generieke beschrijving van wat zou moeten worden opgenomen in de onderling afgesloten overeenkomsten, alsook de *usage policy*. Een omschrijving van hoe de overeenkomsten in het kader van de Health Data Space zich verhouden tot (of afwijken van) andere contractuele overeenkomsten wordt dus opgenomen. Een eerste schets van een *usage policy* wordt als annex (Annex 6.B) opgenomen in dit rapport. Voor een meer diepgaande uitleg en beschrijving van de partijen die betrokken zijn bij de Health Data Space, zie sectie 7 Governance in dit rapport.

In het tweede deel van dit hoofdstuk, namelijk sectie 6.2 Aandachtspunten vanuit de brede legale scan (vl, be, eu), worden de relevante bepalingen in de bestaande wetgeving die van toepassing zijn of kunnen zijn op de Health Data Space uitgelicht. Aangezien het project in ontwikkeling is, beoogt dit deel een overkoepelende scan te bieden voor het relevante juridische kader en houdt het rekening met de relevante regionale (Vlaamse), federale (België) en Europese-Uniewetgeving. In deze context worden in dit hoofdstuk belangrijke juridische definities, concepten/principes en vereisten geschetst die een impact hebben op de vorming van een Health Data Space in Vlaanderen. Verder richt het juridisch gedeelte zich op de belangrijkste juridische kwesties en vragen die zich op het moment van schrijven voordoen en momenteel nader onderzoek behoeven.

Hoewel verschillende rechtsgebieden aan bod komen, ligt de focus op die aspecten die nu cruciaal zijn voor het opstarten van een Health Data Space. Er zal een overzicht worden gegeven van de geldende wetgeving, maar dat zal niet overal in detail worden besproken, alleen waar relevant. Waar dit relevant wordt geacht, wordt aangegeven waar verdere uitwerking in de toekomst nodig zal zijn. Naar aanleiding van het onderzoek naar de wettelijke vereisten worden deze regels vervolgens toegepast op de Health Data Space. Zo biedt dit rapport een diepgaand inzicht in hoe de huidige wetgeving van toepassing is op de specifieke situatie en identificeert het mogelijke juridische hiaten die verdere aandacht vereisen.

Deze opsomming dient als leidraad voor de toekomstige opbouw van een Health Data Space in Vlaanderen, en België bij uitbreiding. Hier moet aan worden toegevoegd dat de huidige analyse zich vooral richt op het secundair gebruik van gegevens in het kader van een Health Data Space. In sectie 6.2.1 Primaire verwerkingen in een Health Data Space worden enkele aspecten besproken die relevant zijn voor het moment waarop de Health Data Space primaire verwerkingsactiviteiten in haar werking zal opnemen. Voorlopig ligt de focus van dit rapport echter op secundaire verwerkingsactiviteiten, omdat ook de governance en technische aspecten voor primair gebruik nog niet volledig zijn afgestemd. Een diepgaande analyse voor wat betreft het primaire gegevensgebruik zal aldus voer zijn voor een follow-up studie.

Het vierde deel van dit hoofdstuk, sectie 6.4 Ethische principes, zal vervolgens, zoals de titel al doet vermoeden, verschillende ethische principes bespreken die potentieel hebben om bij te dragen aan het ethisch gebruik, hergebruik en delen van data. In dit kader zal met name verder worden ingegaan op de vier biomedische principes van Beauchamp en Childress. Deze principes zijn gekozen als basis voor een ethisch kader, omdat ze algemeen aanvaard zijn in de medische ethiek.

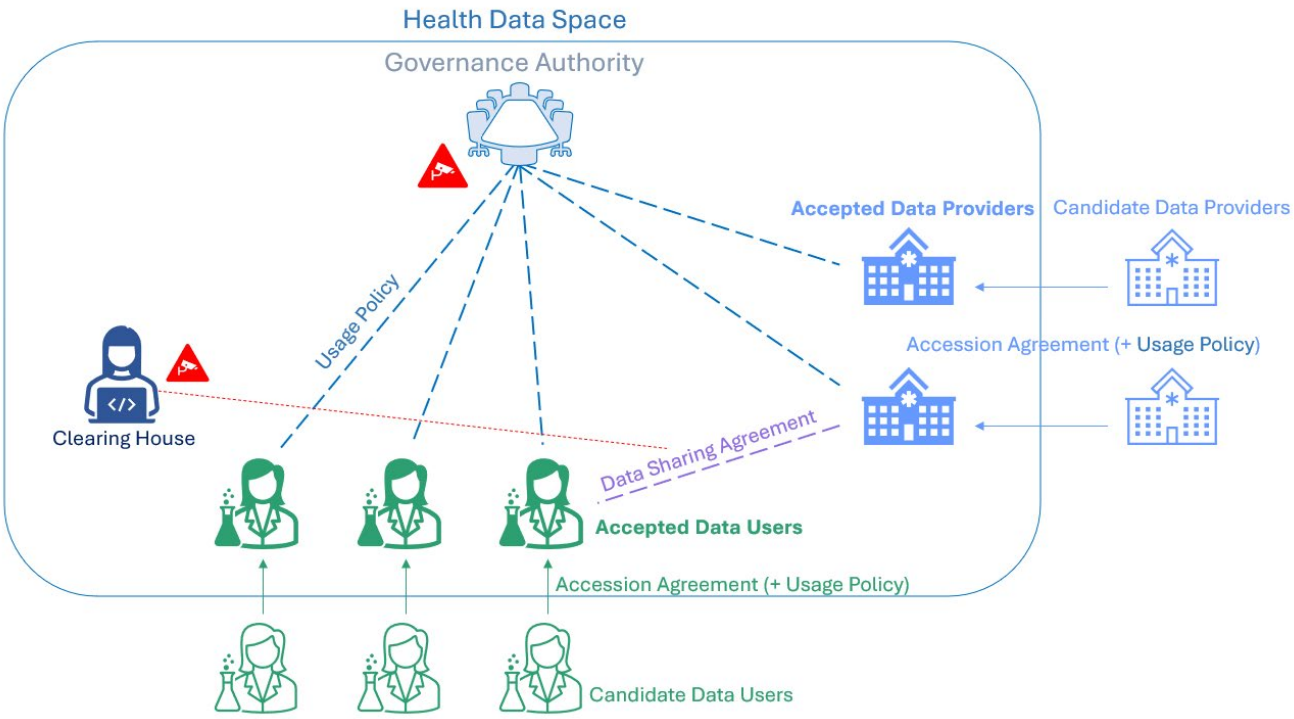
Ten slotte is het belangrijk om aandacht te besteden aan de gebruikte terminologie. Bij het analyseren van de toepasselijke wetgevende instrumenten blijkt dat er niet altijd consistentie is in het gebruik van bepaalde concepten. Ook in de praktijk heerst er niet altijd overeenstemming over welke term precies welke betekenis heeft. In sectie 6.1 Contractueel kader worden begrippen steeds gedefinieerd wanneer zij een specifieke juridische definitie hebben.

6.1 CONTRACTUEEL KADER

Vooreerst zal het nodig zijn in het kader van een Health Data Space om een solide contractueel kader te installeren om de samenwerking tussen alle deelnemende partners zo vlot als mogelijk te doen verlopen. Daartoe kunnen verschillende overeenkomsten worden beschouwd als een essentiële basis voor de succesvolle totstandbrenging en het beheer van een Health Data Space, met name toetredings-overeenkomsten (*accession agreements*), overeenkomsten inzake gegevensuitwisseling (*data sharing agreements*) en gebruiksbeleid (*usage policy*). Het onderstaande kader is gericht op het secundaire gebruik van gegevens in een Health Data Space. Het concrete contractuele kader voor het primaire gebruik van gegevens in de Health Data Space zal moeten worden bekeken wanneer meer zekerheid bestaat over hoe de technische implementatie hiervan plaatsvindt en hoe de concrete gegevensuitwisselingen in het Vlaamse/Belgische zorglandschap in elkaar zitten.

De relevantie van en het verband tussen de relevante overeenkomsten voor wat betreft het secundair gebruik in het kader van de Health Data Space kunnen worden geïllustreerd aan de hand van de volgende figuur.

Overzicht:



Figuur 10: Contracten en usage policies in een data space

In het bijzonder zouden de volgende overeenkomsten kunnen worden opgesteld en overeengekomen in het kader van een Health Data Space.

> **Usage Policy**: Dit zijn de regels die de participanten van de Health Data Space verbinden met de Health Data Space zelf. Hierin staat uitgelegd wat de verschillende rollen en verantwoordelijkheden zijn in de Health Data Space en welke algemene regels door de Data Space participanten moeten worden gevolgd. De hierin opgenomen regels kunnen ofwel afspraken zijn, gemaakt in het kader van de Health Data Space, zoals bijvoorbeeld gedragsregels, alsook omzettingen van vereisten die terug te vinden zijn in wetgeving (Europees of nationaal/regionaal). Dit verschilt van een usage policy binnen de EDC Connector, waar deze specifiek betrekking heeft op een bepaalde data asset. Hier wordt de term breder en overkoepelend gebruikt, van toepassing op alle Health Data Space participanten gelijktijdig, waarbij eventuele verfijningen van toepassing op bepaalde datasets of afgesproken tussen bepaalde participanten nader kunnen worden opgenomen in de Data Sharing Agreement (zie hieronder).
> In **Annex 6.B** wordt een **template** opgenomen voor de usage policy dat een rudimentair overzicht geeft van wat hierin zou kunnen staan. De Annex bevat ook bepalingen die zouden kunnen opgenomen worden in een accession agreement (bij het onboarden van de Health Data Space). Een accession agreement zou alle regels moeten bevatten waaraan participanten moeten voldoen vooraleer zij volwaardig lid van de Health Data Space kunnen worden. Het omvat technische voorschriften opdat de nodige technische infrastructuur kan worden opgezet en de Health Data Space technisch functioneel is, alsook vereisten op juridisch of organisationeel vlak waaraan zij moeten voldoen. Daarnaast kan de accession agreement ook verwijzen naar de regels die van toepassing zijn en waaraan een participant moet voldoen vooraleer volwaardig lid te kunnen worden en blijven van de Health Data Space.
> Deze regels kunnen (ook) opgenomen zijn in de usage policy. Aangezien toetredende participanten ook moeten voldoen aan de regels die zijn opgenomen in de usage policy, zijn deze documenten op dit moment samengevoegd, waar deze later op zichzelf staand horen te zijn. Voor meer informatie omtrent de usage policy, zie sectie 7.4.2 Voorstel: accession agreement.

> **Data Sharing Agreement (DSA)**: Wanneer een data provider en een data consumer beiden akkoord gaan met een toegang tot een dataset (er wordt dus als het ware een gegevensvergunning verleend aan de data consumer door de data provider), kunnen bijkomende specificeringen worden opgenomen in de DSA. Dit geeft hen de ruimte om specifieke beperkingen (bv. specifieke toegelaten doeleinden) op het datagebruik te zetten en te concretiseren hoe er met de gegevens moet worden omgegaan.
> Deze DSA kan bovendien ingaan op de opgenomen rollen en verantwoordelijkheden van de betrokken entiteiten.
> In sommige gevallen vereist de Algemene Verordening Gegevensbescherming (AVG)[24] dat er onderlinge afspraken worden gemaakt tussen partijen.[25] Deze onderlinge afspraken moeten niet verplicht worden opgenomen in een schriftelijke overeenkomst, maar in de praktijk blijkt dit natuurlijk de meest courante vorm. Een DSA in het kader van een Health Data Space zou ook tegemoet kunnen komen aan deze verplichtingen.

6.2 AANDACHTSPUNTEN VANUIT DE BREDE LEGALE SCAN (VL, BE, EU)

In het volgende deel wordt het relevante juridische kader besproken dat in de context van het huidige project is vastgesteld. De analyse en identificatie van regels zijn afgestemd op de specifieke context en fase waarin het project zich op het moment van schrijven bevindt. In dit verband hebben verschillende zaken vormgegeven aan de totstandkoming van het kader, aangezien zij zijn geïdentificeerd als cruciale hoekstenen waaraan aandacht moet worden besteed, zoals essentiële vereisten voor gegevensverwerking

[24] *Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (hierna: AVG).*

[25] *Zie artikel 26.1 AVG voor gezamenlijke verwerkingsverantwoordelijken en artikel 28.3 AVG ten aanzien van de relatie tussen verwerkingsverantwoordelijken en verwerkers.*

en voorwaarden die van invloed zijn op de toegang tot gegevens en die vormgeven aan de vorming van de Health Data Space in kwestie. Met name wat dit laatste betreft, is de vaststelling van een adequaat bedrijfsmodel aangemerkt als een essentiële kwestie die op nationaal en EU-niveau nog onvoldoende aandacht heeft gekregen en die in een speciaal hoofdstuk verder is onderzocht.

Daartoe wordt in het volgende deel kort ingegaan op de Europese datastrategie die door de Europese Commissie is opgesteld. Deze strategie legt de politieke basis voor het bevorderen van een succesvolle data-economie die het hergebruik en de grensoverschrijdende uitwisseling van persoonsgegevens en niet-persoonsgebonden gegevens tussen zowel particuliere en/of publieke actoren in de hele Europese Unie omvat. Vervolgens zullen verschillende wetten worden geschetst, met name op het gebied van gegevensbescherming, gegevensbeheer en kunstmatige intelligentie (AI), waarbij de nadruk zal liggen op kwesties die in dit project zijn geïdentificeerd. De juridische analyse hanteert een **top-downbenadering**, te beginnen met het onderzoek van de relevante EU-wetgeving en haar regels, terwijl we dieper in de discussie duiken om geselecteerde aspecten van het nationale (Vlaamse) recht onder de loep te nemen.

Met name in de hieronder besproken regelgevingsinstrumenten is het taalgebruik niet consistent in alle wetgeving, waardoor een actor vele verschillende hoedanigheden of rollen kan aannemen variërend per wetgevend instrument. Deze variatie in terminologie is niet bevorderlijk voor de duidelijkheid van het Europese rechtskader. Deze termen zullen daarom altijd in de respectievelijke hoofdstukken worden toegelicht. Bij het lezen van sectie 6.2 Aandachtspunten vanuit de brede legale scan (vl, be, eu) is het daarom belangrijk om aandacht te besteden aan de specifieke betekenis van elke term.
Bovendien komen de benamingen gekozen in dit project niet altijd overeen met de juridische terminologie in de wetgeving. Een data user in het kader van de op te stellen Health Data Space is bijvoorbeeld niet zomaar hetzelfde als een gegevensgebruiker in het kader van de Data Governanceverordening (DGA).

6.2.1 Primaire verwerkingen in een Health Data Space

Artikel 1 van de EHDS-verordening benadrukt dat het de bedoeling is van een Health Data Space om zowel verwerkingen van elektronische gezondheidsgegevens te faciliteren voor primair als secundair gebruik.[26] Primair gebruik wordt omschreven in de verordening als "*the processing of electronic health data*[27] *for the provision of healthcare, in order to assess, maintain or restore the state of health of the natural person to whom those data relate, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for the relevant social, administrative or reimbursement services."*[28] De invalshoek bij primair gebruik is dus anders, dan bij het secundair gebruik van gegevens, waarmee "*the processing of electronic health data for the purposes set out in Chapter IV of this Regulation, other than the initial purposes for which they were collected or produced."*[29] Op termijn zullen dus de beide gebruiken, zowel primair, als secundair, een plaats krijgen in het kader van de Health Data Space. Ten tijde van het schrijven van het rapport ligt de nadruk meer op het secundaire gebruik van gegevens (zie ook de use cases hierrond in hoofdstuk 5 Use cases). Dit doet niet af aan het belang van het primaire gebruik van gegevens in de toekomstige Health Data Space. Er moet daarom ook gekeken worden naar de wetgeving die van toepassing is op de zorgrelaties en hoe een patiëntendossier moet worden beheerd bijvoorbeeld. Deze regelgeving heeft immers een weerslag op de implementatie van de EHDS. Daarom vindt hieronder een gelimiteerde analyse plaats van welke instrumenten bepalend kunnen zijn om vorm te geven aan hoe de Health Data Space naar de toekomst toe verder dient te evolueren. Hierbij dient te worden benadrukt dat diepgaand onderzoek vereist zal zijn, waarbij bovendien in communicatie wordt getreden met de actoren in het veld.

---

[26] Artikel 1 van de EHDS-verordening zoals opgenomen in het Corrigendum to the position of the European Parliament adopted at first reading on 24 April 2024 with a view to the adoption of Regulation (EU) 2024/… of the European Parliament and of the Council on the European Health Data Space (Hierna: EHDS).

[27] Het begrip elektronische gezondheidsgegevens wordt gedefinieerd en verder besproken in ***Fout! Verwijzingsbron niet gevonden.****.*

28 Artikel 2.2.d) EHDS.

[29] Artikel 2.2.e) EHDS.

Hoe de informatie-uitwisseling in de praktijk verloopt, is immers cruciaal om mee op te nemen in de opbouw van een volwaarde Health Data Space, waarbij ook het primair gebruik centraal staat.

6.2.1.1 Informatie-uitwisseling tussen arts en patiënt

Tussen de gezondheidsbeoefenaar en zijn patiënt bestaat er een vertrouwensrelatie.
De gezondheidsbeoefenaar verwerkt immers uiterst sensitieve gegevens van de patiënt. In dit verband zijn bepalingen opgenomen in het gezondheidsrecht om het gegevensbeschermingsrecht te incorporeren. Veel van de principes van de AVG komen overeen met de basisbeginselen omtrent gegevensverwerking in het gezondheidsrecht.
Om te beginnen moet een gezondheidsbeoefenaar in beginsel immers steeds een **geïnformeerde toestemming** hebben om *toegang* tot persoonsgegevens betreffende de gezondheid van de patiënt te verschaffen.[30] Deze toegang is bovendien gelimiteerd tot enkel die gezondheidsbeoefenaars die ook effectief een therapeutische relatie met de patiënt hebben.[31] Deze vereiste wordt ook gereflecteerd in de rechten van de patiënt, waar wordt gesteld dat iedere patiënt het recht heeft om geïnformeerd, voorafgaandelijk en vrij toe te stemmen met iedere tussenkomst van de gezondheidsbeoefenaar, al gaat dit meer om het effectief toedienen van gezondheidszorg. Deze toestemming moet bovendien uitdrukkelijk zijn.[32] Een uitzondering op deze geïnformeerde toestemming ten aanzien van een tussenkomst van een gezondheidsbeoefenaar bestaat in het geval van nood.[33] Dit zijn al aspecten die in het kader van een Health Data Space moeten worden ingebouwd; wanneer raadplegingen plaatsvinden voor primair gebruik van de gezondheidsgegevens, dan zullen enkel gezondheidsbeoefenaars die effectief de patiënt behandelen toegang mogen verkrijgen. Eventueel kan het clearing house hierbij optreden als een controlerende factor.
Enkel al uit de voorgaande paragraaf blijkt dat het begrip 'toestemming' in het gezondheidsrecht een doos van Pandora blijkt te zijn. Nagenoeg iedere sectorspecifieke wetgeving bevat bepalingen omtrent de toestemming van een patiënt.[34]
In de tekst van de EHDS-verordening wordt de mogelijkheid geboden om slechts deels toegang te geven tot hun elektronische gezondheidsgegevens.[35]

Daarnaast zijn er ook beperkingen opgelegd op het gebruik van patiëntgegevens:

1. De finaliteit van de toegang bestaat uit het verstrekken van gezondheidszorg;
2. De toegang is **noodzakelijk** voor de continuïteit en kwaliteit van het verstrekken van gezondheidszorg;
3. De toegang beperkt zich tot de gegevens die dienstig en pertinent zijn in het kader van het verstrekken van gezondheidszorg.[36]

Uit de Kwaliteitswet vloeit dat er een controle moet bestaan op wie toegang heeft tot het patiëntendossier[37]. Wellicht zal in het kader van een Health Data Space dus eveneens een dergelijke controle moeten worden opgericht. Hiervoor is de rol van het clearing house wellicht onontbeerlijk, aangezien hier een gedetailleerd overzicht wordt gegenereerd waarin wordt weergegeven wanneer welke entiteit bepaalde data raadpleegt.

---

[30] *Artikel 36 van de wet inzake de kwaliteitsvolle praktijkvoering in de gezondheidszorg van 22 april 2019 (hierna: Kwaliteitswet).*

[31] *Artikel 37 Kwaliteitswet.*

[32] *Artikel 8 van de wet betreffende de rechten van de patiënt van 22 augustus 2002.*

[33] *Artikel 39 Kwaliteitswet.*

[34] *Zie voetnoten 30 en 32. Zie als voorbeeld daarnaast ook eventueel artikel 14 Decreet tot oprichting van het platform Vitalink van 8 juli 2022.*

[35] *Overweging 17 en artikelen 3 en 8 EHDS.*

[36] *Artikel 38 Kwaliteitswet.*

[37] *Gegevensbeschermingsautoriteit (GBA). (2019). Nota over de verwerking van gegevens uit patiëntendossiers, DOS-2019-04611.*

Het patiëntendossier wordt verder beschermd door een **deontologisch opgelegde vertrouwelijkheidsverplichting** op de arts.[38]

In het Vlaamse zorglandschap wordt al ingezet op gegevensdeling. Interessant hierbij is de rol van het **eHealth-platform**, dat bevoegd is voor het ter beschikking stellen van een verwijzingsrepertorium met de aanduiding bij welke actoren in de gezondheidszorg welke types van gegevens worden bewaard met betrekking tot welke patiënten. Het is wel mogelijk dat een patiënt zich tegen deze verwijzingen uitdrukkelijk verzet.[39] Ook **Vitalink** heeft een rol te spelen in de communicatie van patiëntgegevens met andere zorgverstrekkers.[40] Zij zijn onder meer bevoegd voor het faciliteren van wetenschappelijke of statistische studies.[41] Een volwaardige health data space zou met de reeds bestaande initiatieven rekening moeten houden en bekijken hoe deze eventueel te integreren zijn.

Daarnaast moet gekeken worden naar de **sectorspecifieke wetgeving** die telkens van toepassing is op een bepaalde zorgrelatie of op specifieke zorgbeoefenaars. Deze wetgeving bepaalt nader hoe met bepaalde patiëntdata moet worden omgegaan, alsook welke informatie over de zorgbeoefenaars zelf moet duidelijk zijn. Zo kunnen de persoonsgegevens over de zorgbeoefenaars zelf ook leiden tot waardevolle inzichten.[42] Enkele voorbeelden hiervan zijn het Woonzorgdecreet[43] en het Eerstelijnszorgdecreet[44]. Zo gaat het Woonzorgdecreet dieper in op het verzamelen van gegevens omtrent de gebruikers van woonzorgvoorzieningen, hun mantelzorgers, de personeelsleden, vrijwilligers, verenigingswerkers en de bestuurders van de woonzorgvoorziening of vereniging.[45] Dit allemaal om een beter overzicht te krijgen over de zorg en de nodige ondersteuning aan patiënten.

6.2.1.2 Informatie-uitwisseling ten gevolge van onderzoek

(Wetenschappelijk) onderzoek kan ook direct op mensen worden uitgevoerd, doorgaans in de vorm van klinische proeven met patiënten of proefpersonen. Ook in dit verband zijn er talloze wetgevende instrumenten van toepassing. Het gaat hier om **primaire verwerkingsactiviteiten**; dit zijn proeven waaraan de patiënt/proefpersoon rechtstreeks deelneemt. Een verschil kan worden gemaakt met retrospectieve proeven, waarbij er aan de slag kan worden gegaan met reeds bestaande data – typisch secundair gebruik van gegevens. Aangezien het in dat geval gaat om retrospectieve studies, is niet alle hieronder besproken wetgeving van toepassing. Zo zal bijvoorbeeld de Wet Klinische Proeven[46] niet van toepassing zijn, omdat deze louter observatieve onderzoeken betreft (ook al wordt misschien aan de slag gegaan met data die ooit door een observatief onderzoek is gegenereerd) en is ook niets steeds een **advies van een ethisch comité** verplicht.[47]

Het wordt steeds aangeraden om samen te werken met een **data access committee** (DAC) om toegang tot en het beheer van de gegevens te organiseren.[48] Het is dan ook raadzaam om een dergelijke instantie te creëren in het kader van de Health Data Space, waarbij het DAC bestaat uit multidisciplinaire leden,

---

[38] GwH, 26 september 2013, nr. 127/2013.

[39] Artikel 5, 4°, b) van de wet houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen van 21 augustus 2008.

[40] Vlaanderen (Vlaamse Overheid). Vitalink, het digitaal platform voor het delen van gezondheidsgegevens.; Artikel 3, Decreet tot oprichting van het platform Vitalink van 8 juli 2022.

[41] Artikel 4, lid 1, 6°, Decreet tot oprichting van het platform Vitalink van 8 juli 2022.

[42] Artikel 23 Decreet betreffende de organisatie van de eerstelijnszorg, de regionale zorgplatformen en de ondersteuning van de eerstelijnszorgaanbieders van 26 april 2019 (hierna: Eerstelijnszorgdecreet).

[43] Decreet betreffende de woonzorg van 15 februari 2019 (hierna: Woonzorgdecreet).

[44] Eerstelijnszorgdecreet.

[45] Artikel 59 Woonzorgdecreet.

[46] Wet betreffende klinische proeven met geneesmiddelen voor menselijk gebruik van 7 mei 2017.

[47] Zie Hoofdstuk VIII van de wet inzake experimenten op de menselijke persoon van 7 mei 2004 (hierna: Experimentenwet).

[48] Het oprichten van en samenwerken met een DAC wordt niet verplicht in de Belgische wetgeving. In de praktijk worden deze echter wel opgericht en gebruikt. Zie bijvoorbeeld https://www.uzleuven.be/nl/dac.

waaronder experts in juridische, ethische, en technische aspecten van datagebruik. Het DAC zou als voornaamste taak hebben om te evalueren of bepaalde verwerkingsactiviteiten voldoen aan de AVG en nationale regelgeving, of er ethische principes in de weg staan van datagebruik en of er eventueel bijkomende randvoorwaarden voor het datagebruik genoodzaakt zijn. Dit is voornamelijk van belang in een context dat er gevoelige of vertrouwelijke informatie wordt verwerkt, zoals gezondheids- en genetische gegevens.

Wanneer er sprake is van primair gebruik van gegevens in het kader van onderzoek met patiënten/proefpersonen moeten bepaalde aspecten in verband met de gegevensverwerking in acht genomen worden. Zo kan de toepasselijke wetgeving onderverdeeld worden in twee "soorten" van regelgeving. Allereerst kan **de wetgeving aangaande onderzoek** van toepassing zijn; met name de Wet Experimenten van 7 mei 2004[49], de Verordening 536/2014 inzake klinische proeven[50] en de implementatie wet rond klinische proeven van 7 mei 2017[51], alsook de Verordening 2017/745 aangaande medische hulpmiddelen[52] en diens implementatiewet van 22 december 2020[53] en het bijhorende KB van 18 april 2021[54], en ten slotte de Richtlijn van 31 maart 2024 tot vaststelling van kwaliteits- en veiligheidsnormen voor het doneren, verkrijgen testen, bewerken, bewaren en distribueren van menselijke weefsels en cellen[55], evenals de wet van 19 december 2008 inzake het verkrijgen en het gebruik van menselijk lichaamsmateriaal met het oog op de geneeskundige toepassing op de mens of het wetenschappelijk onderzoek[56]. Deze regelgeving bespreekt hoe het onderzoek dient te verlopen, wat de voorschriften zijn en hoe de proefpersonen moeten worden behandeld. Daarnaast is **de wetgeving met betrekking tot gegevensaspecten** van toepassing, waarbij voornamelijk de in dit hoofdstuk aangehaalde wetgeving van tel is; de Datagovernanceverordening (DGA)[57], Algemene Verordening Gegevensbescherming (AVG)[58] en EHDS-verordening (EHDS)[59]. Dit wordt aangevuld door de Belgische implementatiewetgeving, zoals de Wet verwerking Persoonsgegevens (WVP) of de wet tot omzetting van de DGA. Beide soorten wetgeving behandelen andere aspecten; waar de eerste soort wetgeving meerdere aspecten reguleert (zoals ook de veiligheid van proefpersonen bijvoorbeeld), richt de tweede soort zich louter op de gegevensaspecten.
Zo is er een verschil tussen de geïnformeerde toestemming in het kader van klinische proefprojecten en de toestemming onder de AVG. Er zijn echter ook raakvlakken tussen de twee; zo bespreekt de wet van 29 december 2008 inzake het verkrijgen en het gebruik van menselijk lichaamsmateriaal de aanbeveling om te anonimiseren wanneer gegevens worden verwerkt met het oog op onderzoek.[60] Een zekere overlap bestaat dus wel degelijk.

[49] *Zie de Experimentenwet.*

[50] *Verordening (EU) 536/2014 betreffende klinische proeven met geneesmiddelen voor menselijk gebruik en tot intrekking van Richtlijn 2001/20/EG van 16 april 2014.*

[51] *Wet betreffende klinische proeven met geneesmiddelen voor menselijk gebruik van 7 mei 2017.*

[52] *Verordening (EU) 2017/745 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EH, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad, van 5 april 2017 (hierna: MDR).*

[53] *Wet betreffende medische hulpmiddelen van 22 december 2020.*

[54] *KB betreffende klinische onderzoeken van medische hulpmiddelen van 18 mei 2021.*

[55] *Richtlijn 2004/23/EG tot vaststelling van kwaliteits- en veiligheidsnormen voor het doneren, verkrijgen, testen, bewerken, bewaren en distribueren van menselijke weefsels en cellen van 31 maart 2004.*

[56] *Wet inzake het verkrijgen en het gebruik van menselijk lichaamsmateriaal met het oog op de geneeskundige toepassing op de mens of het wetenschappelijk onderzoek van 19 december 2008.*

[57] *Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 20 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724.*

[58] *Verordening (EU) 2018/1807 van het Europees Parlement en de Raad inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie van 14 november 2018.*

[59] *Verordening (EU) 2024/… van het Europees Parlement en de Raad van … on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847.*

[60] *Zie ook Raadgevend Comité voor Bio-ethiek, 2003.*

6.2.1.3 Bevoegdheidsverdeling ten aanzien van het organiseren van gezondheidszorg

De bevoegdheid om gezondheidszorg te organiseren ligt niet bij louter één autoriteit in België.
De grootste verantwoordelijkheid ligt bij de gemeenschappen, aangezien deze bevoegd zijn voor gezondheidsopvoeding, preventieve gezondheidszorg, en lokale zorgdiensten,[61] mits deze niet rechtstreeks gekoppeld zijn aan de verplichte ziekte- en invaliditeitsverzekering wat dan weer federale materie is[62].

Praktische verdeling tussen Vlaamse en federale overheid:

> Federale bevoegdheden
  - Basisfinanciering van de gezondheidszorg (via RIZIV).
  - Normen voor ziekenhuiswerking, medische beroepen en geneesmiddelen.
  - Orgaantransplantatie, klinische proeven en medische technologie.
  - Ethische vraagstukken zoals euthanasie en abortus.

> Vlaamse bevoegdheden (en andere gemeenschappen)
  - Preventieve gezondheidszorg (zoals vaccinatiecampagnes en rookpreventie).
  - Gezondheidsbevordering en voorlichting.
  - Organisatie van lokale zorgdiensten en woonzorgcentra.
  - Gezinszorg, ouderenzorg en revalidatie.
  - Ondersteunende functies zoals eerstelijnszorg en geestelijke gezondheidszorg.

In het kader van de Health Data Space wordt het interessant om te volgen hoe de verschillende bevoegdheden zich uiteindelijk zullen manifesteren. Het oprichten van een Health Data Access Body (HDAB) (zie sectie 6.2.6 EHDS-verordening) bijvoorbeeld illustreert hoe deze bevoegdheden de werking van de Health Data Space kunnen beïnvloeden. Een mogelijk scenario is dat er meerdere entiteiten ontstaan, bijvoorbeeld een Vlaamse én een federale, waarbij een van deze entiteiten fungeert als Europees aanspreekpunt, wat de governance structuur van de Health Data Space beïnvloedt. Dit zou vergelijkbaar zijn met de huidige rolverdeling tussen de federale Gegevensbeschermingsautoriteit[63] en de Vlaamse Toezichtscommissie[64].

Een andere vraag is of een federale HDAB bevoegd zou zijn om beslissingen te nemen over gemeenschapsmateries. “Preventieve gezondheidszorg” en “gezondheidsbevordering” vallen bijvoorbeeld onder de bevoegdheid van de gemeenschappen. Kan een federale HDAB in dat geval vergunningen afgeven voor gegevensgebruik ten behoeve van statistisch onderzoek, bijvoorbeeld voor *population health management*, wat wellicht onder deze Vlaamse bevoegdheden kan worden gesitueerd? Ook deze aspecten zijn nog nader te onderzoeken en afhankelijk van politieke keuzes in de toekomst.

6.2.1.4 Gezondheidsrecht in de Health Data Space

In de Health Data Space zal naast de wetgeving die van toepassing is op het gebruik van gegevens, ook de bepalingen aangaande het gezondheidsrecht zoals hierboven vermeld in rekening moeten worden genomen. In welke mate de Health Data Space zelf verantwoordelijk is voor de naleving hiervan, is op dit moment echter niet duidelijk. In principe zijn de bepalingen die de relaties met patiënten en proefpersonen regelen immers van toepassing op de zorgbeoefenaars of wetenschappers, en niet op de Health Data Space als dusdanig (zie sectie 6.2.1.4 Gezondheidsrecht in de Health Data Space).

---

[61] *Artikel 5, §1, I, eerste lid, Bijzondere Wet tot Hervorming der Instellingen van 8 augustus 1980 (hierna: BWHI) juncto artikel 128 Gecoördineerde Grondwet (hierna: Gw.).*

[62] *Artikel 5, §1, I, tweede lid, BWHI.*

[63] *Zie https://www.gegevensbeschermingsautoriteit.be/burger.*

[64] *Zie https://www.vlaanderen.be/vlaamse-toezichtcommissie.*

In een follow-up studie kan diepgaandere aandacht uitgaan naar hoe en of de bepalingen opgenomen in het 'primaire' gezondheidsrecht de werking van de Health Data Space impacteren. Aangezien de focus in het huidige project het secundaire gebruik van gegevens is, zal dit rapport hier niet verder op in gaan. Al valt een eerste lacune alvast te worden opgemerkt, namelijk dat het wetgevend landschap ondoorzichtig en moeilijk te doorkammen is. Aangezien de bepalingen verspreid zijn over sectorale wetgeving, waarbij ieder(e) type zorg of soort zorgbeoefenaar onder eigen wetgeving valt, is het lastig een overzicht te geven van alle toepasselijke wetgeving. Zo bestaat er een Eerstelijnszorgdecreet, maar ook een Woonzorgdecreet voor de woonzorgcentra, een decreet voor de geestelijke gezondheidszorg[65], enzovoort. Deze wetgeving blijkt prima facie geen obstakels te bevatten ten aanzien van een health data space, maar vergt wel onderzoek over hoe ze kan worden geïntegreerd in de werking van een health data space. Er valt te denken aan vastgelegde bewaartermijnen die ook in het kader van de Health Data Space moeten worden gerespecteerd,[66] en reeds bestaande initiatieven, zoals het eHealth-platform en Vitalink, die eventueel preferabel in de Health Data Space zouden moeten opgenomen worden.

Los hiervan is het duidelijk dat aangaande het primaire gebruik van gezondheidsgegevens er een alomvattend overzicht ontbreekt welke wetgeving, met al de implementatiewetgeving die erbij hoort, nu precies per sector bestaat. Het blijkt een uitdaging te zijn om een opsomming te geven van decreten, beraadslagingen, enzovoort, die allemaal van toepassing zijn op het uitwisselen van gegevens in de gezondheidscontext. Een dergelijk overzicht is vooral van belang wanneer de Health Data Space op termijn zich ook uitbreidt naar de context van primair gegevensgebruik. Daarnaast is het daarom ook onduidelijk hoe secundair gebruik van gezondheidsgegevens dient te verlopen. Hier is niet veel wetgeving over.

6.2.2 Vennootschapsrecht

Het kiezen van een organisatievorm voor een Health Data Space vereist zorgvuldige afweging van verschillende factoren, zoals de precieze functie en het vooropgestelde doel van de HDS, wie deelneemt aan de organisatie/stichting ervan, etc. Hieronder volgt een overzicht van enkele mogelijke organisatievormen, samen met de voor- en nadelen ervan, rekening houdend met de specifieke doelen van een HDS, zoals ze op het moment van schrijven van toepassing zijn.

Dit onderdeel bevat geen exhaustieve opsomming van elke mogelijke organisatievorm, maar richt zich op de meest relevante organisatievormen binnen het Belgische en, in bredere zin, het Europese vennootschapsrecht die van toepassing zijn op de implementatie van de HDS, op het moment van schrijven. Deze benadering stelt ons in staat om de potentiële voor- en nadelen van de hieronder beschreven organisatievormen te bespreken en mee te nemen in de verdere ontwikkeling van het project.

6.2.2.1 Algemeen

In onderstaande figuur wordt een overzicht van enkele organisatievormen met hun kenmerken weergegeven. Hoewel dit geen exhaustieve oplijsting is, weerspiegelt het de meest voorname aspecten die in acht moeten/kunnen worden genomen bij het vaststellen van welke organisatievorm het meest geschikt is voor een Health Data Space. Voor een gedetailleerdere toepassing van deze elementen, zie ook sectie 7.2.3.2 Financiering en businessmodel volgens het ecosysteem.

Voor dit rapport zijn zowel Belgische als Europese rechtsvormen onderzocht. Hoewel de Europese organisatievormen in een later stadium van belang kunnen zijn voor de ontwikkeling van de HDS, is op het moment van schrijven duidelijk dat enkel een Belgische organisatievorm relevant is voor de huidige visie. Dit komt doordat de HDS voorlopig enkel gericht is op Vlaanderen, met desgewenst een uitbreiding naar een Belgische context. Daarom bevat dit onderdeel een algemeen overzicht van de Europese organisatievormen, waarbij de nadruk ligt op de nationale, Belgische organisatievormen die op dit moment het meest geschikt zijn.

[65] *Decreet betreffende de centra voor geestelijke gezondheidszorg van 18 mei 1999.*

[66] *Zie bijvoorbeeld artikel 9 Decreet tot oprichting van het platform Vitalink van 8 juli 2022.*

In het kader van het huidige onderzoek heeft deze studie zich voornamelijk gericht op onderzoek naar de vzw en de stichting wat betreft de *non-for-profit* organisatievormen en de BV voor wat betreft de *for-profit* organisatievormen.

	VZW (*non-profit association*)	IVZW (*international non-profit association*)	Private Stichting (*foundation*)	BV & NV (*for-profit*)	SE & SCE
Doel	Belangeloos doel (geen winstnastreving)	Belangeloos doel (geen winstnastreving) met internationale relevantie[67]	Belangeloos doel, bepaald door stichter(s)	Winstnastrevend oogmerk[68]	Grensoverschrijdend project
Rechtspersoonlijkheid	RPH + beperkte AH	Enkel na uitvaardiging van een KB	RPH + beperkte AH	RPH + beperkte AH	RPH + beperkte AH
Stichting	Minstens twee leden. Geen minimumkapitaal vereist.		Kan in samenwerking (met meerdere stichters), of eenzijdig. Geen minimumkapitaal vereist.	NV: 61.500 euro startkapitaal BV: geen minimumkapitaal vereist	SE: 120.000 euro startkapitaal SCE: 30.000 euro startkapitaal Voldoende startkapitaal vereist.
Organen	Bestuursorgaan[69] (minstens twee/drie bestuurders) + AV	Kan vrij georganiseerd worden in de statuten.	Verplicht bestuursorgaan met minstens één bestuurder) + Geen AV, kan wel bijkomende organen creëren zoals bv. een raad van toezicht die controle uitoefent op het bestuursorgaan.	Bestuursorgaan + AVA	
Toegang tot kapitaal	Minder voorspelbaar vanwege de afhankelijkheid van donaties, subsidies of lidmaatschap vergoedingen.	Idem VZW	Idem VZW	Ophalen van kapitaal is relatief eenvoudig door nieuwe aandelen uit te geven.	
Tax	Rechtspersonenbelasting	Idem VZW	Rechtspersonenbelasting	Vennootschapsbelasting	

[67] *Moet de belangen van de wereldgemeenschap dienen en bijdragen tot de verwezenlijking van de doelstellingen en principes van het VN-Handvest en het Statuut van de Raad van Europa + Grensoverschrijdend effect of voordeel.*

[68] *Al kan het naast het winstnastrevende oogmerk ook een belangeloos doel op het oog hebben.*

[69] *Het bestuursorgaan is bevoegd om alle handelingen te verrichten die nodig of dienstig zijn tot verwezenlijking van het doel van de vereniging, behoudens die handelingen die volgens de wet behoren tot de uitsluitende bevoegdheid van de AV.*

6.2.2.2 Europese organisatievormen

6.2.2.2.1 SE & SCE

De **Europese Naamloze Vennootschap (SE)** en de **Europese Coöperatieve Vennootschappen (SCE)** worden gekenmerkt door de eenvoud waarmee grensoverschrijdende samenwerking binnen de Europese Unie kan worden gerealiseerd. Voor beide vennootschapsvormen is het vereist dat rechtspersonen (en in het geval van de SCE eventueel ook natuurlijke personen) uit verschillende lidstaten betrokken zijn bij de oprichting.

Aangezien dit in het kader van de HDS voorlopig niet van toepassing is, hoeft er momenteel geen rekening gehouden te worden met deze vennootschapsvormen. In de toekomst, indien er samenwerkingsverbanden ontstaan met andere buitenlandse Europese Data Spaces, kan het zinvol zijn om opnieuw te overwegen of samenwerking via een SE of SCE een geschikte optie is.

6.2.2.2.2 EESV

Een **Europees Economisch Samenwerkingsverband (EESV)** is bedoeld om samenwerkingen tussen verschillende bedrijven te vereenvoudigen. Ook hier is het internationale karakter van haar oprichters vereist, wat een uitsluiting van de overwogen organisatievormen in het kader van een HDS met zich mee brengt.

6.2.2.3 Belgische non-profit organisatievormen

6.2.2.3.1 VZW (non-profit)

De vzw wordt besproken in Boek 9 van het Wetboek van Vennootschappen en Verenigingen (WVV)[70].

Doel

Een vzw heeft **een belangeloos doel**, wat betekent dat er geen winststreven is (i.e. *non-for-profit*) (artikel 1:2 WVV). Dit sluit niet uit dat de vzw winst kan maken, maar deze winst mag niet worden verdeeld onder de leden.[71] De afwezigheid van een winstoogmerk impliceert een verbod op het toekennen van financieel voordeel aan oprichters, leden, bestuurders of andere betrokkenen, zowel direct (zoals de uitkering van dividenden) als indirect (bijvoorbeeld door diensten aan te bieden tegen prijzen die lager zijn dan marktconform), tenzij dit bijdraagt aan het verwezenlijken van het belangeloos doel. Overtredingen van dit principe, waarbij de winst wel wordt nagestreefd, leiden tot de nietigheid van dergelijke transacties (artikel 1:3, *in fine*, WVV). Het vastgestelde doel moet worden opgenomen in de statuten[72].

Oprichting

In tegenstelling tot vennootschapsvormen vereist een vzw geen minimum startkapitaal, wat het toegankelijker maakt om op te richten. De oprichting van een vzw moet wel gepaard gaan met het ter beschikking stellen van een vermogen, of op zijn minst het engagement daartoe, en dit ten einde het doel van de vzw te kunnen bereiken. Het is essentieel dat de vzw over voldoende activa beschikt om haar in staat te stellen haar doel te bereiken, al vereist de wet geen minimumbedrag hiervoor. Het vermogen van de vzw wordt uitsluitend ingezet in het belang van de vzw zelf. Met andere woorden, het toegekende vermogen moet in verhouding staan tot het nagestreefde doel en voldoende zijn om dit belangeloze doel te kunnen bereiken.[73]

---

[70] *Wetboek van vennootschappen en verenigingen (hierna: WVV).*

[71] *D. Van Gerven. (2022). Verenigingen, vennootschappen en stichtingen, Wolters Kluwer Belgium, Mechelen, p. 367 (hierna: D. Van Gerven, Verenigingen, vennootschappen en stichtingen.); artikel 1:2 WVV.*

[72] *Artikel 2:9, §2, 4° WVV.*

[73] *Zie FOD Justitie, VZW.*

Interne organisatie
De vzw bestaat uit een algemene vergadering (AV) waarin de stichtende leden en de werkende leden zetelen en een bestuursorgaan, dat minstens uit drie bestuurders bestaat,[74] dat wordt samengesteld door de AV[75]. In principe zijn er minstens drie bestuursleden, al kan hier statutair van worden afgeweken. Het dagelijkse bestuur kan aan een of meer (derde) personen worden opgedragen.[76]

Formalisme
Over het algemeen is de vzw minder onderworpen aan formele vereisten, waardoor de structuur flexibeler en eenvoudiger is in vergelijking met vennootschapsvormen. In vergelijking met de stichting is de vzw dan weer sterker geformaliseerd.

Belastingen
Een vzw valt meestal onder het inkomstenbelastingregime voor rechtspersonen. Onder dit regime moet de vereniging enkel roerende voorheffing betalen (d.w.z. inkomsten uit spaarrekeningen, termijndepositorekeningen, leningen, obligaties, aandelen, beleggingen, fondsen …) (tot 30%) en onroerende goederen (roerende voorheffing op kadastrale inkomsten of huurinkomsten belast tegen 20%). Opdat een vzw onderworpen zou zijn aan de rechtspersonenbelasting, mag ze:

1. Geen bedrijf hebben en
2. Geen activiteiten hebben met winstoogmerk.

De belastingadministratie legt deze twee voorwaarden als volgt uit:

> Geen onderneming exploiteren: geen industriële, commerciële of agrarische onderneming op duurzame wijze, meer bepaald door een reeks handelingen die nodig zijn voor het produceren of verhandelen van goederen of het verlenen van diensten.
> Geen winstgevende activiteiten: geen activiteiten die worden gekenmerkt door een voortdurende activiteit, bestaande uit handelingen van industriële, commerciële of agrarische aard die zo vaak worden herhaald dat ze een beroep vormen of door het toepassen van industriële of commerciële methoden.

Houd er echter rekening mee dat als deze activiteiten (i) op zichzelf staande of uitzonderlijke activiteiten zijn of (ii) incidenteel of niet volgens industriële of commerciële methoden plaatsvinden, deze activiteiten niet als activiteiten met winstoogmerk worden beschouwd. Dit vereist een analyse per geval (toewijzing van personeel, reclame, deelname aan beurzen, verkoopstrategie …).

Wellicht vallen de beoogde activiteiten van een Health Data Space hieronder, waardoor deze slechts onderhevig zouden zijn aan de rechtspersonenbelasting. Het systeem van de rechtspersonenbelasting zou een stuk eenvoudiger zijn dan dat van de vennootschapsbelasting.

Een vzw is ook onderworpen aan de jaarlijkse belasting op verenigingen zonder winstoogmerk, die verschuldigd is op het vermogen van de vereniging als de totale waarde van het vermogen meer dan 50.000 euro bedraagt (belastingtarieven 0,15%-0,45%).

6.2.2.3.2 Stichting
Er zijn twee soorten stichtingen: private stichtingen en stichtingen van openbaar nut. Een stichting van openbaar nut moet een van de volgende zeven specifieke doelen nastreven, namelijk de realisatie van een werk van filantropische, levensbeschouwelijke, religieuze, wetenschappelijke, artistieke, pedagogische of culturele aard.

[74] *Artikel 9:5 WVV.*
[75] *Artikel 9:6, §1, WVV.*
[76] *Artikel 9:10 WVV.*

Een belangrijke vraag is of het toegankelijk maken van data voor wetenschappelijk onderzoek door het faciliteren van gegevensstromen onder “een werk van wetenschappelijke aard” valt. Er wordt door de rechtspersoon immers niet zelf aan wetenschappelijk onderzoek gedaan, het wordt louter ondersteund door de HDS aangezien onderzoeksinstellingen en commerciële partners eenvoudiger toegang verkrijgen tot gegevens vereist voor onderzoek. In ieder geval wordt het faciliteren van wetenschappelijk onderzoek wellicht als een belangeloos doel gezien, al kan het niet worden beschouwd als het uitvoeren van wetenschappelijk onderzoek zelf, wat wel vereist is om te worden beschouwd als een stichting van openbaar nut. Daarom ligt de focus verderop uitsluitend op de private stichting. De stichting wordt besproken in Boek 11 van het WVV.

Oprichting

Een stichting wordt opgericht door de wil van één of meerdere personen, die een deel van hun vermogen in een juridische entiteit onderbrengen met als doel dit vermogen te bestemmen voor een specifiek doel.[77] Dit vermogen mag uitsluitend worden aangewend om het beoogde doel te realiseren. Een stichting kan eenzijdig worden opgericht of door middel van een overeenkomst tussen meerdere partners. In het eerste geval ontstaat de stichting door afzonderlijke eenzijdige rechtshandelingen, in het tweede geval door een overeenkomst tussen de oprichters die zich verbinden tot de oprichting van de stichting.

De oprichting van een stichting moet gepaard gaan met het ter beschikking stellen van een vermogen of op zijn minst het engagement daartoe, en dit ten einde het doel van de stichting te kunnen bereiken.
Het is essentieel dat de stichting over voldoende activa beschikt om haar in staat te stellen haar doel te bereiken, al vereist de wet geen minimumbedrag hiervoor. Het vermogen van de stichting wordt uitsluitend ingezet in het belang van de stichting zelf. Met andere woorden, het toegekende vermogen moet in verhouding staan tot het nagestreefde doel en voldoende zijn om dit belangeloze doel te kunnen bereiken.

Doel

Het doel van de stichting moet belangeloos zijn. Het faciliteren van gegevensstromen om onderzoek te ondersteunen kan wellicht als een dergelijk belangeloos doel worden aangemerkt.

Organisatie

Een stichting staat op zich en heeft geen leden of vennoten[78] die beslissingen nemen over haar toekomst. De wet of de statuten kunnen echter bepalen dat er leden zijn die in een speciaal orgaan beslissingen kunnen nemen. De aanwezigheid van leden en vennoten is niet noodzakelijk voor het bestaan van de stichting; hun vertrek heeft dan ook geen invloed op het voortbestaan, tenzij hierdoor de stichting niet meer kan functioneren of haar doel niet meer kan verwezenlijken. De rechten van deze leden worden bepaald door de raad van bestuur of een bevoegd orgaan bij de stichting, en kunnen in de statuten worden vastgelegd, maar dit is alleen verplicht als ze invloed hebben op de structuur van de stichting, zoals het inperken van de bevoegdheden van wettelijke of statutaire organen.[79] De private stichting geniet een grote flexibiliteit met betrekking tot de werkingsregels van het bestuursorgaan.

De oprichter bepaalt het doel en de werking van de stichting. De bestuurders (en de rechter, indien nodig) moeten dit respecteren. Dit betekent dat het bestuur geen bevoegdheid heeft om ingrijpende wijzigingen aan te brengen in het doel of de organisatie van de stichting.[80]

---

[77] D. Van Gerven, Verenigingen, vennootschappen en stichtingen, p. 649.

[78] Dit wordt, voor zover als nodig, uitdrukkelijk bevestigd in artikel 1:3 WVV.

[79] D. Van Gerven, Verenigingen, vennootschappen en stichtingen, 650.

[80] E.M. Meijers, (1948). Algemene begrippen van het burgerlijk recht. Leiden: Universitaire Pers, p. 262.

Belastingen
Een stichting is onderworpen aan de rechtspersonenbelasting[81], die wordt omschreven bij het belastingregime van de VZW, en niet aan de vennootschapsbelasting, dit op voorwaarde dat ze geen winstgevende activiteiten ontplooit. Het feit dat stichtingen onderworpen zijn aan de rechtspersonenbelasting betekent dat ze slechts belastbaar zijn over een beperkt deel van hun inkomsten.

Merk op dat een private stichting is onderworpen aan de jaarlijkse taks op de effectenrekeningen van 0,15% wanneer ze een effectenrekening aanhoudt met een gemiddelde van meer dan 1 miljoen euro.

Ontbinding
Het bestuur van de stichting kan niet besluiten om de stichting te ontbinden. De reden hiervoor is dat de oprichter zich onherroepelijk heeft ontdaan van de juridische eigendom van aan de stichting overgedragen activa. Ook het verstrijken van de statutaire termijn leidt niet automatisch tot ontbinding van de stichting.

Alleen de rechtbank kan een private stichting ontbinden (gerechtelijke ontbinding) op verzoek van de oprichter of een van zijn opvolgers, een bestuurder, een belanghebbende derde of het openbaar ministerie.

6.2.2.4 Nationale for-profit organisatievormen

Tegenover de *non-for-profit* organisatievormen die hierboven besproken worden, staan de *for-profit* vormen, die in het Belgische rechtsstelsel kunnen gesitueerd worden onder de vennootschappen.

Er zijn verschillende voor- en nadelen verbonden aan de vennootschapsvormen in België, waarvan de **Naamloze Vennootschap (NV)** en de **Besloten Vennootschap (BV)** waarschijnlijk de belangrijkste organisatievormen voor een Health Data Space zijn. Deze vennootschappen hebben dus gemeen dat ze allen winstgericht zijn.

De NV onderscheidt zich door de vereiste van een minimumkapitaal van 61.500 euro bij oprichting (artikel 7:50 WVV). Dit in tegenstelling tot de BV, die geen vast minimumkapitaal vereist, maar wel een toereikend aanvangsvermogen dat volstaat voor hun activiteiten moet hebben.

Doel
Een van de doelen van een vennootschap is steeds een rechtstreeks of onrechtstreeks vermogensvoordeel uit te keren of te bezorgen (artikel 1:1 WVV).

Kapitaal
De manier waarop een vennootschap kapitaal aantrekt is eenvoudiger dan bij een non-profitorganisatie. Kapitaal kan worden verkregen door het uitgeven van nieuwe aandelen of door de verkoop van aandelen van de oprichters. Hoewel dit een relatief eenvoudige methode is, brengt het wel met zich mee dat de vennootschap (nieuwe) aandeelhouders krijgt. Tegenover elk stuk (nieuw) kapitaal in de vennootschap staat dus een aandeelhouder.

Aandeelhouders hebben aanzienlijke invloed op de *corporate governance*, wat verwijst naar hoe een bedrijf wordt bestuurd en geleid. De jaarlijkse algemene vergadering (AVA) is hierbij een belangrijk moment waarop aandeelhouders hun stem kunnen laten horen en cruciale beslissingen kunnen nemen.
Het hebben van aandeelhouders kan ook leiden tot meer marktdruk, waarbij winstmaximalisatie vaak de belangrijkste drijfveer is. Dit kan in contrast staan met andere doelen, zoals het creëren van maatschappelijke meerwaarde door onderzoek. Dit spanningsveld moet zorgvuldig worden overwogen bij de beslissing om een BV of NV op te richten rond een HDS.

[81] *De boekhoudkundige en jaarrekeningrechtelijke voorschriften die stichtingen moeten naleven worden verder uitgewerkt in twee koninklijke besluiten, nl. het KB van 21 oktober 2018 tot uitvoering van de artikelen III.82 tot en met III.95 van het WER en het KB tot uitvoering van het Wetboek van Vennootschappen en Verenigingen van 29 april 2019.*

Interne organisatie
In een NV of BV is er steeds een Algemene Vergadering die is samengesteld uit aandeelhouders. Daarnaast is er een bestuursorgaan.[82]

Belastingen
Beide vennootschapsvormen zijn onderworpen aan de vennootschapsbelasting. In de vennootschapsbelasting word je belast op de verkregen winst, ook wel de 'belastbare basis' genoemd. Ofwel geldt het basistarief (25%), ofwel een verlaagd tarief in bepaalde gevallen (20%). Wat na de belastingen overblijft, kan worden uitgekeerd aan de aandeelhouders in de vorm van dividenden.

6.2.2.5 Bijkomstige overwegingen

Afgezien van de overwegingen en argumenten vanuit het vennootschaps- en verenigingsrecht, zijn er ook andere factoren die een doorslaggevende rol kunnen spelen bij de keuze van een organisatievorm. Enkele wetgevende instrumenten, zoals de DGA hebben immers een invloed op de wijze waarop aan databemiddeling kan worden gedaan, of hoe op termijn de Health Data Space dient deel uit te maken van de EHDS. Zo heeft de keuze tussen *for-profit* en *not-for-profit* een mogelijk aanzienlijke impact op het vertrouwen en neutraliteit die een organisatie kan uitstralen. Aangezien de Health Data Space een maatschappelijke functie zal vervullen, moet dit dus mee in overweging worden genomen wanneer een keuze wordt gemaakt van organisatievorm.

(i) Gaat winststreven hand in hand met het doel van een HDS?
De doelstelling die het huidige project voor ogen heeft, is gericht op een efficiëntere gegevensdeling voor secundaire doeleinden met als gevolg ook voordelige effecten voor de maatschappij in zijn geheel. Als één van de doelen van een Health Data Space is om het hergebruik van gegevens te bevorderen en mogelijk - op termijn - ook het primaire gebruik van data te faciliteren (bij uitbreiding van de huidige use cases naar een volwaardige Health Data Space in de zin van de EHDS-Verordening waarbij ook primair gebruik van persoonsgegevens wordt gefaciliteerd in de Health Data Space), kan er een maatschappelijke dimensie aan deze activiteiten worden gekoppeld. Bovendien wordt het organiseren van gezondheidszorg in het algemeen aanzien als een activiteit "in het algemeen belang".[83] Hieruit blijkt aldus een duidelijke maatschappelijke invalshoek. De discussie rond de organisatievorm van een Health Data Space werpt de vraag op of het combineren van winststreven met de maatschappelijke doelstellingen van een Health Data Space mogelijk is. Dit leidt tot de overweging of een niet-commerciële benadering, zoals een VZW, beter aansluit bij de fundamentele waarden van een Health Data Space, of dat een vennootschapsvorm, die wel winst nastreeft, ook geschikt kan zijn. De vraag is dan of een winstgerichte aanpak (*for-profit*) te rijmen valt met deze maatschappelijke doelstelling. De afwezigheid van een winstoogmerk kan voor een Health Data Space voordelig zijn, aangezien een belangeloze motivatie beter zou kunnen aansluiten bij de fundamentele doelstellingen en *raison d'être* van een Health Data Space. Er is geen druk om winst te realiseren, wat de focus houdt op de maatschappelijke of gemeenschappelijke waarde van de organisatie.

Het is belangrijk te benadrukken dat het creëren van winst zowel binnen vennootschappen (*for-profit*) als binnen verenigingen (*not-for-profit*) mogelijk is. Het belangrijkste verschil tussen deze organisatievormen ligt in de bestemming van de winst. Binnen een vereniging moet de winst worden geherinvesteerd om het belangeloze doel te realiseren, terwijl in een vennootschap de winst kan (en soms moet) worden uitgekeerd aan de aandeelhouders in de vorm van dividenden. Dit betekent dat winst nastreven ook binnen een vereniging mogelijk is, mits de winst wordt geherinvesteerd. Omgekeerd is het ook mogelijk om een belangeloos doel na te streven binnen een vennootschap.

[82] *Het bestuursorgaan bestaat uit minstens drie bestuurders in een NV. In een BV moet er één of meer bestuurders zijn.*

[83] *Zie bijvoorbeeld de definitie van "data-altruïsme" in artikel 2(16) DGA waarin gezondheidszorg én wetenschappelijk onderzoek worden vermeld als een doeleinde van algemeen belang.*

Een voorbeeld van een vennootschap met een belangeloos doel is Athumi, het Vlaamse Datanutsbedrijf. Athumi heeft de vorm van een NV aangenomen. In de statuten van Athumi staat dat de doelstelling van de vennootschap is om "in een datagedreven ecosysteem de samenwerking rond veilige gegevensdeling tussen burgers en overheidsinstanties te faciliteren, en om de uitoefening van rechten van burgers op het gebied van gegevensbescherming te optimaliseren met minimale administratieve lasten". Een dergelijk doel zou ook kunnen worden ondergebracht onder een vereniging, aangezien het ook als belangeloos doel zou kunnen worden geïnterpreteerd.

Ook kan de vraag gesteld worden of de data users de via de Health Data Space verkregen data kunnen aanwenden voor commerciële doeleinden, en of dit een weerslag heeft op het in essentie belangeloze doel van de Health Data Space *an sich*. Dit is vooreerst niet het geval; wat een afnemer van de dienst van een vereniging of stichting doet, heeft in beginsel geen invloed op de eigenlijke missie en het al dan niet belangeloze karakter van het vooropgestelde doel van de vereniging of stichting. De EHDS volgt deze redenering ook, aangezien hier geen onderscheid wordt gemaakt tussen niet-commerciële en commerciële "partners". Ook de DGA maakt hier weinig woorden aan vuil, wat doet vermoeden dat het uiteindelijke einddoel van de verkregen data geen invloed heeft op de aard van een databemiddelingsdienst.
Wel bepaalt de DGA duidelijk dat wanneer een entiteit zich wil kwalificeren als een organisatie voor data-altruïsme deze in beginsel niet-commercieel dient te zijn.

Daarnaast is het van belang dat het uiteindelijke gebruik van de gegevens door de data users geen invloed heeft op de doelstelling van de Health Data Space zelf. Ook als de data users commerciële doelen nastreven, kan de Health Data Space nog steeds een belangeloos doel hebben, zoals het faciliteren van gegevensstromen voor wetenschappelijk onderzoek.

(ii) Beïnvloedt de verdere financiering van de Health Data Space de keuze van organisatievorm?

Als de overheidsfinanciering wegvalt, moet de Health Data Space andere inkomstenbronnen hebben om duurzaam te kunnen functioneren. Mogelijke financieringsbronnen zijn sponsoring en ledenbijdragen, die beide verenigbaar zijn met de verschillende onderzochte organisatievormen. In dit verband moet worden opgemerkt dat een vennootschap aanvullende financieringsmogelijkheden heeft, zoals het uitgeven van nieuwe aandelen, wat geen optie is bij een vereniging.

Het huidige project neemt op het moment van het schrijven eerder de vorm aan van een aanbieder van databemiddelingsdiensten in de DGA, dan van een volwaardige Health Data Space zoals omschreven in de EHDS-Verordening. Op de lange termijn dient dus ook te worden gekeken naar de toekomst van de Health Data Space en hoe de use cases uitgebreid kunnen worden.

Bovendien is het momenteel onduidelijk wie de eindverantwoordelijkheid draagt voor de financiering van een Health Data Space. Uit de voorlopige versie van de EHDS-Verordening kan worden afgeleid dat deze verantwoordelijkheid bij de lidstaten ligt. Dit blijkt ook uit persberichten van de Europese Commissie.[84]
De vraag kan dus gesteld worden of lidstaten zich überhaupt mógen onttrekken van het verder financieren van een Health Data Space, indien de Health Data Space als gevolg van het toedraaien van de geldkraan niet langer in staat zouden zijn te opereren. Hiertegenover staat dan weer de nuance dat het huidige project eerder gekwalificeerd kan worden als een aanbieder van databemiddelingsdiensten overeenkomstig de DGA, dan een Health Data Space overeenkomstig de EHDS-Verordening, waardoor er *in casu* mogelijk geen verplichting voor de Belgische/Vlaamse overheid bestaat tot het blijvend financieren van een dergelijk project. De DGA, die de werking van aanbieders van geregistreerde databemiddelingsdiensten reguleert, gaat niet in op wie de kosten voor het creëren en onderhouden van een aanbieder van databemiddelings-diensten moet dragen. Er is alleszins geen verplichting naar de lidstaten opgenomen om een dergelijke aanbieder van databemiddelingsdiensten op te richten en/of te onderhouden. Subsidiëring vanuit de overheid uit is dan ook niet Europees verplicht.

[84] *Zie Europese Commissie. (24 april 2024). Questions and Answers on the European Health Data Space.*

Op basis van het bovenstaande moet worden geconcludeerd dat de verdere financiering niet wordt besproken in de wetgeving voor de aanbieders van databemiddelingsdiensten. Een HDS onder de EHDS-verordening moet wel worden ondersteund door de lidstaten, maar hoever deze verplichting gaat is onduidelijk.

(iii) Organisatie van de activiteiten

De DGA legt enkele belangrijke voorwaarden op voor databemiddelingsdiensten. Volgens artikel 12 (a) DGA mag de aanbieder van databemiddelingsdiensten de gegevens waarvoor hij deze diensten verleent niet voor andere doeleinden gebruiken dan het beschikbaar stellen aan gegevensgebruikers. Bovendien moet deze aanbieder opereren via een afzonderlijke rechtspersoon, wat betekent dat de Health Data Space in dezelfde rechtspersoon geen andere activiteiten[85] kan uitvoeren dan die in het kader van het aanbieden van databemiddelingsdiensten. Wel is het mogelijk voor de aanbieder van een databemiddelingsdienst om aanvullende specifieke instrumenten en diensten aan te bieden, zoals tijdelijke opslag, curatie, conversie, anonimisering en pseudonimisering, om de gegevensuitwisseling te faciliteren (artikel 12 (c) DGA). Indien de Health Data Space wil worden gekwalificeerd als een databemiddelingsdienst onder de DGA, moeten deze voorwaarden strikt worden nageleefd.

(iv) Transitie: van for-profit naar non-for-profit en omgekeerd

De keuze voor de rechtsvorm van een Health Data Space is een cruciale beslissing die zorgvuldig moet worden overwogen. Hoewel deze keuze later kan worden aangepast, is een dergelijke wijziging niet eenvoudig en kan deze slechts beperkt worden doorgevoerd. Vooral de omzetting van een *for-profit* rechtsvorm, zoals een BV, naar een *non-for-profit* vorm, zoals een stichting, is bijzonder complex vanwege de veranderingen in toepasselijke belastingregels. De omzetting van een (internationale) *non-profit* organisatie naar een bedrijf is over het algemeen niet toegestaan, behalve in het geval van omzetting naar een erkende coöperatieve sociale onderneming (CVSO) of een coöperatie die als sociale onderneming is erkend (i.e. een coöperatieve venootschap). Het omvormingsverslag zou wel eenvoudiger op te stellen zijn van een *for-profit* vorm naar een *non-profit*.

Een bijkomend aandachtspunt is het vermogen van de organisatie. Bij een *non-profit* organisatie is het vermogen bestemd voor een belangeloos doel, en dit kapitaal kan niet zomaar worden omgezet naar een doel met winststreven binnen een *for-profit* organisatie. Als bijvoorbeeld een vzw, met een belangeloos doel, wordt omgevormd tot een *for-profit* organisatie, moet het vermogen van de vzw worden overgedragen aan een andere non-profit organisatie, zodat het oorspronkelijk beoogde doel behouden blijft.

(v) Rechtsgrond voor secundaire verwerkingen

Ten slotte moet worden benadrukt dat er rekening moet worden gehouden met het doeleinde waarmee persoonsgegevens initieel werden verzameld, en of dit doeleinde verenigbaar is met een verdere verwerking. Hierbij dient vnl. gedacht te worden aan het verwerken van persoonsgegevens in het kader van data-altruïsme, waarbij er verwerkt wordt op de rechtsgrond toestemming (artikel 6.1.a) AVG). Indien deze toestemming enkel is gegeven ten aanzien van doelen die het algemene belang ten goede komen, mogen zij dan verder gebruikt worden om bovendien winst te maken voor de leden van een vennootschap? Niet ieder business model, met name de *for-profit* modellen, zijn daarom misschien even geschikt om bepaalde activiteiten te verrichten. Het bestemmen van de winst moet mogelijk ook in lijn liggen met de oorspronkelijke intentie van de betrokkenen bij het delen van hun gegevens. Dit betekent dat het belangrijk kan zijn om de organisatievorm zodanig in te richten dat eventuele winst wordt gebruikt voor een belangeloos doel.

[85] *Een voorbeeld van dergelijke activiteiten is het aggregeren, verrijken of transformeren van gegevens met het oog op het toevoegen van substantiële waarde en het gebruik van de resulterende gegevens in licentie geven aan data users, zonder dat er een commerciële relatie tussen data holders of providers en data users tot stand wordt gebracht.*

6.2.3 De Europese datastrategie

De Europese Commissie heeft een Europese strategie voor gegevens ontwikkeld[86] met als doel de gegevenseconomie in de EU te stimuleren en tegelijkertijd de fundamentele rechten en vrijheden van burgers, die de kern van de Europese samenleving vormen, te beschermen. Gegevens worden beschouwd als een essentiële hulpbron voor het bevorderen van maatschappelijke en economische groei en innovatie[87] en zijn cruciaal voor het creëren van een interne markt voor gegevens die het internationale concurrentievermogen en de soevereiniteit op het gebied van gegevens waarborgt. Het doel van de Europese strategie voor gegevens is het vergroten van de beschikbaarheid van persoonsgegevens en niet-persoonsgebonden gegevens voor het gebruik en hergebruik van gegevens[88] en het bevorderen van mechanismen voor gegevensbeheer. Op die manier wil deze strategie verschillende sectoren omvatten, waaronder gezondheidszorg, milieu, energie, transport en openbare diensten in de hele EU.

Om de gegevenseconomie binnen de EU te bevorderen, voorziet de Europese strategie voor gegevens in de omzetting van verschillende wetgevingsmaatregelen die bijdragen aan de uitvoering van mechanismen voor gegevensbeheer en die de toegang tot gegevens bevorderen. Hierbij zijn zowel particuliere als publieke belanghebbenden betrokken (bv. voor het delen van gegevens tussen bedrijven en de overheid). In de context van de Europese strategie voor gegevens vormen met name de Data Governanceverordening (DGA)[89] en de Data Verordening[90] de twee cruciale wetgevingsstukken. De Data Verordening, aan de ene kant, richt zich voornamelijk op de beschikbaarheid van industriële (niet-persoonlijke) gegevens.[91]
De Data Governanceverordening daarentegen is, zoals de naam al aangeeft, een sectoroverschrijdend bestuurskader dat het delen van gegevens ondersteunt door twee soorten *tussenpersonen* op te richten voor het commercieel en altruïstisch delen van gegevens. De wet heeft betrekking op zowel persoonlijke als niet-persoonlijke gegevens en vult, vooral met betrekking tot de eerstgenoemde soort gegevens, de vereisten van de Algemene Verordening Gegevensbescherming (AVG) aan die van toepassing zijn op persoonlijke gegevens. Hiernaast is de Europese strategie voor gegevens een horizontaal kader en voorziet het in het bevorderen van de ontwikkeling van gemeenschappelijke Europese ruimten (*common data spaces*) voor gegevens. In dit opzicht zal de DGA een aanvulling vormen op (aanstaande) wetgeving die meer op sectoren is toegesneden, zoals de European Health Data Space Verordening (EHDS-verordening), om de beschikbaarheid van gegevens in verschillende sectoren te vergroten.

De Europese Commissie zet sterk in op de creatie van dergelijke gegevensruimten (of *data spaces*). Ze geeft mee dat de volgende aspecten kenmerkend zijn voor de *Common European Data Spaces*:[92]

- Ze staan **open** voor **deelname** door alle organisaties en individuen;
- Ze beschikken over een **veilige en privacybeschermende** infrastructuur om gegevens te bundelen, er toegang toe te krijgen, ze te delen, te verwerken en te gebruiken;

---

[86] *Europese Commissie, z.d.-a; Europese Commissie, z.d.-b*

[87] *Overweging 157 AVG haalt zo bijvoorbeeld aan dat het koppelen van gegevens uit verschillende registers onderzoekers nieuwe en zeer waardevolle kennis over veel voorkomende medische aandoeningen zoals hart- en vaatziekten, kanker en depressie kan opleveren. Omdat zij op een groter deel van de bevolking zijn gebaseerd, kunnen onderzoeksresultaten met behulp van registers worden verbeterd. […] Daarom moet, teneinde wetenschappelijk onderzoek te faciliteren, worden bepaald dat persoonsgegevens, met inachtneming van de passende voorwaarden en waarborgen die in het Unierecht of het lidstatelijke recht zijn vastgesteld, met het oog op wetenschappelijk onderzoek mogen worden verwerkt.*

[88] *Er wordt ook fel ingezet op het hergebruik van gegevens, en niet enkel op Europees niveau. Zo heeft het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid Afdeling "Gezondheid" (thans de kamer voor Sociale Zekerheid en Gezondheid) in beraadslaging nr. 15/014 van 17 maart 2015 betreffende de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen in het kader van de oprichting van een register over cardiale incidenten en het gebruik van de gegevens voor wetenschappelijke doeleinden reeds aangehaald dat dubbele registratie vermeden dient te worden en dat hergebruik van reeds beschikbare gegevens beoogd moet worden (Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid, 2015).*

[89] *Verordening (EU) 2022/868 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 van 30 mei 2022 (hierna: DGA).*

[90] *Verordening (EU) 2023/2864 betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data en tot wijziging van Verordening (EU) 2017/3294 en Richtlijn (EU) 2020/1828 van 13 december 2023 (hierna: Dataverordening).*

[91] *Europese Commissie, z.d.-a.*

[92] *Europese Commissie, z.d.-c.*

> Ze hebben een duidelijke en praktische structuur voor de toegang tot en het gebruik van gegevens:
  - De gemeenschappelijke Europese dataruimten hebben **eerlijke, transparante, evenredige en niet-discriminerende toegangsregels**, dankzij goed gedefinieerde en betrouwbare mechanismen voor gegevensbeheer;
> De **regels en waarden van de EU** moeten worden **gerespecteerd**, met name op het gebied van **gegevensbescherming, consumentenbescherming en mededingingswetgeving**;
> Houders van gegevens moeten in staat zijn gesteld **toegang te verlenen** tot bepaalde **persoonlijke** of **niet-persoonlijke gegevens** of deze te **delen**;
> Houders van gegevens moeten in staat zijn gesteld hun gegevens **gratis** of **tegen vergoeding** beschikbaar te stellen voor hergebruik.

Tegen deze achtergrond moet in gedachten worden gehouden dat de verwerking van patiëntgegevens onderworpen is aan een complexe reeks regels die leiden tot de toepassing van wetten op verschillende gerechtelijke niveaus (bv. nationaal, EU, Europees, internationaal) en sectoren (bv. gezondheidszorg, onderzoek). De mogelijkheid om patiëntgegevens te gebruiken, in hun ruwe of anonieme vorm, kan dus verschillende juridische vragen oproepen, afhankelijk van de context waarin ze worden gebruikt.
Dit hoofdstuk is daarom selectief in die zin dat het een overkoepelend beeld geeft van de kaders en regels die in deze context relevant zijn. In de volgende paragrafen worden relevante bepalingen voor de verwerking van persoonsgegevens, gezondheidsgegevens en niet-persoonlijke gegevens in het kader van dit project uitgelicht. De nadruk van deze bespreking ligt op secundaire gegevensverwerking, met het oog op wetenschappelijke, historisch of statistisch onderzoek. De resultaten van dergelijk onderzoek kunnen uiteindelijk dienen om innovatie te stimuleren, beleidsinzichten te creëren en/of aan preventieve gezondheidszorg te doen en kan wetenschappelijk of eerder statistisch (retrospectief) van aard zijn.

Met dat in gedachten zijn de volgende paragrafen gewijd aan het onderzoek van meerdere wetgevende instrumenten, waaronder die welke deel uitmaken van de Europese datastrategie. Allereerst zal de AVG worden onderzocht, aangezien deze rechtstreeks van toepassing is in alle EU-lidstaten en daarom de belangrijkste verordening inzake gegevensbescherming vormt die de basisregels vaststelt voor de verwerkingen betreffende persoonsgegevens, onder meer voor wetenschappelijk, historisch of statistisch onderzoek (sectie 6.2.4 Algemene Verordening Gegevensbescherming (AVG). Vervolgens worden enkele instrumenten ontleed die als doel hebben om “open data” te stimuleren; de Dataverordening, waarna de DGA aan bod komt, die ingaat op de manieren waarop delingen kunnen plaatsvinden. Hierna worden enkele andere aspecten besproken (zie sectie 6.2.10.6 Afgeleide rechten), zoals hoe het intellectuele eigendomsrecht zich verhoudt tot het creëren van een data space en of de AI-verordening van toepassing kan zijn. Ten slotte, wordt er een overzicht gegeven van het vennootschapsrecht (zie sectie 6.4 Ethische principes) en welke aspecten mogelijks interessant zijn bij het opstellen van een Health Data Space.

6.2.4 Algemene Verordening Gegevensbescherming (AVG)

In het kader van een volwaardige Health Data Space worden er persoonsgegevens verwerkt. [93]
Daarom wordt in de volgende paragrafen onderzocht hoe de Vlaamse Health Data Space zou interageren met de Algemene Verordening Gegevensbescherming (AVG).

[93] *Artikel 2 AVG beperkt het materieel toepassingsgebied van de AVG tot die verwerkingen die kunnen worden gekwalificeerd als een geheel of gedeeltelijk geautomatiseerde verwerking of de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.*

Het bovenstaande betreft de datastromen die ontstaan binnen de Health Data Space tussen de data providers en data consumers. Dit doet geen afbreuk aan de verplichtingen die voortvloeien uit de AVG met betrekking tot interne verwerkingen en de normale bedrijfsvoering, zoals het beheer van arbeidsrelaties, contacten met andere bedrijven via natuurlijke personen, enzovoort. Al deze relaties blijven onderworpen aan de AVG, en het is belangrijk om zorgvuldig met deze gegevens om te gaan.

6.2.4.1 Relevante definities

De AVG introduceert belangrijke definities die de toepassing van de AVG vormgeven. In de eerste plaats worden specifieke rollen geïntroduceerd voor degenen die betrokken zijn bij verwerkingsactiviteiten, namelijk verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken en verwerkers, en worden hun verantwoordelijkheden uiteengezet. Bovendien bevat het kader voor gegevensbescherming meerdere concepten en beginselen die leiden tot de toepassing van verschillende regels in de AVG.

6.2.4.1.1 Persoonsgegevens en gezondheidsgegevens

Zodra een verwerkingsverantwoordelijke gevestigd is in de Unie en in het kader van haar activiteiten persoonsgegevens van Unieburgers verwerkt,[94] is de AVG van toepassing.[95] Hetzelfde geldt wanneer persoonsgegevens van betrokkenen die zich in de Unie bevinden worden verwerkt, ook als de verwerkingsverantwoordelijke zelf niet in de Unie gevestigd is.[96] Persoonsgegevens worden in de AVG gedefinieerd als alle informatie met betrekking tot een geïdentificeerde of identificeerbare persoon[97] (ook wel "de betrokkene" genoemd). Voorbeelden van persoonsgegevens zijn namen, adressen of locaties.

De persoonsgegevens in de Health Data Space zijn vaak **gezondheidsgegevens**. Deze gegevens zijn persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.[98] Artikel 9 van de AVG kwalificeert genetische, biometrische en gezondheidsgegevens als een bijzondere categorie van persoonsgegevens waarvoor in principe een verwerkingsverbod bestaat. Er bestaan uitzonderingen op dit verbod, dewelke worden opgesomd in paragraaf 2 van artikel 9. Hieronder wordt ingegaan op enkele mogelijke uitzonderingen van dit verbod.

6.2.4.1.2 (Gezamenlijke) Verwerkingsverantwoordelijke(n)/verwerker

De **verwerkingsverantwoordelijke** wordt in artikel 4, 7) van de AVG omschreven als “een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; […]”.

---

[94] *Zie artikel 3 AVG voor het territoriale toepassingsgebied.*

[95] *Artikel 2 AVG beperkt het materieel toepassingsgebied van de AVG tot die verwerkingen die kunnen worden gekwalificeerd als een geheel of gedeeltelijk geautomatiseerde verwerking of de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.*

[95] *Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4, 1) AVG).*

[96] *Artikel 3.2 AVG.*

[97] *Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4, 1) AVG).*

[98] *Artikel 4, 15) AVG.*

In de AVG wordt bovendien ook melding gemaakt van de term "**gezamenlijke verwerkingsverantwoordelijken**". De kwalificatie als gezamenlijke verwerkingsverantwoordelijke ontstaat wanneer meerdere partijen betrokken zijn bij de verwerking van persoonsgegevens en zij gezamenlijk het doel en de middelen van die verwerking bepalen.[99] Volgens de AVG zijn gezamenlijke verwerkingsverantwoordelijken verplicht om onderling afspraken vast te leggen in een overeenkomst.[100]

De **verwerker** wordt in artikel 4, 8) van de AVG omschreven als "*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.*"

Wanneer een verwerkingsverantwoordelijke persoonsgegevens overdraagt aan een derde partij, spreken we in principe over een overdracht tussen verwerkingsverantwoordelijken. Beide entiteiten zijn verwerkingsverantwoordelijke in de zin van de AVG.

Voor een diepgaandere discussie over de rolverdeling in de Health Data Space, zie 7.2.3 Bouwblok 2: Juridische en organisatorische vorm.

6.2.4.1.3 Geanonimiseerde/geaggregeerde/gepseudonimiseerde gegevens

Omdat anonieme gegevens redelijkerwijs niet meer kunnen worden gekoppeld aan een geïdentificeerde of identificeerbare persoon, vallen deze in principe buiten de reikwijdte van de AVG.[101] De AVG stelt dat bij het bepalen of een persoon identificeerbaar is, alle middelen in overweging moeten worden genomen die redelijkerwijs kunnen worden gebruikt door de verwerkingsverantwoordelijke of een andere partij om die persoon direct of indirect te identificeren (zie *infra*). Hierbij moet rekening worden gehouden met objectieve factoren zoals de kosten en de tijd die nodig zijn voor (her-)identificatie, met de technologie die op dat moment beschikbaar is en toekomstige technologische ontwikkelingen.[102] Kortom, indien de verwerkingsverantwoordelijke er redelijkerwijze niet in slaagt de betrokkenen te (her)identificeren rekening houdend met de objectieve factoren van de specifieke context, dan valt de verwerking niet onder het toepassingsgebied van de AVG. Een voorbeeld hiervan kan een verwerking van anonieme gegevens voor statistische of onderzoeksdoeleinden zijn.[103] Deze denkwijze bouwt voort op de Opinie van de GROEP GEGEVENSBESCHERMING ARTIKEL 29 die al in 2007 aangaf dat anonieme gegevens informatie betreffende een natuurlijke persoon die niet kan worden geïdentificeerd is. De identificatie kan noch door de verwerkingsverantwoordelijke, noch door een andere persoon gebeuren, *rekening houdende met alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verwerkingsverantwoordelijke dan wel door enig ander persoon in te zetten zijn.*[104]

Data aggregatie is een proces waarin informatie wordt verzameld en uitgedrukt in een beknopte vorm, voor doeleinden zoals statistisch analyseren. Een bekend aggregatiedoel is om meer informatie over bepaalde groepen, gebaseerd op specifieke variabelen, zoals leeftijd, beroep of inkomen, te verkrijgen.[105] Indien de aggregatie goed verloopt, zullen ook geaggregeerde data als geanonimiseerd kunnen worden beschouwd, aangezien iedere link naar een identificeerbare betrokkene wordt doorbroken.[106]

---

[99] *European Data Protection Board (2021), p. 21.*

[100] *Artikel 26 AVG.*

[101] *Overweging 26 AVG.*

[102] *Ibid.*

[103] *Ibid.*

[104] *Groep Gegevensbescherming Artikel 29 (20 juni 2007). Advies 4/2007 over het begrip persoonsgegevens.*

[105] *Zie Vloca Kennishub. (2024) Geaggregeerde data.*

[106] *De GBA geeft dit ook aan in haar advies 133/2018 dd. 28 november 2018.*

Een belangrijke distinctie die moet worden gemaakt wanneer er gesproken wordt over geaggregeerde gegevens, is dat dit geen duidelijk gedefinieerd begrip is in de context van de EU-gegevensbeschermings-wetgeving. Er kan worden vanuit gegaan dat de term geaggregeerde data verwijst naar niet-persoonsgebonden gegevens.[107] Dit valt onder meer af te leiden uit de verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie (FFDR) die stelt dat geaggregeerde datasets gebruikt voor *big data analytics* als niet-persoonsgebonden informatie kan worden beschouwd.[108] Toch kan er niet van worden uitgegaan dat geaggregeerde gegevens automatisch anoniem zijn. Anonimisering is een **proces** en daarom moet de aard van de gegevens van geval tot geval worden geëvalueerd om ervoor te zorgen dat de anonimiseringstechnologie robuust is.

Een onderscheid met ***gepseudonimiseerde gegevens*** moet worden gemaakt. Gepseudonimiseerde gegevens zijn gegevens die niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.[109] Er zal steeds moeten worden onderzocht of er daadwerkelijk gesproken wordt over geanonimiseerde gegevens, en niet feitelijk gepseudonimiseerde gegevens, aangezien gepseudonimiseerde gegevens wél beschouwd worden als persoonsgegevens onder de AVG.

De meningen over waar de praktische grens ligt voor wat anoniem is (en bijgevolg ook voor wat geaggregeerd is) en wat “slechts” gepseudonimiseerde gegevens zijn, lopen echter uiteen. Zo is de GROEP GEGEVENSBESCHERMING ARTIKEL 29 van mening dat gegevens nooit anoniem zijn zodra identificatie technisch mogelijk is (er bestaat bijvoorbeeld érgens een sleutel tot heridentificatie, ook al heeft de onderzoeker het sleutelbestand niet).[110] Dit is een voorbeeld van aanhangers van de ***absolute benadering*** ten aanzien van anonimisatie. Dit zou met zich meebrengen dat geaggregeerde data, waarvan meer gedetailleerde informatie beschikbaar is bij bepaalde instanties, niet kan worden aangemerkt als geanonimiseerde data, met als gevolg dat de AVG wel degelijk van toepassing is.[111] Op deze benadering is al veel kritiek gekomen wegens de onwerkbaarheid hiervan in de praktijk. Ze werd daarentegen bevestigd en herhaald door de EUROPEAN DATA PROTECTION BOARD (EDPB).[112]

Er is ook een minder strikte, ***relatieve benadering*** die rekening houdt met hoeveel moeite het identificeren zou zijn en wat de specifieke context is (bijvoorbeeld of identificatie verboden is).[113] Hierbij wordt dan gekeken naar het perspectief van de gegevensontvanger en of deze in staat is om over te gaan tot heridentificatie. Zo kan eenzelfde dataset voor de ene partij geanonimiseerd zijn, aangezien deze geen toegang heeft tot een encryptiesleutel bijvoorbeeld, maar is voor de entiteit die deze sleutel nog heeft, de dataset slechts gepseudonimiseerd. Deze relatieve benadering zou aansluiten bij jurisprudentie[114] volgens dewelke moet onderzocht worden of heridentificatie mogelijk is aan de hand van de *redelijkerwijs te verwachten middelen*.
De context van de gezondheidszorg is specifiek en maakt dat gegevens in gezondheidsonderzoek voldoende genuanceerd moeten zijn om tot geldige conclusies te kunnen komen. Enigszins paradoxaal genoeg moeten grotere gegevenssets worden onderzocht om voldoende statistische geldige correlaties te vinden voor kleinere subgroepen.[115] Het is daarom cruciaal om te benadrukken dat niet zomaar iedere

[107] *Centre for IT & IP (CiTiP), 2023.*

[108] *Overweging 9 Verordening (EU) 2018/1807 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie van 14 november 2018 (hierna: FFDR).*

[109] *Artikel 4(5) AVG.*

[110] *Groep Gegevensbescherming Artikel 29 (10 april 2014), Opinion 05/2014 on Anonymisation Techniques.*

[111] *Groos & van Veen, 2020.*

[112] *Zie para. 76, European Data Protection Board, 4 mei 2020; European Data Protection Board, 21 april 2020.*

[113] *Groos & van Veen, 2020, 498.*

[114] *Hof van Justitie van de Europese Unie (2016), Patrick Breyer/Bundesrepublik Deautschland.*

[115] *Hoeyer, 2019, p. 531.*

vorm van anonimisatie/aggregatie uit het toepassingsgebied van de AVG valt. In de technische uitvoering hiervan zal er dus steeds concreet moeten worden gekeken naar welke data nog worden overgemaakt en hoe groot **de kans tot heridentificatie** door de data user of data consumer werkelijk is. Dit impliceert dus ook een onderzoeksplicht voor de verzender van anonieme data (*in casu* de data provider). **De verzender dient na te gaan of de identificatie met de verzonden gegevens vanuit het perspectief van de ontvanger bij wet verboden is, of in de praktijk onmogelijk is, bijvoorbeeld omdat zij excessieve inspanning zou vergen**. Indien de gegevens immers niet als anoniem te beschouwen zijn, begaat de verzender ervan mogelijk inbreuken op de AVG wanneer deze niet adequaat geanonimiseerde gegevens, en dus *persoonsgegevens*, verzendt zonder alle verplichtingen van de AVG in acht te nemen. Indien er enkel geanonimiseerde gegevens worden overgemaakt aan de data consumer, of op z'n minst gegevens die voor de ontvangende partij niet heridentificeerbaar zijn, dan dient er bijvoorbeeld geen verwerkingsovereenkomst te worden opgemaakt[116] en is er geen noodzaak tot het hebben van een rechtsgrond.[117] Het zal dus essentieel zijn om een zeker "niveau van anonimisatie" te verwachten van de data providers indien zij zich ertoe verbinden om anonieme gegevens te delen in de Health Data Space. Dit zijn aspecten die tevens in de *Usage policy* kunnen worden opgenomen.

Een bijkomende nuance moet worden gemaakt ten aanzien van geanonimiseerde gezondheidsgegevens, waar altijd een groter risico op heridentificatie zal blijven bestaan. Dit risico is des te groter wanneer het gaat om gedetailleerde medische informatie over specifieke gezondheidsincidenten, aandoeningen of behandelingen op individueel niveau. Het INFORMATIEVEILIGHEIDSCOMITÉ (IVC) beschouwt dergelijke informatie doorgaans als dermate specifiek dat absolute zekerheid over de anonimiteit *a priori* niet kan worden gegarandeerd.[118] Hetzelfde wordt gesteld in de EHDS-verordening; namelijk dat bepaalde categorieën elektronische gezondheidsgegevens bijzonder gevoelig blijven, zelfs wanneer ze in anoniem formaat zijn.[119] Er blijft immers het risico bestaan dat middelen worden gebruikt die buiten de middelen liggen die *redelijkerwijs* kunnen worden gebruikt. Zij wijzen er echter op dat anonimisering of codering, mits uitgevoerd volgens de vereisten zoals vastgelegd in beraadslaging nr. 14/059 van 15 juli 2014, door een *trusted third party* een mogelijke oplossing kan bieden.[120]

Het uitvoeren van een ***small cell risk*-analyse** is in dit verband relevant. Een dergelijke analyse wordt uitgevoerd bij geanonimiseerde datasets om het risico te beoordelen dat een individu indirect kan worden geïdentificeerd door het combineren van unieke of zeldzame gegevenspunten (zogenaamde "small cells"). In de context van gezondheids- of persoonsgegevens verwijst een "small cell" naar een datapunt of combinatie van kenmerken die betrekking heeft op een zeer klein aantal personen, vaak minder dan drie. Dit zal niet enkel door de data provider moeten worden uitgevoerd wanneer deze datasets ter beschikking stelt, maar ook voor het opstellen van de catalogus van metadata door de Health Data Space zelf, zal dit een noodzakelijke oefening zijn.

Of en hoe gezondheidsgegevens kunnen worden geanonimiseerd opdat ze buiten het toepassingsgebied van de AVG vallen, is nog geen helemaal uitgeklaarde zaak, helaas. In het kader van het creëren van een Health Data Space zal opvolging inzake deze materie noodzakelijk zijn. De Health Data Space is op dit ogenblik zodanig opgebouwd dat de Health Data Space zelf geen persoonsgegevens verwerkt (buiten de catalogus van metadata). Desondanks blijft dit een belangrijk debat om verder op te volgen.

---

[116] Hof van Justitie van de Europese Unie (2023), Meta/Bunderkartellamt.

[117] Groos & van Veen, 2020, p. 499.

[118] Zie bijvoorbeeld Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid, afdeling "Gezondheid". (17 maart 2015). Beraadslaging nr. 15/014 betreffende de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen in het kader van de oprichting van een register over cardiale incidenten en het gebruik van de gegevens voor wetenschappelijke doeleinden.

[119] Overweging 64 EHDS.

[120] Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid Afdeling "Gezondheid". (15 juli 2014). Beraadslaging nr. 14/059 met betrekking tot de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen in het kader van het Thales project.

6.2.4.2 Verwerken van persoonsgegevens

6.2.4.2.1 Rechtsgronden

Onder de AVG zijn er **zes rechtsgronden** waarop de verwerking van persoonsgegevens kan worden gebaseerd. Artikel 6.1 AVG stelt dat de verwerking alleen rechtmatig is als één van de zes rechtsgronden, zoals beschreven onder a) tot en met f), van toepassing is. Dit betekent dat een verwerkingsverantwoordelijke, voordat deze met de verwerking begint, moet vaststellen welke rechtsgrond van toepassing is en ervoor moet zorgen dat aan de voorwaarden van die specifieke rechtsgrond wordt voldaan. Dit is de taak van de verwerkingsverantwoordelijke, in lijn met het verantwoordingsbeginsel, tenzij anders bepaald door wetgeving.[121] De verwerkingsverantwoordelijke moet kunnen aantonen dat de **persoonsgegevens worden verzameld voor specifieke, expliciete en gerechtvaardigde doeleinden, en dat de verwerking plaatsvindt op een rechtmatige, eerlijke en transparantie manier ten opzichte van de betrokkene**.[122] Het is hierbij van belang om te onthouden dat de AVG geen hiërarchie aanbrengt tussen de verschillende rechtsgronden.[123]

Als persoonsgegevens voor verschillende doeleinden worden verwerkt moet de verwerking voor elk afzonderlijk doel binnen een van de rechtsgronden van artikel 6.1 AVG vallen. De doeleinden en de rechtsgrondslag voor de verwerking moeten vanaf het begin worden vastgesteld en aan de betrokkenen worden gecommuniceerd (artikelen 13.1.*c)* en 14.1.*c)* AVG). Wanneer de verwerking is gebaseerd op artikel 6.1.*f)* AVG, mogen er niet meerdere doeleinden worden gecommuniceerd zonder voor elk doel afzonderlijk de rechtsgrond te beoordelen.[124]

6.2.4.2.2 Initiële en verdere verwerking

Onder de AVG kan zowel een initiële als verdere verwerking plaatsvinden. Hoewel deze termen niet expliciet in de verordening zijn gedefinieerd, differentieert de AVG in feite dus wel tussen de twee. Ook in de context van een Health Data Space is het belangrijk om onderscheid te maken tussen de initiële verzameling en verwerking van persoonsgegevens door *data providers* (i.e. initiële verwerking) en de daaropvolgende doorgifte van die gegevens via de Health Data Space-infrastructuur (i.e. verdere verwerking). In dit verband moet worden opgemerkt dat de EHDS-verordening dit concept verder vormgeeft, aangezien zij nieuwe definities voor deze concepten bevat, die verder zullen worden toegelicht in sectie 6.2.6.2 Toepassingsgebied en relevante definities.

Op grond van de AVG kan de verwerkingsverantwoordelijke (in dit geval de data provider) de persoonsgegevens in eerste instantie hebben verzameld en gebruikt voor zijn eigen doeleinden, die los kunnen staan van het uitvoeren van onderzoek. Daarbij moet de data provider een geldige rechtsgrondslag of rechtsgrond hebben onder artikel 6.1 AVG, aangezien het de plicht van de data provider is om als verwerkingsverantwoordelijke te voldoen aan de regels van de AVG (in lijn met de verantwoordingsplicht). Het is ook de taak van de data provider om te bepalen of de gegevens mogen worden geanonimiseerd en vervolgens mogelijk voor een ander doel mogen worden gebruikt, zoals voor secundair gebruik van gegevens in de Health Data Space. Als de data provider als verwerkingsverantwoordelijke van plan is om de gegevens (opnieuw) te gebruiken voor een ander doel dan waarvoor ze in eerste instantie zijn verzameld, dan wordt dit beschouwd als een verdere verwerking.

De verdere verwerking van gegevens verwijst naar het hergebruik van gegevens voor andere doeleinden, zoals onderzoek, innovatie, beleidsvorming, patiëntveiligheid, enz.[125] Het hergebruik van persoonsgegevens moet voldoen aan één van de volgende voorwaarden: het moet ofwel gebaseerd zijn op een eigen

[121] *Artikel 5.2 AVG.*

[122] *HvJ (2023) Meta/Bundeskartellamt, para. 109.*

[123] *European Data Protection Board (EDPB), (26 november 2024). Richtsnoeren 1/2024 on processing of personal data based on Article 6(1)(f) GDPR; zie ook L., Cools, (26 November 2024). Is consent taking priority over legitimate interest under the GDPR?*

[124] *European Data Protection Board (EDPB), (26 november 2024). Richtsnoeren 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, p. 6.*

[125] *C. Baartmans & W. Steenbruggen, Een Europese Unie voor zorgdata: so close yet so far, Computerrecht (NL), 2023(3), 215.*

rechtsgrondslag, waardoor de verwerking een volledig zelfstandige activiteit wordt en daarmee als een initiële of primaire verwerking wordt beschouwd, ofwel verenigbaar zijn met de oorspronkelijke primaire verwerking, in welk geval het hergebruik wordt gekwalificeerd als een verdere of "secundaire" verwerking.[126] Om te beoordelen of de verdere verwerking legitiem is, moet bij de beoordeling rekening worden gehouden met de oorspronkelijke doeleinden waarvoor de persoonsgegevens in eerste instantie zijn verzameld en verwerkt, en of het oorspronkelijke doel overeenstemt met het doel dat wordt overwogen voor de verdere verwerkingsactiviteiten die moeten worden uitgevoerd.[127] In dit verband moet worden opgemerkt dat, als persoonsgegevens worden verwerkt voor een ander doel dan waarvoor ze oorspronkelijk zijn verzameld, de verwerkingsverantwoordelijke moet nagaan of het nieuwe doel verenigbaar is met het oorspronkelijke doel volgens artikel 6.4 AVG.[128] Overweging 50 gaat hier verder op in door te stellen dat er in het geval van een verdere verwerking geen afzonderlijke rechtsgrond dan die op grond waarvan de verzameling van de persoonsgegevens werd toegestaan vereist is en geeft enkele aspecten mee waarmee rekening moet worden gehouden om te bepalen of een verdere verwerking "verenigbaar" is. In artikel 5.1.*b)* AVG is bepaald dat de **verdere verwerking met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden** overeenkomstig artikel 89.1 AVG **niet als onverenigbaar met de oorspronkelijke doeleinden wordt beschouwd**.[129] Ook het faciliteren van het gebruik van (gezondheids)gegevens kan worden gekwalificeerd als het gebruik van data voor secundaire doeleinden volgens de BELGIAN HEALTH DATA AGENCY[130]. Ook de GROEP GEGEVENSBESCHERMING ARTIKEL 29 (WP29) is van mening dat een brede interpretatie moet worden gegeven aan het concept "verdere verwerking".[131] Het is essentieel dat de betrokkenen voldoende worden geïnformeerd en dat de persoonsgegevens, in het bijzonder indien men voor secundair gebruik van gegevens in een (health) data space niet uitsluitend met geanonimiseerde gegevens zou werken, de vastgestelde doeleinden van de oorspronkelijke verwerking respecteren.

Ten slotte moet de data provider ook steeds rekening houden met de bepalingen die zijn opgenomen in het gezondheidsrecht. De meeste wetgeving gaat niet concreet in op de verdere verwerking van patiëntgegevens voor onderzoeksdoeleinden, maar vaak wordt wel anonimisatie aangemoedigd.[132] Dit kan trouwens als een lacune worden opgevat. De toepasselijke gezondheidswetgeving is niet bepaald uitgesproken over hoe precies onderzoek moet worden uitgevoerd op reeds bestaande gezondheidsgegevens.

6.2.4.2.3 Anonimiseren van persoonsgegevens als verdere verwerking onder de AVG

In de context van de Health Data Space zal er, in het bijzonder voor wat het secundair gebruik betreft, veel gewerkt worden met geanonimiseerde gegevens. Het anonimiseren van persoonsgegevens is een proces dat de verwerking van persoonsgegevens met zich meebrengt en dus moet de activiteit van het anonimiseren van persoonsgegevens zelf in overeenstemming zijn met de AVG.

---

[126] Er wordt dan rekening gehouden met:

- *a) ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;*
- *b) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;*
- *c) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10;*
- *d) de mogelijke gevolgen van de voorgenomen verdere verwerking van de betrokkenen;*
- *e) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.*

[127] Zie artikel 6.4 AVG dat enkele aspecten opsomt waarmee rekening gehouden dient te worden bij de beoordeling of een secundaire verwerking verenigbaar is met de primaire verwerking.

[128] European Data Protection Board (EDPB), (26 november 2024). Richtsnoeren 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, p. 11.

[129] Zie ook Overweging 50 AVG.

[130] Zie Health Data Agency, z.d.

[131] Article 29 Data Protection Working Party, 2 april 2013.

[132] Gegevensbeschermingsautoriteit (GBA). (2019). Nota over de verwerking van gegevens uit patiëntendossiers, DOS-2019-04611.

De beslissing of gegevens mogen worden geanonimiseerd ten behoeve van onderzoek kan daarom in sommige gevallen worden aangemerkt als een verdere verwerking van persoonsgegevens.

De beslissingsbevoegdheid om over te gaan tot anonimisering ligt bij de verwerkingsverantwoordelijke, die hiervoor over een rechtsgrond moet beschikken aangezien het proces van anonimiseren een verwerkingsactiviteit van persoonsgegevens is. In de Health Data Space zal dit waarschijnlijk worden besloten door de data provider in zijn hoedanigheid van verwerkingsverantwoordelijke. Het is dus aan de data provider om te verifiëren of de initiële verwerkingsgrond in overeenstemming is met het anonimiseren van gegevens en het delen ervan voor onderzoeksdoeleinden. De Health Data Space zelf is in principe niet betrokken bij dit besluitvormingsproces en fungeert eerder als verbinder om een relatie tussen de *data provider* en de ontvanger van de gegevens tot stand te brengen. Desalniettemin zullen bepaalde aspecten in deze context worden besproken in de volgende sectie, voor zover ze relevant worden geacht. Bovendien moet het gebruik van de gegevens door de ontvanger/data consumer zodanig worden uitgevoerd dat de gegevens anoniem blijven. Alleen als de gegevens echt anoniem zijn zoals vereist onder de AVG, heeft de ontvanger/data consumer van de gegevens geen eigen rechtsgrond nodig om die gegevens opnieuw te gebruiken. Toch moeten ze eventuele beperkingen die zijn opgelegd door de data provider, indien deze bepaald en van toepassing zijn, op het gebruik van de gegevens respecteren. Ten slotte moet verduidelijkt worden dat het eigenlijke uitvoeren van wetenschappelijk onderzoek op geanonimiseerde gegevens in principe buiten het toepassingsgebied van de AVG vallen.

De verwerking van gezondheidsgerelateerde patiëntgegevens als onderdeel van een datavalorisatieproject of het uitvoeren van statistisch onderzoek, zoals wat onder meer de bedoeling is in een health data space, maakt dus een verdere verwerking van de data uit en is rechtmatig wanneer:

- **De verdere verwerking verenigbaar is met de initiële verwerking;**
- **Het gaat om wetenschappelijk, historisch of statistisch onderzoek (artikel 6.4 AVG + overweging 50); of**
- **Dit in het gerechtvaardigd belang van de verwerkingsverantwoordelijke (bv. een ziekenhuis) is (artikel 6.1.f) AVG) (zie infra).**

Bovendien moet bij de verwerking van gezondheidsgegevens rekening worden gehouden met artikel 9.2 AVG, waar artikel 9.2.j) AVG van tel is.

In werkelijkheid zal het anonimiseren van gegevens een blijvend knelpunt vormen, waarbij het noodzakelijk is om het actuele debat nauwgezet te blijven volgen. Dit heeft te maken met de steeds complexere scheidingslijn tussen anonimisering en pseudonimisering, die door technologische vooruitgang steeds dunner lijkt te worden. Wat vandaag als anoniem wordt beschouwd, kan door toekomstige technieken en datasets mogelijk opnieuw worden herleid tot een individu, waardoor de grens tussen veilige gegevensverwerking en privacyrisico's vervaagt.

Daarnaast speelt de voortdurende vooruitgang van technologieën zoals machine learning, big data-analyse en artificiële intelligentie een cruciale rol. Deze technologieën kunnen patronen herkennen in grote hoeveelheden gegevens, waardoor het mogelijk wordt om uiteindelijk informatie te herleiden die oorspronkelijk als anoniem werd beschouwd. Dit benadrukt de noodzaak van robuuste richtlijnen en regelmatige evaluatie van de methodologieën die worden gebruikt voor gegevensanonimisering.
Het lastige is hierbij dat juristen, zoals hoger reeds aangehaald, in twee kampen zijn verdeeld en de rechtspraak van het Hof van Justitie momenteel nog niet uitdrukkelijk genoeg is geweest, al lijkt er meer aanhang te bestaan voor het kamp van de relatieve benadering.

Bovendien zijn er juridische en ethische implicaties verbonden aan de keuze tussen anonimiseren en pseudonimiseren. Anonimiseren verwijdert de koppeling met identificeerbare individuen volledig, maar pseudonimiseren laat de mogelijkheid tot heridentificatie open, mits er aanvullende informatie beschikbaar is.

Deze nuance is niet alleen van invloed op de naleving van regelgeving zoals de AVG, maar ook op het vertrouwen van burgers in hoe hun gegevens worden behandeld binnen initiatieven zoals de European Health Data Space (EHDS). Ten slotte valt op te merken dat de EHDS-verordening bovendien een verplichting heeft opgenomen in artikel 61(3). Deze bepaling schrijft voor dat de gebruiker van gezondheidsgegevens de natuurlijke personen waarop de elektronische gezondheidsgegevens die zij hebben verkregen op basis van de gegevensvergunning, het gegevensverzoek of het besluit tot goedkeuring van toegang door een bevoegde deelnemer aan Health Data EU, betrekking hebben, niet opnieuw mag identificeren of trachten te identificeren. Indien de EHDS-verordening dus van toepassing blijkt op data providers in de Health Data Space, dan rust er een wettelijke bepaling op hen om niet te heridentificeren. Dit is in het bijzonder van belang aangezien het Hof van Justitie in een arrest uitdrukkelijk aangeeft dat indien de identificatie van de betrokkene bij de wet verboden zou zijn, het gevaar voor identificatie in werkelijkheid "onbeduidend" zou zijn,[133] en dit blijkt dan weer relevant voor de juridische beoordeling of er sprake is van een geanonimiseerde dataset. Ditzelfde arrest onderschrijft bovendien de relatieve benadering, waarbij er dus naar een specifieke actor moet worden gekeken en diens redelijk beschikbare middelen om al dan niet over te gaan tot heridentificatie.

Dit is positief voor de ontwikkeling van een Health Data Space, waarbij het kunnen werken met geanonimiseerde datasets de verhoudingen tussen actoren aanzienlijk vereenvoudigt. Het debat lijkt dus in de gunstige richting te evolueren wanneer secundaire verwerkingsactiviteiten worden beoogd. Desondanks zou het bevorderend zijn dat beleidsmakers, technologische experts en juridische professionals samenwerken om duidelijke definities, richtlijnen en technologische standaarden te ontwikkelen. Duidelijkere (nationale) richtlijnen omtrent anonimisering blijken immers toch een gemis te zijn. Dit moet gepaard gaan met een voortdurende monitoring van de stand van de techniek en aanpassingen aan de regelgeving waar nodig door de Health Data Space. Alleen zo kan de balans worden gevonden tussen innovatie en het waarborgen van de privacy van individuen.

6.2.4.3 Rechtsgronden voor het verwerken van persoonsgegevens en bijzondere categorieën van persoonsgegevens

In het algemeen kunnen persoonsgegevens worden geanonimiseerd voor onderzoeksdoeleinden. Hiervoor kunnen verschillende rechtsgronden van artikel 6 AVG van toepassing zijn. Met het oog op de doelstellingen van de Health Data Space, kunnen met name de volgende rechtsgronden relevant worden om het anonimiseren van persoonsgegevens toe te staan; i) indien hiervoor toestemming is gegeven (artikel 6.1.a) AVG), indien de verwerkingsverantwoordelijke een wettelijke verplichting heeft om dit te doen (artikel 6.1.c) AVG), of indien het binnen het gerechtvaardigde belang valt (artikel 6.1.f) AVG), of het hiermee verenigbaar is (artikel 6.4 AVG). Deze gronden worden hieronder slechts beknopt besproken, aangezien het uiteindelijk aan de *data provider* zal zijn om dit toe te passen, en niet aan de Health Data Space zelf.

1. **Toestemming**. Indien de initiële verwerking plaatsvindt op basis van de toestemming (artikel 6.1.a) juncto artikelen 7 en 8 AVG), betekent dit dat de gegeven toestemming ook betrekking moet hebben op het anonimiseren van persoonsgegevens voor onderzoeksdoeleinden. Immers, ook al zijn de gegevens die in het kader van de Health Data Space worden gebruikt in principe geanonimiseerde gegevens, de anonimisering met het oog op het gebruik van de gegevens voor onderzoeksdoeleinden is ook een aspect dat moet zijn opgenomen in de oorspronkelijke toestemming die is gegeven.
   De betrokkene moet hierover bij het geven van de toestemming afdoende zijn geïnformeerd.
   a. Rekening houdend met overweging 33 AVG is het vaak niet mogelijk om op het ogenblik waarop de persoonsgegevens worden verzameld het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven. Daarom moet de betrokkenen worden toegestaan hun toestemming voor bepaalde terreinen van wetenschappelijk onderzoek te verlenen, en het

[133] *Hof van Justitie van de Europese Unie. (26 april 2023). Gemeenschappelijke Afwikkelingsraad (GAR) t. Europese Toezichthouder voor Gegevensbescherming (EDPS) (T-557/20, ECLI:EU:T:2023:219), para. 93.*

voor andere eventueel te weigeren.[134] Het doel mag ook niet ongelimiteerd breed omschreven zijn, maar een bepaalde afbakening kan volstaan (zoals voor trauma-onderzoek). Er zal bovendien steeds rekening moeten worden gehouden met de proportionaliteit van een nieuw onderzoek. Hierbij moet een kanttekening worden gemaakt, aangezien een "geïnformeerde toestemming" zoals vereist is in het gezondheidsrecht[135] (bv. voor medische ingrepen) wezenlijk verschilt van de toestemming onder de AVG. Een geïnformeerde toestemming richt zich op het informeren van een patiënt over de aard, risico's en voordelen van een medische procedure, met als doel een weloverwogen keuze mogelijk te maken.[136] Toestemming onder de AVG daarentegen moet voldoen aan specifieke criteria: deze moet *vrij, specifiek, geïnformeerd en ondubbelzinnig* zijn.[137]
De interpretatie en toepassing van deze concepten lopen uiteen, wat kan leiden tot juridische en operationele complexiteit in een Health Data Space.
In de relatie arts-patiënt of onderzoeker-deelnemer (in het kader van klinische proeven) kan sprake zijn van een machtsonevenwicht, wat de vrijwilligheid van de toestemming overeenkomstig de AVG onder druk zet. Dit wordt bijvoorbeeld erkend in de Opinie van de EDPB van 23 januari 2019.[138] Patiënten of deelnemers aan klinische studies voelen zich mogelijk verplicht om toestemming te geven voor gegevensverwerking, omdat zij bijvoorbeeld al hebben ingestemd met deelname aan een onderzoek. Dit roept vragen op over de geldigheid van de "vrije" toestemming en benadrukt de noodzaak om alternatieve rechtmatigheidsgronden te overwegen.

b. Een interessante discussie betreft het concept van *brede toestemming*. Vooral in het domein van genoomonderzoek is het gebruikelijk dat deelnemers brede toestemming geven, zodat hun gegevens kunnen worden gebruikt voor meerdere mogelijke onderzoeksprojecten.[139] Dit roept echter de vraag op of een dergelijke brede toestemming ook voldoet aan de vereisten van de AVG en daarmee als rechtsgrond kan dienen. Of een 'brede toestemming', waarbij gegevens voor álle mogelijke onderzoeken kunnen worden gebruikt, juridisch houdbaar is, blijft een grijs gebied. Dit raakt immers aan het concept van *data-altruïsme* (zie sectie 6.2.4.1 Relevante definities), dat verdere overweging vereist.

2. **Wettelijke verplichting**. Volgens artikel 6.1.c) AVG mogen verwerkingsverantwoordelijken gegevens verwerken als de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting waaraan de de verwerkingsverantwoordelijke is onderworpen. Volgens de huidige versie van het voorstel voor de EHDS-verordening kunnen *data holders*[140] of gegevensverstrekkers verplicht worden bepaalde elektronische gezondheidsgegevens (en bijbehorende metagegevens) beschikbaar te stellen voor secundair gebruik door *data users*.[141] Dit betekent dat deze verordening voorziet in een wettelijke verplichting om in bepaalde gevallen persoonsgegevens te verwerken,[142] waardoor in een rechtsgrond overeenkomstig artikel 6.1.c) van de AVG wordt voorzien. In combinatie met de bepaling die voorziet welke categorieën elektronische gezondheidsgegevens beschikbaar moeten worden gesteld,[143] lijkt de rechtsgrondslag op basis waarvan gegevens moeten worden gedeeld zeer breed. In feite moet elke organisatie die actief is in de gezondheidszorg en/of biowetenschappen en beschikt over elektronische gezondheidsgegevens er rekening mee houden dat zij gezondheidsgegevens beschikbaar moeten stellen voor secundair gebruik. In sommige gevallen vereist deze verplichting ook dat de gegevensverstrekker aanvullende gezondheidsgegevens verzamelt. In zo'n geval is er geen sprake van het louter hergebruiken van

[134] *Overweging 33 AVG.*

[135] *Bijvoorbeeld artikel 6 e.v. Experimentenwet; artikel 28, §1, Verordening Klinische Proeven of artikel 36 Kwaliteitswet.*

[136] *Ibid.*

[137] *Artikel 7 AVG.*

[138] *European Data Protection Board (EDPB), (23 januari 2019). Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art. 70.1.b)).*

[139] *D. Hallinan, (2020). Broad consent under the GDPR: an optimistic perspective on a bright future. Life Sciences, Society and Policy, 16.*

[140] *Data holders in de EHDS-verordening worden gedefinieerd als iedere natuurlijke of rechtspersoon, publieke autoriteit of agentschap, of enig ander orgaan in de gezondheids- en zorgsector (artikel 2, lid 2, y) EHDS).*

[141] *Artikel 32 j° 33 EHDS.*

[142] *C. Baartmans & W. Steenbruggen. (2023) Een Europese Unie voor zorgdata: so close yet so far, Computerr., p. 216.*

[143] *Artikel 33 EHDS.*

gezondheidsgegevens die al voor een bepaald doel zijn verzameld voor een ander, secundair doel, maar worden de nieuwe gegevens specifiek voor dat nieuwe doel verzameld. Toch beschouwt de EHDS-verordening de gegevensverzameling als een vorm van secundair gebruik. Hier is iets voor te zeggen zolang het verzamelen van de extra gegevens gericht is op effectief hergebruik van de al bestaande dataset, en er geen compleet nieuwe dataset ontstaat voor een ander doel dan het verlenen van zorg.[144]

a. **Gerechtvaardigd belang**. Volgens artikel 6.1.f) AVG moet de verwerking noodzakelijk zijn voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer deze belangen moeten wijken voor de belangen of de fundamentele rechten en vrijheden van de betrokkene die de bescherming van persoonsgegevens vereisen, in het bijzonder wanneer de betrokkene een kind is.[145] Het voeren van wetenschappelijk, historisch of statistisch onderzoek zelf kwalificeert als een gerechtvaardigd belang.[146] Hoewel het huidige doel van de Health Data Space wel ligt in het creëren van maatschappelijke en/of commerciële meerwaarde door onderzoek te doen op basis van geanonimiseerde persoonsgegevens, ligt het uiteindelijke doeleinde niet vast en kan dit veranderen naarmate het project vordert. Zo kan de gecreëerde kennis worden aangewend om preventieve gezondheidszorg toe te passen (zoals wordt beoogd in de Data4PHM use case), maar kan even goed epidemiologisch onderzoek plaatsvinden, of gepersonaliseerde gezondheidszorg worden gefaciliteerd. Terugvallen op het gerechtvaardigd belang als rechtsgrond kan vanwege deze onzekerheid daarom soms noodzakelijk zijn.
   Om zich te kunnen beroepen op het gerechtvaardigd belang moet een verwerkingsverantwoordelijke kunnen aantonen dat i) het een legitiem belang is, ii) de verwerking noodzakelijk is om het belang te verwezenlijken en iii) de belangen en fundamentele rechten/vrijheden van de betrokkenen niet zwaarder doorwegen dan het belang van de verwerkingsverantwoordelijke.[147] Hoewel er aanvullende voorwaarden zijn waaraan moet worden voldaan voordat een verwerkingsverantwoordelijke zich op deze rechtsgrondslag kan beroepen, wordt hier in deze studie niet verder op ingegaan, gezien de uitgebreide juridische literatuur die al over dit onderwerp bestaat.

   NB Overheidsinstanties kunnen niet terugvallen op het gerechtvaardigd belang als rechtsgrondslag in het kader van de uitoefening van hun taken.[148] Voor de oprichting van een Health Data Space heeft dit in beginsel geen gevolgen, aangezien de Health Data Space op dit moment geen persoonsgegevens verwerkt. Wanneer deze situatie wijzigt, bijvoorbeeld wanneer er in de toekomst ook primaire verwerkingen plaatsvinden in het kader van de Health Data Space, dan kan de overheid in principe terugvallen op artikel 6.1.e) van de AVG, zijnde een verwerking voor de vervulling van een taak van algemeen belang. Daarnaast zal er waarschijnlijk een wettelijke implementatie volgen van de EHDS-verordening, waarbij er ook een concrete wettelijke basis overeenkomstig artikel 6.1.c) van de AVG wordt verschaft om de verwerkingen in het kader van de Health Data Space te faciliteren, dit om de rechtszekerheid te garanderen. Hiervoor is een samenwerking tussen de verschillende overheden vereist, aangezien de bevoegdheden in de gezondheidszorg niet allemaal bij één overheid rusten (zie sectie 6.2.1.3 Bevoegdheidsverdeling ten aanzien van het organiseren van gezondheidszorg). Voor wat betreft het creëren van een volwaardige Health Data Space zal, gezien de verdeling in bevoegdheden, een samenwerking tussen het Vlaamse niveau en het federale echelon vereist zijn.

---

[144] C. Baartmans & W. Steenbruggen. (2023) Een Europese Unie voor zorgdata: so close yet so far, Computerr., p. 216.

[145] D., De Bot, (2020). De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit, p. 438 e.v.

[146] European Data Protection Board (EDPB), richtsnoeren 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, p. 11; Zie ook de conclusie van de advocaat-generaal G. F. Mancini (25 oktober 1984). Conclusie zaak 234/83, Gesamthochschule Duisburg v. Hauptzollamt München. Deze bespreekt de interpretatie van "wetenschappelijke activiteiten" in het kader van wetgeving rond douanetarieven; "werkzaamheden van een openbare of particuliere onderwijs- of onderzoeksinstelling, gericht op het verwerken, verdiepen, weergeven en verbreiden van wetenschappelijke kennis, wanneer de werkzaamheden worden verricht met instrumenten die geschikt zijn voor het leveren van prestaties van hoog niveau".

[147] European Data Protection Board (EDPB), richtsnoeren 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, p. 8.

[148] Artikel 6.1, lid 2, AVG.

Wat betreft het secundair gebruik van gegevens, lijkt dit een bevoegdheid voor de Vlaamse Gemeenschap, aangezien deze bevoegd is voor bijvoorbeeld preventieve gezondheidszorg.[149]

Naast persoonsgegevens kunnen ook **bijzondere categorieën van persoonsgegevens**, zoals gegevens over gezondheid of genetische gegevens, worden verwerkt in het kader van de Health Data Space.
Om dit te doen, moet de verwerkingsverantwoordelijke voldoen aan de vereisten in artikel 9 AVG in aanvulling op de vereisten van artikel 6 AVG. Artikel 9.1 AVG verbiedt in het algemeen de verwerking van bijzondere categorieën van persoonsgegevens. De verwerking van deze soorten gegevens is bij uitzondering toegestaan als een van de vereisten van artikel 9.2 AVG van toepassing is. Bovendien geeft de AVG aan dat er afwijkingen op het verwerkingsverbod mogelijk moeten zijn met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.[150]

a. **Uitdrukkelijke toestemming**. Aangezien het in dit geval om gezondheidsgegevens gaat, moet er ook een uitzonderingsgrond onder artikel 9.2 van de AVG zijn om de eerste verwerking rechtmatig te laten zijn. In de praktijk kan dit betekenen dat er met uitdrukkelijke toestemming van de betrokkenen zoals in artikel 9.2.a) AVG wordt gewerkt. Hoe deze er concreet moet uitzien wordt niet gespecifieerd in de AVG, wel wordt algemeen aanvaard dat een schriftelijke verklaring als "uitdrukkelijk" kan worden beschouwd.[151]

   De Verordening Klinische Proeven voorziet in een mogelijkheid om de toestemming van de proefpersoon te verzoeken om zijn of haar gegevens buiten het protocol van de klinische proef uitsluitend voor wetenschappelijke doeleinden te gebruiken in het kader van klinische proeven.[152] In deze verordening lijkt de wetgever aan te geven dat, ondanks de mogelijkheid om wetenschappelijk onderzoek op andere rechtsgronden te baseren, een toestemming toch ethisch verantwoord is.

b. **Archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden**. Artikel 9.2.j) AVG voorziet een uitzonderingsgrond voor onderzoek overeenkomstig artikel 89.1 AVG, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene. Het begrip "onderzoek" wordt in dit geval breed geïnterpreteerd (bv. technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek).[153]

   De verwerking moet *noodzakelijk* zijn, gebaseerd zijn op Unierecht of lidstatelijk recht. De wetgeving zelf moet proportioneel zijn aan het doeleinde en de essentie van het recht op gegevensbescherming respecteren. Bovendien moeten er gepaste en specifieke maatregelen worden genomen om de fundamentele rechten en belangen van individuen te beschermen.[154]

   De verwijzing naar artikel 89.1 AVG houdt in dat de verwerking onderworpen moet zijn aan passende waarborgen voor de rechten en vrijheden van de betrokkene. De waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. De bepaling geeft mee dat wanneer

[149] *Artikel 5, §1, I, eerste lid, BWHI.*

[150] *Overweging 52 AVG.*

[151] *European Data Protection Board (EDPB), richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, 4 mei 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf, 29.*

[152] *Artikel 28, §2, Verordening Klinische Proeven.*

[153] *Overwegingen 33 en 159 AVG.*

[154] *D. De Bot. (2020) De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit, 39.*

deze doeleinden eveneens kunnen worden verwezenlijkt aan de hand van manieren die de identificatie van betrokkenen niet of niet langer toelaat, dit moet gebeuren. In artikel 197 van de Wet Verwerking Persoonsgegevens (hierna: WVP) staat een watervalregeling opgenomen die voorschrijft dat indien dit mogelijk is wetenschappelijk onderzoek dient plaats te vinden aan de hand van anonieme gegevens. [155] Indien dit niet mogelijk blijkt te zijn, dan kan pseudonimisatie worden toegepast. Pas als ook dit niet mogelijk/wenselijk blijkt, kan er worden teruggevallen op niet-gepseudonimiseerde gegevens. Titel 4 van de WVP gaat dieper in op regels die van toepassing zijn rond deze passende waarborgen uit artikel 89.1 AVG.[156] Aangezien *in casu* het anonimiseren van persoonsgegevens de verwerking zelf is, lijkt hier *ab initio* aan te zijn voldaan.

NB Lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven en invoeren.[157] In artikel 9 van de WVP is de nationale wetgever hierop ingegaan door de verwerking van genetische, biometrische of gezondheidsgegevens bovendien te onderwerpen aan de volgende maatregelen:
de verwerkingsverantwoordelijke of, in voorkomend geval, de verwerker

- Wijst de categorieën aan van personen die toegang hebben tot de persoonsgegevens, waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig wordt omschreven;
- Houdt de lijst van de aldus aangewezen categorieën van personen ter beschikking van de bevoegde toezichthoudende autoriteit; en
- Zorgt ervoor dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardig contractuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen.

Dit zijn ook maatregelen die moeten worden getroffen bij het verwerken van gezondheidsgegevens in het kader van de Health Data Space. Hierbij moet ook onderzocht worden hoe de finale versie van de tekst van de EHDS-verordening als rechtsgrond conform artikel 6.1.c) van de AVG kan dienen.

6.2.4.4 Informatieverplichting

De AVG vereist dat de patiënt/proefpersoon geïnformeerd wordt over de verwerkingen die plaatsvinden op diens gegevens. Deze informatieverplichting is nog anders dan deze opgenomen in de Wet Patiëntenrechten[158], waar ze meer invloed heeft op het informeren over de behandeling zelf, eerder dan het gebruik van de gegevens van de patiënt. Het is essentieel dat de betrokkenen voldoende worden geïnformeerd over de verwerkingen dus en dat de persoonsgegevens, in het bijzonder indien een (health) data space niet uitsluitend met geanonimiseerde gegevens zou werken, de vastgestelde doeleinden van de oorspronkelijke verwerking respecteren. De informatieverplichting zit gevat in de artikelen 13 en 14 van de AVG.
Er zijn echter uitzonderingen op deze informatieplicht, vooral wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene zijn verzameld. Dit kan het geval zijn als:

- De betrokkene al over de relevante informatie beschikt;[159] of
- De persoonsgegevens niet rechtstreeks bij de betrokkene zijn verzameld en de betrokkene beschikt reeds over de informatie of het is onmogelijk om de informatie te verstrekken of dit blijkt een onevenredige inspanning te vereisen.[160]

---

[155] Zie ook het KB ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 13 februari 2001.

[156] Artikelen 190 e.v. Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens van 30 juli 2018 (hierna: WVP).

[157] Artikel 9.4 AVG.

[158] Artikel 5 Wet Patiëntenrechten.

[159] Artikel 13(4) AVG.

[160] Artikel 14(5) AVG.

Artikel 13 en 14 van de AVG verplichten de verwerkingsverantwoordelijke om de betrokkene te informeren wanneer hij voornemens is persoonsgegevens verder te verwerken voor een ander doel dan waarvoor deze oorspronkelijk zijn verzameld of verkregen. In een dergelijk geval moet de verwerkingsverantwoordelijke vóór de verdere verwerking informatie verstrekken over het nieuwe doel en alle relevante aanvullende informatie zoals beschreven in lid 2.

Deze verplichting is een uitwerking van het beginsel in artikel 5.1.*c)* van de AVG, dat bepaalt dat persoonsgegevens alleen mogen worden verzameld voor specifieke, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Verdere verwerkingen die onverenigbaar zijn met deze doeleinden zijn verboden. Het tweede deel van artikel 5.1.*c)* maakt echter een uitzondering voor verdere verwerking voor archiveringsdoeleinden in het algemeen belang, wetenschappelijk of historisch onderzoek, of statistische doeleinden, mits deze verwerking plaatsvindt overeenkomstig artikel 89, lid 1.[161] Als de verdere verwerking verenigbaar is met de oorspronkelijke doeleinden (zoals beschreven in artikel 6.4 AVG), zijn de bepalingen van artikel 13.3 en 14.4 van toepassing. Indien er informatie moet worden gegeven, moet dit plaatsvinden vóór de verdere verwerking van start gaat. Dit is uiteraard van belang voor de Health Data Space waarbij de Health Data Space-participanten vooreerst moeten nagaan of het redelijkerwijs te verwachten is door de betrokkenen dat hun persoonsgegevens worden verwerkt in de Health Data Space (al dan niet in geanonimiseerde format). Indien dit niet het geval is, dan zijn de nodige informatieverplichtingen op hen van toepassing.

6.2.4.5 Uitzonderingen op de uitoefening van rechten van betrokkenen

De AVG voorziet in de mogelijkheid tot het uitoefenen van rechten door betrokkenen in Hoofdstuk III. Betrokkenen hebben recht op rectificatie (artikel 16 AVG), gegevenswissing (artikel 17 AVG), beperking van de verwerking (artikel 18 AVG) en overdraagbaarheid van de gegevens (artikel 20 AVG). In sommige gevallen kunnen zij bezwaar tegen de verwerking uitoefenen (artikel 21 AVG). Echter, bij het bepalen van de rechten van betrokkenen moet rekening worden gehouden met de mogelijkheid tot uitzonderingen volgens artikel 89, lid 2 en 3 van de AVG.[162] Artikel 89.2 van de AVG maakt het mogelijk om bij het verwerken van persoonsgegevens voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden af te wijken van bepaalde rechten, zoals het recht op inzage, correctie, beperking van verwerking, en bezwaar (artikelen 15, 16, 18, en 21 van de AVG).

Deze afwijkingen zijn niet alleen gedeeltelijk, maar ook gebonden aan voorwaarden. Ze mogen alleen worden toegepast als het naleven van deze rechten het onderzoek onmogelijk zou maken of ernstig zou belemmeren, en als de afwijking noodzakelijk is om de onderzoeksdoeleinden te bereiken. Er moeten wel voldoende waarborgen zijn om de rechten en vrijheden van de betrokkenen te beschermen, zoals het nemen van technische en organisatorische maatregelen om te voldoen aan het principe van minimale gegevensverwerking.[163]

In de Belgische wetgeving (Titel IV van de WVP) worden deze afwijkingen verder uitgewerkt. Ze mogen alleen worden toegepast als het onderzoek anders ernstig zou worden belemmerd of onmogelijk zou worden.[164] Er worden bovendien enkele formele stappen vereist vooraleer er sprake kan zijn van dergelijke afwijkingen, zoals het aanstellen van een *Data Protection Officer*[165] en het aanpassen van het verwerkingsregister[166].

---

[161] *Groep Gegevensbescherming Artikel 29 (WP 29). (22 augustus 2018) Guidelines on Transparency under Regulation 2016/679.*

[162] *D. De Bot. (2020) De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit, 19.*

[163] *Ibid, 29.*

[164] *Artikel 186 WVP.*

[165] *Artikel 190 WVP.*

[166] *Artikel 192 WVP.*

Bij het secundair gebruik van gegevens in de Health Data Space worden meestal geanonimiseerde gegevens verwerkt. Hierdoor kunnen de betrokkenen hun rechten in principe niet uitoefenen, aangezien anonieme gegevens buiten de reikwijdte van de AVG vallen.[167] Anonimisering zorgt ervoor dat de gegevens niet langer herleidbaar zijn tot een specifieke persoon, waardoor de bescherming van individuele rechten zoals toegang, rectificatie en verwijdering niet van toepassing is. Dit neemt echter niet weg dat, indien de anonimiteit in de toekomst door technologische vooruitgang in gevaar zou komen, de situatie heroverwogen moet worden.

6.2.4.6 Privacy by design and default

In de Health Data Space wordt gekozen voor een **gedecentraliseerde** aanpak, waarbij gegevens niet centraal worden opgeslagen, maar dicht bij de bron blijven. Deze werkwijze sluit aan bij het **principe van *privacy by design and default*** (gegevensbescherming door ontwerp en standaardinstellingen).[168]
Dit principe vereist dat privacy en gegevensbescherming vanaf het begin worden geïntegreerd in de architectuur en processen van systemen en dat alleen de strikt noodzakelijke gegevens worden verwerkt.

De Gegevensbeschermingsautoriteit heeft in adviezen reeds haar steun uitgesproken voor dergelijke benaderingen, omdat het verzamelen van gegevens in een centrale database vaak moeilijk te verzoenen is met de grondbeginselen van de AVG, zoals noodzakelijkheid en gegevensminimalisering.[169] Het principe van noodzakelijkheid houdt in dat alleen gegevens worden verwerkt die absoluut nodig zijn voor het beoogde doel. Gegevensminimalisering stelt dat niet meer gegevens mogen worden verzameld dan strikt vereist is.[170]

Een centrale verzameling van gezondheidsgegevens kan bovendien leiden tot grotere risico's, zoals verlies van controle over gegevens, een verhoogde kans op datalekken, en misbruik van gegevens. Door de gegevens decentraal te houden, wordt niet alleen de privacy beter beschermd, maar blijven de gegevens ook meer onder controle van de partijen die ze oorspronkelijk beheren, zoals zorgverleners of onderzoeksinstellingen.

6.2.4.7 GEB/DPIA

Bij het opzetten van de Health Data Space, waarbij het de bedoeling is om data providers en users met elkaar te verbinden, kan best een **gegevensbeschermingseffectenbeoordeling of data protection impact assessment (DPIA)** worden uitgevoerd, zoals bepaald in artikel 35 van de AVG. Een DPIA dient voornamelijk om de beoogde verwerking, de beoordeelde risico's en hoe deze zullen worden beperkt door de toezichthoudende autoriteit te documenteren, indien deze hierom verzoekt. Deze beoordeling moet plaatsvinden voordat de verwerking begint. Als er een functionaris voor gegevensbescherming wordt aangesteld, moet deze om advies worden gevraagd.

Artikel 35 AVG vereist dat een verwerkingsverantwoordelijke een DPIA uitvoert wanneer nieuwe technologieën worden gebruikt of wanneer de **verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, gezien de aard, de reikwijdte, de context en de doeleinden ervan**. Vooral wanneer het de bedoeling is om grote hoeveelheden gezondheidsgegevens te verwerken, wordt het aangeraden om een DPIA op te stellen.[171] Zelfs als de verwerking betrekking heeft op het gebruik van anonieme gegevens en de gegevens bovendien niet verwerkt worden door de Health Data Space zelf, is het

[167] *Artikel 11.2 AVG.*

[168] *Artikel 25 AVG.*

[169] *Zie Gegevensbeschermingsautoriteit (GBA). (25 mei 2020). Advies nr. 42/2020 betreffende een wetsvoorstel tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19 dat het volgende stelt: "Deze centralisatie van een grote hoeveelheid gezondheidsgegevens in één enkele gegevensbank die is opgezet, eigendom is van en wordt beheerd door een actor die slechts als tussenpersoon optreedt is niet in overeenstemming met de beginselen van noodzakelijkheid en minimalisering".*

[170] *Artikel 5.1.c) AVG; zie ook European Data Protection Supervisor (EDPS), Necessity & Proportionality.*

[171] *Groep Gegevensbescherming Artikel 29 (WP 29). (13 oktober 2017) Guidelines on Data Protection Impact Assessment (DPIA).*

aangeraden om toch een DPIA uit te voeren. Hiermee kan worden onderzocht hoe de verwerkingen binnen de Health Data Space mogelijk gevolgen hebben voor de betrokkenen, zoals door de metadata die beschikbaar worden gesteld in een catalogus voor data consumers. Het is daarbij belangrijk om de algemene risico's van de gekozen werkwijze in kaart te brengen, zoals de mogelijke zwaktes op het gebied van beveiliging of kwetsbaarheden bij het gebruik van connectoren. Bovendien straalt het hebben van een DPIA vertrouwen uit naar eventuele partners voor de oprichting van de Health Data Space, wat alleen maar een voordeel kan zijn.

Verder kan worden nagedacht over de vraag of Health Data Space participanten verplicht zijn een DPIA uit te voeren en te delen met de Health Data Space. Het kan *aanbevolen* zijn dat participanten in hun hoedanigheid van data users of consumers binnen de Health Data Space een DPIA uitvoeren. De voorloper van de huidige Gegevensbeschermingsautoriteit heeft een lijst gepubliceerd waar deze enkele verwerkings-activiteiten identificeert die een DPIA vereisen[172] en in gevallen waar het gaat om persoonsgegevens en gezondheidsgegevens, zal hoogstwaarschijnlijk een DPIA verplicht zijn, vooral als er al een groot risico bestaat voor de rechten en vrijheden van betrokkenen die voortvloeien uit de verwerking van de gegevens van de betrokkenen.[173]

6.2.4.8 Functionaris voor Gegevensbescherming

Het wordt aangeraden om binnen de werking van de Health Data Space een functionaris voor gegevensbescherming (DPO) aan te wijzen, in het bijzonder wanneer er op grote schaal relaties ontstaan tussen *data providers* en *data users* in de vooropgestelde Health Data Space. De huidige use cases behandelen hoofdzakelijk geanonimiseerde gegevens, maar indien op termijn ook persoons- en gezondheidsgegevens worden verwerkt, wat wordt vooropgesteld in de EHDS-verordening, dan dient een dergelijke DPO te worden aangesteld om toezicht te houden op de blijvende verwerkingen.[174]
De DPO wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen (artikel 37.5 AVG). Dit kan een personeelslid zijn (artikel 37.6 AVG).

6.2.4.9 IVC – Beraadslaging

Ten slotte, in een context van gegevensbeschermingsrecht moet het Informatieveiligheidscomité (IVC) vermeld worden. Het IVC is bevoegd om beraadslagingen te houden waarbij de overdracht van persoonsgegevens door een instelling van sociale zekerheid of een federale overheidsinstelling aan "derden" wordt gemachtigd. Het IVC bestaat uit twee kamers: de Kamer Sociale Zekerheid en Gezondheid en de Kamer Federale Overheid.

In het kader van een Vlaamse HDS is het essentieel om deze formele vereiste in acht te nemen en een beraadslaging bij het IVC aan te vragen voordat bepaalde gegevens kunnen worden overgedragen. Hieronder wordt daarom geanalyseerd welke actoren de beraadslaging (al dan niet) moeten aanvragen en hoe dit eventueel (contractueel) kan worden afgedwongen.

Bij het bepalen of een beraadslaging vereist is voordat een bepaalde gegevensoverdracht kan plaatsvinden, moet rekening worden gehouden met het onderscheid tussen anonieme, gepseudonimiseerde en niet-gepseudonimiseerde persoonsgegevens. In het geval van de overdracht van geanonimiseerde persoonsgegevens door een instelling van sociale zekerheid, kan mogelijk worden teruggevallen op de

172 Commissie voor de bescherming van de persoonlijke levenssfeer. (16 januari 2019). Aanname van de lijst met verwerkingen waarvoor een Gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd conform artikel 35.4 van de Algemene Verordening Gegevensbescherming.

173 European Data Protection Supervisor (EDPS). Necessity & Proportionality.

174 Dit is gebaseerd op artikel 37.1.c) AVG.

algemene beraadslaging nr. 18/140 van 6 november 2018, die het gebruik van anonieme gegevens voor onderzoek toestaat zonder dat voor elke overdracht een nieuwe beraadslaging van het IVC nodig is.

Er bestaan ook uitzonderingen op deze machtigingsbevoegdheid, namelijk:

> Indien de mededeling gebeurt tussen beroepsbeoefenaars in de gezondheidszorg die door het beroepsgeheim gebonden zijn en persoonlijk betrokken zijn bij de uitvoering van diagnostische, preventieve of zorgverlenende handelingen ten opzichte van een patiënt;
> Indien de mededeling is toegestaan door of krachtens een wet, een decreet of een ordonnantie, na advies door de Gegevensbeschermingsautoriteit;
> In de gevallen door de Koning bepaald;
> Indien gegevens worden meegedeeld tussen instanties van eenzelfde Gemeenschap of Gewest die geen gebruik maken van de basisdiensten van het eHealth-platform.[175]

Kruispuntbank van de Sociale Zekerheid (KSZ) vs. afzonderlijke instelling van Sociale Zekerheid

Wanneer één enkele instelling van sociale zekerheid de vereiste informatie kan verschaffen, kan het verzoek rechtstreeks bij die instelling worden ingediend. Indien de opgevraagde gegevens door die instelling kunnen worden geleverd, zal deze het verzoek afhandelen, na beraadslaging van de kamer sociale zekerheid en gezondheid, als het om gepseudonimiseerde of niet-gepseudonimiseerde sociale persoonsgegevens gaat. Indien de instelling van sociale zekerheid geanonimiseerde gegevens dient te verstrekken, kan zij zelf voor de anonimisatie zorgen, zonder dat een beraadslaging van het IVC nodig is . De verstrekker van de gegevens moet echter altijd waarborgen dat de gegevens volledig anoniem zijn en de betrokkenen niet kunnen worden herkend.
Aanvragen om gegevens die geleverd moeten worden door meerdere instellingen van sociale zekerheid worden evenwel steeds door de Kruispuntbank voor de Sociale Zekerheid (KSZ) behandeld. In dat geval regelt de KSZ eerst de praktische aspecten, waarna het IVC zich kan uitspreken. De KSZ zal ook instaan voor de pseudonimisatie of anonimisatie van de gegevens, indien dat nodig is. De KSZ verstrekt momenteel alleen anonieme gegevens of gepseudonimiseerde persoonsgegevens uit het door haar beheerde datawarehouse arbeidsmarkt en sociale bescherming. De KSZ beschikt, afgezien van enkele uitzonderingen, niet over eigen persoonsgegevens. Andere instellingen van sociale zekerheid blijven authentieke bronnen van informatie en moeten afzonderlijk worden benaderd voor hun gegevens.

Voor de mededeling van anonieme gegevens is geen beraadslaging vereist, zoals vastgelegd in beraadslaging nr. 18/140 van 6 november 2018. Deze beraadslaging geldt alleen voor de KSZ wanneer zij persoonsgegevens verzamelt, koppelt en anonimiseert (en dus niet wanneer een aanvraag wordt gericht aan één enkele instelling van sociale zekerheid), voor onderzoeken die bijdragen aan de “sociale bescherming”. De beraadslaging heeft enkel betrekking op de mededeling van anonieme gegevens door de KSZ, dat wil zeggen wanneer de KSZ persoonsgegevens uit diverse authentieke bronnen verzamelt, koppelt en anonimiseert. Voor zover er bij één enkele instelling van sociale zekerheid wordt gevraagd om anonieme gegevens, dan kan zij de anonimisatie zelf uitvoeren. Een beraadslaging van het IVC is dan ook vereist.
Let wel: de meedelende organisatie moet er steeds grondig op toezien dat ze wel degelijk enkel anonieme gegevens meedeelt (m.a.w. de betrokkenen mogen op geen enkele wijze kunnen worden geheridentificeerd).

Bij elk verzoek moeten twee vragen worden beantwoord:

> Welke instelling(en) verstrek(t)(ken) de gevraagde gegevens?
> Wat is het risico op (her)identificatie?

[175] *Artikel 42, 3°, Wet houdende diverse bepalingen betreffende gezondheid van 13 december 2006.*

Het maakt voor het IVC niet uit wie de beraadslaging aanvraagt, zolang deze maar plaatsvindt. Vaak is dit de onderzoeker (in casu de data user), die het beste inzicht heeft in het doel van het onderzoek en bijgevolg het best geplaatst is een verzoek in te dienen.
Wat betreft de rol van de instellingen van sociale zekerheid: er is nog geen overleg gevoerd over hun mogelijke instap.

Tot slot, kan worden opgemerkt dat het onduidelijk is wat de gevolgen zijn van het niet aanvragen van een machtiging bij het IVC. In de wetgeving is alleszins geen sanctiemogelijkheid of een controlebevoegdheid opgenomen. Het verkrijgen van een machtiging is dus niet per se gecontroleerd, maar dit laat de toepassing van de AVG onverlet, alsook de controlebevoegdheid van de GBA. Een machtiging van het IVC sluit dus geenszins uit dat een eventuele (toekomstige) controle door de GBA plaatsvindt.

6.2.4.10 Slotoverwegingen

1. Wegens het gebruik van hoofdzakelijk geanonimiseerde/geaggregeerde data in de context van secundair gebruik in de Health Data Space, vallen de datastromen die plaatsvinden in de Health Data Space niet onder het toepassingsgebied van de AVG. Hierbij moet rekening worden gehouden met de toekomstige ontwikkelingen in de jurisprudentie rond het begrip “anonieme gegevens”. Dit past immers mogelijk de juridische kwalificatie aan.
2. De Health Data Space zelf is verwerkingsverantwoordelijke ten aanzien van de catalogus metadata die deze bijhoudt over de beschikbare datasets bij aangesloten data providers. Indien deze in de toekomst andere diensten zal aanbieden (bv. het encrypteren of pseudonimiseren van persoonsgegevens), dan zal zij moeten herevalueren hoe zij ten aanzien van die verwerkingsactiviteit wordt gekwalificeerd onder de AVG.
3. De Health Data Space dient in het contractuele kader in te bouwen dat de initiële verwerking van persoonsgegevens rechtmatig verloopt en gestoeld is op een **rechtsgrond uit artikel 6 en 9.2 van AVG**.
4. De *data provider* in een HDS moet zich ertoe verbinden om telkenmale zij persoonsgegevens verwerken voor een onderzoek, zij een **gegevensbeschermingseffectbeoordeling (DPIA)** opstellen. Dit is hun verantwoordelijkheid.

5. De Health Data Space dient bij de eigenlijke opstart een DPIA op te stellen, ook al betreft het *in casu* geanonimiseerde gegevens. Iedere keer dat er aanzienlijke wijzigingen plaatsvinden met het oog op de verwerking van persoonsgegevens, moet hieraan een update worden gegeven.
6. De Health Data Space zal in haar werking een functionaris gegevensbescherming moeten aanstellen (**DPO**).

6.2.5 Datagovernanceverordening

6.2.5.1 Inleiding

De Datagovernanceverordening[176] (DGA) is van toepassing sinds september 2023 en draagt zo bij aan een belangrijke pijler van de Europese datastrategie[177]. Zowel persoonsgegevens als niet-persoonsgebonden gegevens vallen onder de toepassing van de DGA. De wetgeving dient ook specifiek om de oprichting en ontwikkeling van gemeenschappelijke Europese dataruimten op strategische gebieden te ondersteunen[178], wat de relevantie van het wetgevende instrument voor het huidige onderzoek aantoont. In het bijzonder zijn de regels aangaande het stimuleren van gegevensdeling door de regulering van aanbieders van gegevensbemiddelingsdiensten en het aanmoedigen van het delen van gegevens voor altruïstische doeleinden van belang.

De verordening beoogt voornamelijk het beschikbaar stellen van data en het faciliteren van gegevensdeling in verschillende sectoren. Door een degelijk gegevensbeheer zal er immers meer mogelijk zijn op vlak van innovatie. Specifiek heeft het delen van gezondheidsgegevens voor ogen om meer gepersonaliseerde behandelingen te bieden, een algemeen verbeterde gezondheidszorg te verlenen en het helpen bestrijden of opsporen van zeldzame aandoeningen en ziektes.[179] Voor dit doel stelt de DGA twee soorten gegevensintermediairs vast die optreden als neutrale derde partijen om het delen van gegevens in de Europese gegevenseconomie te vergemakkelijken, namelijk organisaties voor data-altruïsme nastreven en aanbieders van databemiddelingsdiensten, die verder zullen worden uitgewerkt in de volgende secties.

6.2.5.2 Relevante definities

6.2.5.2.1 (Organisaties voor) data altruïsme

Data-altruïsme betreft personen en bedrijven die toestemming geven om gegevens over hen – vrijwillig en zonder beloning – beschikbaar te stellen voor doeleinden van algemeen belang. Een eventuele vergoeding kan wel worden gevraagd indien deze niet verder gaat dan een vergoeding van de kosten die zij maken om hun gegevens beschikbaar stellen. Doeleinden van algemeen belang worden voorkomend in het nationale recht bepaald, zoals gezondheidszorg, de strijd tegen klimaatverandering, verbetering van mobiliteit, facilitering van de ontwikkeling, productie en verspreiding van officiële statistieken, verbetering van openbare diensten, openbare besluitvorming of (wetenschappelijk, historisch of statistisch) onderzoek in het algemeen belang.[180] Steun voor wetenschappelijk/statistisch/historisch onderzoek – zoals het creëren van een Health Data Space ter facilitering van gegevensdeling – wordt eveneens beschouwd als een doel van algemeen belang.[181]

De DGA heeft tot doel betrouwbare instrumenten te creëren waarmee gegevens gemakkelijk kunnen worden gedeeld ten behoeve van de samenleving. Rechtspersonen die gegevens beschikbaar willen stellen voor het algemeen belang via data-altruïsme, kunnen zich laten registreren als een “in de Unie erkende organisatie voor data-altruïsme”. Dit label stelt hen in staat zich te profileren als een betrouwbare

[176] *Verordening (EU) nr. 2022/868 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 van 20 mei 2022 (hierna: DGA).*

[177] *Zie Europese Commisse, z.d.-a.*

[178] *Europese Commissie. (23 februari 2022). Commission Staff Working Document on Common European Data Spaces.*

[179] *Ibid.*

[180] *Artikel 2(16) DGA.*

[181] *Overweging 45 DGA.*

organisatie voor data-altruïsme, wat het vertrouwen van zowel gegevensgebruikers en -aanbieders als datasubjecten versterkt. Dit vertrouwen wordt onder meer gewaarborgd door de vereiste van een vestiging in de EU of het hebben van een wettelijke vertegenwoordiger.[182] Daarnaast moeten zij **zonder winstoogmerk** opereren, transparantievereisten naleven, en beschikken over specifieke waarborgen om de rechten en belangen van datasubjecten en ondernemingen te beschermen.[183] Het is de ambitie van de Unie om in de toekomst dankzij erkende organisaties voor data-altruïsme gegevenspools van voldoende omvang beschikbaar te stellen opdat gegevensanalyse en machinaal leren mogelijk is, en dit in heel de Unie.[184]

Entiteiten die als erkende organisaties voor data-altruïsme zijn geregistreerd, *mogen* het label "in de Unie erkende organisatie voor data-altruïsme" gebruiken en *moeten* het door de Commissie vastgestelde gemeenschappelijke logo duidelijk weergeven op elke online en offline publicatie die betrekking heeft op hun activiteiten op het gebied van data-altruïsme.[185]

Artikel 18 DGA vereist dat een organisatie voor data-altruïsme ook aan de volgende kenmerken voldoet:

- Ze voert activiteiten uit op het gebied van data-altruïsme;
- Ze is een rechtspersoon opgericht volgens het nationale recht om doelen van **algemeen belang** te realiseren;
- Ze opereert **zonder winstoogmerk en is juridisch onafhankelijk van entiteiten met winstoogmerk**;
- Haar activiteiten op het gebied van data-altruïsme zijn functioneel gescheiden van eventuele andere commerciële activiteiten;
- Ze voldoet binnen de 18 maanden na inwerkingtreding van de relevante gedelegeerde handelingen aan de regels zoals vastgelegd in artikel 22, lid 1 DGA.

Een organisatie voor data-altruïsme kan zich laten registreren overeenkomstig artikel 19 van de DGA. Wanneer een organisatie is erkend, wordt deze opgenomen in het openbare register voor erkende organisaties voor data-altruïsme dat iedere lidstaat heeft.[186]

Naast de vereisten die reeds zijn opgenomen in de DGA zelf, wordt van de Europese Commissie ook nog een guidance aangaande het rulebook[187] en het toestemmingsformulier[188] zoals vermeld in de DGA verwacht. Het kan aangewezen zijn voor organisaties om te wachten zich te laten erkennen als een organisatie voor data-altruïsme tot bekend is hoe verder uitwerking wordt gegeven aan deze artikelen. Het is mogelijk dat er immers bijkomstige verplichtingen zijn opgenomen in deze guidance.
Ook de bescherming van de rechten van de datasubjecten die toestemming geven in het kader van data-altruïsme worden geregeld in de DGA. Met name de te verstrekken informatie wordt bepaald, er wordt ingegaan op doelbinding en het verkrijgen van de toestemming voor de verwerking van persoonsgegevens. Momenteel blijkt er geen ambitie te zijn om de Health Data Space in de toekomst te kwalificeren als een **organisatie voor data-altruïsme**. Indien deze ambitie op termijn zou ontstaan, waarbij data subjecten vrijwillig hun gegevens openstellen voor bijvoorbeeld onderzoeksdoeleinden, moet met name rekening worden gehouden met de eis dat een dergelijke organisatie organisatorisch volledig onafhankelijk dient te zijn van elke commerciële tak van de Health Data Space. Dit roept echter de vraag op hoe zo'n organisatorische scheiding in de praktijk vormgegeven kan worden. Op dit punt biedt de DGA geen concrete antwoorden. Daarnaast leidt dit vraagstuk ook internationaal tot discussie.

---

[182] *Overweging 46 DGA.*

[183] *Ibid.*

[184] *Europese Commissie. (23 februari 2022). Commission Staff Working Document on Common European Data Spaces, p. 6.*

[185] *Europese Commissie. (24 september 2024). Implementing the Data Governance Act – guidance document, p. 14.*

[186] *Artikel 17 DGA.*

[187] *Artikel 22 DGA.*

[188] *Artikel 25 DGA.; zie ook V. Lähteenoja, J. Himanen, M. Turpeinen & S. Signorelli, The landscape of consent management tools – a data altruism perspective.*

Het vennootschapsrecht verschilt immers per lidstaat, waardoor de Europese Unie geen universeel toepasbare richtlijn kan bieden voor wat als structurele scheiding wordt beschouwd, of dit is toch moeilijk. Elke lidstaat kent eigen juridische en organisatorische nuances, wat een uniforme aanpak bemoeilijkt.

Bij de toepassing van de DGA rijzen er ook vragen over de **financiële duurzaamheid**, vooral met betrekking tot de financiële organisatie van een organisatie voor data-altruïsme. Het afstemmen van het bedrijfsmodel op het label van erkende organisatie voor data-altruïsme en de voorwaarden in de DGA blijkt vaak uitdagend. De Europese Commissie benadrukt bovendien dat "data-altruïsme" vanuit verschillende perspectieven moet worden bekeken, zowel wat betreft gegevensgebruik als de organisatorische opzet. Dit betekent dat zowel het bedrijfsmodel als de interne structuur gericht moeten zijn op het realiseren van een doel van algemeen belang. Het nastreven van winst is daarmee uitgesloten, en het gebruik van gegevens moet consistent blijven met het altruïstisch gedachtegoed.

Een interessante vraag is wat er gebeurt **wanneer onderzoek niet langer belangeloos is, maar eerder commercieel van aard wordt.** Sommigen stellen dat onderzoek altijd in het algemeen belang blijft, zelfs als de resultaten, zoals medicijnen, commercieel worden verkocht. Immers, ook betaalde medicatie dient het welzijn van patiënten en het genereren van kennis is altijd in het algemeen belang. Toch menen anderen dat er een structurele scheiding moet zijn tussen onderzoek in het algemeen belang en commercieel onderzoek. In de praktijk blijkt dit echter moeilijk uitvoerbaar, waardoor dit een blijvend punt van onduidelijkheid is (waar stopt onderzoek dat de opzet heeft meer kennis te creëren en waar begint het streven naar een commercieel haalbaar product). Deze vraag raakt ook aan de keuze van een bedrijfsmodel. Kan commercieel onderzoek worden nagestreefd binnen een "belangeloze context", zoals die van een vzw?

Deze discussie trekt zich door over de landsgrenzen heen, richting internationale context. De notie van **algemeen belang**, relevant voor DAO's aangezien zij een doel in het algemeen belang moeten vooropstellen, wordt nationaal ingevuld. Sommigen stellen dat deze nationale interpretatie de uitvoerbaarheid bemoeilijkt, omdat het begrip daardoor gefragmenteerd raakt. Voor de Health Data Space vormt dit geen groot probleem. Het faciliteren van onderzoek wordt doorgaans beschouwd als een doel van algemeen belang, zeker wanneer dit resulteert in preventieve gezondheidszorg, zoals bedoeld in de Data4PHM use case. De concrete moeilijkheden in toepassing van de notie van "algemeen belang" steekt daarom geen stokken in de wielen van een mogelijke wens tot registratie voor de Vlaamse Health Data Space, al is het mogelijk dat in de toekomst de Health Data Space een divers aantal verwerkingsactiviteiten ondersteunt, waarbij niet alle activiteiten in het algemeen belang zijn.

6.2.5.2.2 Databemiddelingsdiensten

Een databemiddelingsdienst, ook wel *data intermediary service provider* (DISP) genoemd, is een dienst die commerciële relaties faciliteert voor het delen van gegevens tussen een onbeperkt aantal datasubjecten[189] en gegevenshouders[190] aan de ene kant, en gegevensgebruikers[191] aan de andere kant. De regels in de DGA dienen ervoor dat dergelijke tussenpersonen fungeren als betrouwbare organisatoren van het delen of bundelen van gegevens binnen de gemeenschappelijke Europese dataruimten.[192] Het faciliteren van relaties gebeurt met behulp van technische, juridische of andere middelen, inclusief het ondersteunen van de uitoefening van de rechten van datasubjecten op hun persoonsgegevens.[193]

---

[189] Artikel 2(7) DGA omschrijft een "datasubject" als een betrokkene bedoeld in artikel 4, punt 1) AVG.

[190] Artikel 2(8) DGA omschrijft een "gegevenshouders" als een rechtspersoon, met inbegrip van openbare lichamen en internationale organisaties, of een natuurlijk persoon die geen datasubject is met betrekking tot de specifieke gegevens in kwestie, die overeenkomstig het toepasselijke Unierecht of nationale recht, het recht heeft om toegang te verlenen tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens of die te delen.

[191] Artikel 2(9) DGA omschrijft een "gegevensgebruiker" als een natuurlijk persoon of rechtspersoon die rechtmatige toegang heeft tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens en die het recht heeft, onder meer uit hoofde van Verordening (EU) 2016/679 in het geval van persoonsgegevens, om die gegevens voor commerciële of niet-commerciële doeleinden te gebruiken.

[192] Europese Commissie. (24 september 2024). Implementing the Data Governance Act – guidance document, p. 8.

[193] Artikel 2, lid 11, DGA.

De definitie van een DISP werd geschreven met de intentie om enkele reeds bestaande of opkomende modellen hieronder te doen vallen. In haar richtinggevende bijdrage van september 2024 verduidelijkt de Commissie dat DISPs, aangeboden door openbare lichamen om het hergebruik van beschermde gegevens die zij bezitten in overeenstemming met de DGA te vergemakkelijken, of het gebruik van andere gegevens te bevorderen, niet onder het begrip vallen, mits deze diensten geen commerciële relaties beogen tot stand te brengen. Hierdoor worden platforms voor gegevensuitwisseling die door overheidsinstanties zijn opgezet louter voor het digitaliseren van interacties tussen hen en individuen en bedrijven vrijgesteld. Dit betekent niet dat overheidsinstanties geen rol kunnen spelen in ecosystemen voor het delen van gegevens. Dit betekent dat zij bemiddelingsdiensten alleen hoeven te melden wanneer die diensten bedoeld zijn om de uitwisseling van gegevens van commerciële aard te vergemakkelijken en dus vergelijkbaar zijn met particulier aangeboden gegevensbemiddelingsdiensten, waardoor het billijk is deze aan dezelfde regels te onderwerpen.[194] Een van de modellen waarvan de wetgever wél beoogde om deze te laten vallen onder de term DISP zijn de orkestratoren van ecosystemen, bv. (gemeenschappelijke Europese) gegevensruimten waarin de deelnemers bepaalde (wettelijke en/of technische) regels voor deelname aan het ecosysteem aanvaarden.[195] Dit is relevant voor het huidige project, met name voor het secundaire gebruik van gegevens in een Health Data Space.

Een belangrijk gevolg van de regels dat het moet gaan om vrijwillig afgesloten commerciële relaties is dat het bedrijfsmodel van een DISP niet mag steunen op het verder delen van data door de tussenpersoon met partijen die de gebruiker van de dienst ("gegevenshouder") niet zelf heeft gekozen. Dit is bewust zo ingericht om het vertrouwen van gegevenshouders te vergroten. Het biedt hen de zekerheid dat alleen zijzelf – als gegevenshouders– en de door hen aanvaarde gegevensgebruikers kunnen profiteren van de waarde van de data. Bovendien blijft de volledige controle over welke partijen toegang krijgen tot de data bij de gegevenshouder.[196]

Voordat een entiteit zich als DISP kan beschouwen, moet eerst een **kennisgevingsprocedure** worden doorlopen. Artikel 11 van de DGA beschrijft de stappen die entiteiten moeten nemen om als officiële DISP te worden erkend. DISPs zijn verplicht hun voornemen om dergelijke diensten te verlenen te melden bij de bevoegde autoriteiten. Dit betekent dat een entiteit pas met bemiddelingsactiviteiten mag starten nadat de kennisgeving is afgerond.

De DGA gaat vervolgens verder door de term "databemiddelingsdiensten" te onderwerpen aan een resem vereisten in artikel 12 DGA. Enkele voorwaarden opgesomd:

- De DISP gebruikt de gegevens waarvoor hij databemiddelingsdiensten verleent niet voor andere doeleinden dan beschikbaarstelling aan gegevensgebruikers, en verleent databemiddelingsdiensten via een afzonderlijke rechtspersoon;
- DISPs kunnen het aanbieden van aanvullende specifieke instrumenten en diensten aan gegevenshouders of datasubjecten omvatten met het specifieke doel de gegevensuitwisseling te faciliteren, zoals tijdelijke opslag, curatie, conversie, anonimisering en pseudonimisering; die instrumenten mogen alleen worden gebruikt op uitdrukkelijk verzoek of met de uitdrukkelijke goedkeuring van de gegevenshouder of het datasubject, en de in dat verband aangeboden instrumenten van derden gebruiken gegevens niet voor andere doeleinden;
- De DISP zorgt ervoor dat de procedure voor toegang tot zijn dienst **billijk, transparant en niet-discriminerend** is voor zowel datasubjecten als gegevenshouders, alsook voor gegevensgebruikers, ook wat de prijzen en dienstverleningsvoorwaarden betreft;

[194] *Europese Commissie. (24 september 2024). Implementing the Data Governance Act – guidance document, p. 10.*

[195] *Ibid, 9.*

[196] *Ibid, 10.*

- DISPs mogen de gegevens niet delen met andere partijen dan die welke door de gebruiker zijn gekozen, en de verkregen gegevens en metagegevens kunnen alleen worden gebruikt om de gegevensbemiddelingsdienst te verbeteren (bij de verwerking van persoonsgegevens zou daarvoor een rechtsgrondslag uit hoofde van de AVG nodig zijn);
- DISPs zullen moeten voldoen aan strenge vereisten om deze **neutraliteit** te waarborgen en **belangenconflicten te voorkomen**. In de praktijk betekent dit dat voor entiteiten die momenteel ook andere diensten aanbieden, er nu een juridische scheiding moet zijn tussen de entiteit die de DISP aanbiedt en de entiteit die andere diensten verleent (d.w.z. de DISP moet via een afzonderlijke rechtspersoon worden verleend);
- Ook mogen de commerciële voorwaarden (met inbegrip van de prijsstelling) voor het verlenen van bemiddelingsdiensten niet afhankelijk zijn van de vraag of een potentiële gegevenshouder of -gebruiker gebruikmaakt van andere diensten.

Ten slotte bepaalt de DGA in de artikelen 13 en 14 dat iedere lidstaat een of meer bevoegde autoriteiten aanwijst om de taken in verband met de kennisgevingsprocedure uit te voeren en toezicht te houden op de naleving door aanbieders. De uitvoering die België hieraan heeft gegeven wordt hieronder besproken.

Op verzoek van een DISP moet de bevoegde autoriteit bevestigen of de tussenpersoon voldoet aan de kennisgevingsvereisten en de voorwaarden voor het verlenen van bemiddelingsdiensten in het kader van de DGA. Na een dergelijke bevestiging *kan* de tussenpersoon het label “in de Unie erkende aanbieder van databemiddelingsdiensten” gebruiken in zijn schriftelijke en mondelinge communicatie, en *moet* hij het door de Commissie vastgestelde gemeenschappelijke logo duidelijk weergeven op elke online- en offline publicatie die betrekking heeft op zijn gegevensbemiddelingsactiviteiten. De DISP is pas gerechtigd de databemiddelingsdiensten uit te voeren nadat deze de aanmeldingsprocedure heeft doorlopen.[197]

Wanneer ondernemingen of andere entiteiten meerdere gegevensgerelateerde diensten aanbieden, vallen alleen de activiteiten die direct verband houden met databemiddelingsdiensten onder deze verordening. Diensten die niet nastreven commerciële relaties tot stand te brengen, zoals databanken gericht op het hergebruik van wetenschappelijke onderzoeksgegevens volgens open toegang-principes, worden niet als databemiddelinsgdiensten beschouwd.[198] In principe kan een organisatie ook niet tegelijkertijd functioneren als DISP en als organisatie voor data-altruïsme.[199] Een mogelijke uitzondering kan ontstaan bij een voldoende mate van structurele scheiding tussen deze activiteiten, bijvoorbeeld door data-altruïsme onder te brengen in een zustervennootschap. Hoe dit in de praktijk vorm moet krijgen, blijft echter onduidelijk.

Kortom, DISPs ondersteunen het bilateraal of multilateraal delen van gegevens, het opzetten van platforms of databanken voor gedeeld gebruik van gegevens, en het creëren van infrastructuur om gegevenshouders en -gebruikers met elkaar te verbinden. Als organisatoren van ecosystemen voor gegevensdeling spelen DISP’s een sleutelrol bij het ontsluiten van markten binnen de gemeenschappelijke Europese dataruimten.[200]

Op het eerste gezicht lijkt de Health Data Space, althans voor wat betreft het secundair gebruik van gegevens, als **databemiddelingsdienst** te kwalificeren. De Health Data Space biedt immers een dienst aan die commerciële relaties faciliteert tussen datasubjecten en gegevenshouders aan de ene kant, en gegevensgebruikers aan de andere kant.

---

[197] *Europese Commissie. (23 februari 2022). Commission Staff Working Document on Common European Data Spaces, p. 6.*

[198] *Overweging 29 DGA: “Organisaties voor data-altruïsme die onder deze verordening vallen, mogen niet worden beschouwd als aanbieders van databemiddelingsdiensten, op voorwaarde dat die diensten geen commerciële relatie tot stand brengen tussen potentiële gegevensgebruikers enerzijds en datasubjecten en gegevenshouders die om altruïstische redenen gegevens beschikbaar stellen anderzijds.”*

[199] *Ibid.*

[200] *Europese Commissie. (23 februari 2022). Commission Staff Working Document on Common European Data Spaces, p. 6.*

Gegevenshouder (artikel 2(8) DGA = data provider in use case.
Gegevensgebruiker (artikel 2(9) DGA) = data user in use case.

Dit roept wel de vraag op wat precies bedoeld wordt met "**commerciële relatie**". Volgens een eerste *white paper* die geschreven werd door CiTiP[201] ligt de focus hier voornamelijk op de uiteindelijke handeling, namelijk de overdracht van gegevens. Dit betekent niet noodzakelijk dat er een economisch of handelsdoel aanwezig moet zijn. Dit blijkt o.m. uit het feit dat ook datasubjecten (die niet per se een commercieel belang hebben) partij kunnen zijn bij een commerciële relatie zoals bedoeld in de DGA. Hierdoor kan een entiteit ook als DISP kwalificeren wanneer het relaties tussen niet winst nastrevende entiteiten faciliteert. Dit toont dus ook concreet aan dat wanneer onderzoeksinstellingen, die niet noodzakelijk een winst nastrevend oogmerk hebben, de uiteindelijke gegevensgebruikers zijn in het kader van secundair gebruik van gegevens, de Health Data Space wel degelijk als DISP kan kwalificeren. Tot dusver de interpretatie die tot op heden aan het begrip "commerciële relatie" wordt gegeven. In artikel 10(a) van de DGA wordt expliciet vermeld dat de oprichting van platforms of databanken voor gegevensuitwisseling, evenals andere infrastructuren die de verbinding tussen gegevenshouders en -gebruikers mogelijk maken, onder de definitie van DISP vallen. De huidige Health Data Space zou, voor wat betreft het secundair gebruik van gegevens, dus als een DISP kunnen kwalificeren, aangezien het de intentie heeft om commerciële relaties te faciliteren voor het delen van gegevens tussen datasubjecten, gegevenshouders en -gebruikers.

Een registratie met het label "in de Unie erkende aanbieder van databemiddelingsdiensten" zou betrouwbaarheid uitstralen. Omdat vertrouwen een cruciale factor is voor gegevenshouders om hun waardevolle data beschikbaar te stellen aan gebruikers, zou een dergelijke registratie een verstandige keuze zijn. Bij de oprichting van de Health Data Space moet wel rekening worden gehouden met de extra eisen uit de DGA. Gelukkig lijkt de huidige opzet van de Vlaamse Health Data Space grotendeels in lijn te zijn met deze vereisten. Artikel 12 van de DGA is hier de spilbepaling in, waarbij de voornaamste vereisten deze van (structurele) neutraliteit zijn; de Health Data Space zal haar databemiddelingsactiviteiten gescheiden moeten houden van andere bezigheden (indien zij deze op het oog heeft). Zeker wanneer zij van plan is om zelf gegevens voor andere doeleinden te gebruiken, dan dient dit via een afzonderlijke rechtspersoon te gebeuren.

6.2.5.2.3 Gegevensgebruiker en gegevenshouder

Onder de DGA wordt een natuurlijke persoon of rechtspersoon die rechtmatige toegang heeft tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens en die het recht heeft, onder meer uit hoofde van de AVG in het geval van persoonsgegevens, om die gegevens voor commerciële of niet-commerciële doeleinden te gebruiken, beschouwd als een **gegevensgebruiker**.[202] Deze definitie benadrukt dat ook commerciële partners als een gegevensgebruiker kunnen worden aangemerkt.

Een "**gegevenshouder**" in de zin van de DGA is een rechtspersoon, met inbegrip van openbare lichamen en internationale organisaties, of een natuurlijke persoon die geen datasubject is met betrekking tot de specifieke gegevens in kwestie, die overeenkomstig het toepasselijke Unierecht of nationale recht, het recht heeft om toegang te verlenen tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens of die te delen.[203]

In de DGA wordt in beginsel geen onderscheid gemaakt tussen gegevenshouders en datasubjecten; de diensten van een DISP kunnen immers plaatsvinden tussen een gegevensgebruiker en een gegevenshouder of datasubject. Dit lijkt niet overal het geval. Zo zijn bepaalde diensten uitgesloten van de kwalificatie van databemiddelingsdienst, maar enkel indien deze worden verkregen van gegevenshouders.[204]

[201] *Centre for IT & IP. (2 oktober 2023). White Paper on the Definition of Data Intermediation Services.*

[202] *Artikel 2(9) DGA.*

[203] *Artikel 2(8) DGA.*

[204] *Zie artikel 2(11)(a) DGA.*

6.2.5.3 Nationale implementatie

De Kamer keurde op 8 mei 2024 de tekst van de wet tot uitvoering van de DGA goed.[205] Deze tekst regelt de procedures voor het hergebruik van bepaalde beschermde gegevens van de openbare sector, wat ook een aspect is dat door de DGA wordt geregeld. Daarnaast gaat de wet in op de oprichting van een controle- en inschrijvingsautoriteit voor enerzijds de registratie van, en anderzijds de controle op databemiddelings-diensten en organisaties voor data-altruïsme. Ten slotte schetst de wet de sanctiemechanismen die een toezichthoudende autoriteit kan opleggen wanneer een gegevensbemiddelingsdienst of organisaties voor data-altruïsme niet langer aan de vereiste voorwaarden voldoet. De wet wijzigt en voegt bepalingen toe aan het Belgisch Wetboek Economisch Recht (WER), meer bepaald aan Boek XV (Handhaving) en Boek XVII (Bijzondere rechtsprocedures). Via de website van de FOD ECONOMIE, in de implementatiewetgeving aangeduid als de entiteit verantwoordelijk voor de registratie, kan een registratie als databemiddelingsdienst/organisatie voor data-altruïsme worden aangevraagd via het door hen verschafte formulier.[206]

Tot slot verwijst de Memorie van Toelichting naar de federale dienstenintegrator van de FOD BOSA (FOD Beleid en Ondersteuning) als centraal informatiepunt voor vragen over aanvragen tot hergebruik (in overeenstemming met artikel 8 van de DGA) en als bevoegd orgaan op federaal niveau om overheidsorganen bij te staan bij de behandeling van deze aanvragen (in overeenstemming met artikel 7(1) DGA). Dit gebeurde door de Wet van 13 mei 2024 tot wijziging van de Wet van 15 augustus 2012 tot oprichting en organisatie van een federale dienstenintegrator.

Omdat de AVG van toepassing blijft, zijn de gegevensbeschermingsautoriteiten verantwoordelijk voor het toezicht op de naleving hiervan. Dit vereist mogelijk samenwerking tussen de autoriteit die is opgericht op basis van artikel 13 en 23 van de DGA en de bevoegde gegevensbeschermingsautoriteit.[207]

6.2.5.4 Slotoverwegingen

De DGA lijkt de specificiteiten van de **gezondheidscontext** onvoldoende mee te nemen. Het secundair gebruik van gegevens dient in de Health Data Space bijvoorbeeld om preventieve gezondheidszorg te kunnen uitvoeren. Het is echter discutabel dat dergelijke gegevensuitwisselingen vallen onder de term “commerciële relaties” zoals vereist in de definitie van een DISP. Om te kunnen kwalificeren als een DAO moet er dan weer aan (soms wel zeer) strenge voorwaarden worden voldaan[208] en lijkt de ingesteldheid niet geheel overeen te komen met de diversiteit aan uiteindelijke doeleinden die in de Health Data Space beoogd worden. Daarnaast bestaat ook de vraag hoe dit gecombineerd dient te worden met gegevensuitwisselingsaspecten voor primair gebruik ter uitvoering van de **EHDS-verordening**, en of het mogelijk blijft om dan nog als DISP te kwalificeren. Dit verschaft inhoud voor een volwaardige follow-up-studie. Dit kadert bovendien mee in de vraag hoe structurele scheiding er dan concreet uitziet. Is het een mogelijkheid dat een Health Data Space, volledig overeenkomstig de EHDS-verordening opgericht, ook databemiddelingsdiensten verricht zoals bedoeld in de DGA, of moet hier een dusdanige aparte rechtsstructuur voor op poten worden gezet? Dit zijn vragen waar de Commissie op dit ogenblik zelf nog geen antwoord op heeft. Het legt bovendien de vinger op de wonde door aan de kaak te stellen **hoe de DGA concreet interageert met de EHDS**. Dit blijkt niet concreet uitgedacht te zijn, dat terwijl de gezondheidssector net heel specifiek van aard is en dus wellicht extra aandacht verdient.

---

[205] *Wet tot uitvoering van Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 van 15 mei 2024.*

[206] *Zie https://economie.fgov.be/nl/themas/online/data-economie/data-governance-act.*

[207] *Europese Commissie. (24 september 2024). Implementing the Data Governance Act – guidance document, p. 2; Overweging 4 DGA.*

[208] *Het absolute verbod op winstgeneratie, de verplichting om als afzonderlijke rechtspersoon te opereren en het verbod op bepaalde activiteiten vormen echter hindernissen voor een praktische en pragmatische invulling van een dergelijke entiteit.*

Daarnaast blijkt er een probleem te bestaan rond de drijfveer om databemiddelingsdiensten aan te bieden, waarbij er niet voldoende ambitie is bij actoren om DISP te worden. De Commissie is van mening dat het aanbieden van databemiddelingsdiensten een winstgevende activiteit is, maar ook het huidige project is overheidsgefinancierd en -gedreven. De vraag is dus maar of er op termijn private spelers ambiëren om databemiddelingsdiensten te verschaffen, ook zonder financiering/subsidiëring. De wetgever lijkt uit te gaan van de veronderstelling dat datadeling winstgevend is en een financieel voordeel oplevert, waardoor ondernemingen hiertoe aangetrokken zijn.[209] In de praktijk blijkt echter, zoals ook uit dit project naar voren komt, dat de hoge instapkosten een aanzienlijke belemmering vormen, waardoor de return-on-investment – althans in het begin – problematisch is.
Bij de opstart van dit project werd aanvankelijk een gelimiteerde toepassing van een Health Data Space beoogd, waarbij van start werd gegaan met *use cases* die zich centreerden rond secundair gebruik.
Dit brengt met zich mee dat de Health Data Space niet altijd als een volwaardige health data space in de zin van de EHDS-verordening kon worden gezien, maar in sommige gevallen eventueel wél al als een DISP of een DAO kon worden gekwalificeerd. Over het algemeen lijkt de EU-wetgever de registratie te promoten door te stellen dat er een verhoogd vertrouwen aan de organisaties wordt gegeven als gevolg van de registratie en het gebruik van het label. Bovendien lijkt de wetgever uit te gaan van de veronderstelling dat datadeling winstgevend is en een financieel voordeel oplevert.[210] In de praktijk blijkt echter, zoals ook uit dit project naar voren komt, dat de hoge instapkosten een aanzienlijke belemmering vormen, waardoor de return-on-investment – althans in het begin – problematisch is.

6.2.6 EHDS-verordening

6.2.6.1 Inleiding

Op 3 mei 2022 heeft de Europese Commissie het voorstel voor een verordening betreffende de Europese ruimte voor gezondheidsgegevens (EHDS) aangenomen.[211] Het voorstel is het eerste sectorspecifieke kader voor het creëren van een Europese dataruimte in de gezondheidszorg. Op het moment van schrijven lijkt de wetgevingsprocedure de laatste ontwikkelingsfase te hebben bereikt. De medewetgevers van de EU hebben in het vroege voorjaar van 2024 overeenstemming bereikt over de verordening.[212] De compromistekst[213] werd in maart 2024 gepubliceerd in het kader van het bereiken van deze overeenstemming, waarbij de finale versie[214] beschikbaar is sinds 27 november 2024. De publicatie van de definitieve wettekst wordt verwacht tegen het einde van 2024 of het begin van 2025 en zal 20 dagen na publicatie in werking treden, gevolgd door een omzettingsperiode. Zodra de verordening in werking is getreden, zal deze rechtstreeks van toepassing zijn in alle lidstaten.

De verordening zal een Europese ruimte voor gezondheidsgegevens of *European health data space* (EHDS) tot stand brengen door te voorzien in gemeenschappelijke regels, normen, infrastructuren en een governance framework met als doel de toegang tot gezondheidsgegevens in de hele EU te vergemakkelijken. De verordening specificeert en vult de bepalingen en rechten aan die zijn vastgelegd in de AVG met betrekking tot het verzamelen, gebruiken en verwerken van persoonsgegevens of, specifiek in de context van de EHDS, persoonlijke elektronische gezondheidsgegevens.[215]

---

[209] Dit blijkt uit informele gesprekken die CiTiP hield met leden van de Europese Commissie met het oog op herziening van de Datagovernanceverordening.

[210] Dit blijkt uit informele gesprekken die CiTiP hield met leden van de Europese Commissie met het oog op herziening van de Datagovernanceverordening.

[211] Verordening (EU) 2024/… van het Europees Parlement en de Raad van … on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (hierna: EHDS).

[212] Europese Parlement. Legislative Train Schedule – proposal for a regulation on the European Health Data Space..

[213] Raad van de Europese Unie. (18 maart 2024). Proposal for a Regulation on the European Health Data Space – Analysis of the final compromise text with a view to agreement, 2022/0140(COD).

[214] Zie EHDS.

[215] Artikel 1(2) EHDS.

De EHDS zal met name de rechtsgrondslag[216] vormen voor het secundaire gebruik van elektronische gezondheidsgegevens.[217] Verder zullen gemeenschappelijke regels voor de succesvolle omzetting van systemen voor elektronische medische dossiers en een grensoverschrijdende infrastructuur worden omgezet om hun technische en organisatorische interoperabiliteit te bevorderen, aangezien zij de basis vormen voor het gebruik en de verdere uitwisseling van gezondheidsgegevens.[218] In dit verband wordt voorzien in diverse governancemechanismen en de implementatie van een veilige verwerkingsomgeving. Ook zullen individuen meer controle krijgen over hun eigen gezondheidsgegevens.

De regelgeving zal van toepassing zijn op houders en gebruikers van **gezondheidsgegevens**. Welke rol het huidige project zal innemen binnen de implementatie van een Belgische *health data space* (met het oog op de implementatie van een EHDS) moet echter nog worden bepaald. Op het moment van schrijven ligt de focus van de huidige projecten op het delen van geanonimiseerde, geaggregeerde gezondheidsdata, terwijl een nationale *health data space*, opgericht onder de EHDS, toegang zal bieden tot zowel persoonlijke als niet-persoonlijke gezondheidsdata. Gezien de huidige stand van het project kan de Health Data Space in de huidige fase worden beschouwd als een data-intermediair die mogelijk bijdraagt aan de EHDS, of het kan verder evolueren naar een nationale dataruimte zoals voorzien in de EHDS-verordening. Daarom moet op een later moment een definitieve evaluatie worden uitgevoerd.

6.2.6.2 Toepassingsgebied en relevante definities

De EHDS beoogt toegang tot gezondheidsdata opgeslagen in elektronische vorm te faciliteren door regels op te stellen voor het primaire en secundaire gebruik van deze gegevens. Om een beter onderscheid te maken tussen deze twee toepassingen, zijn de definities van primair en secundair gebruik aangepast ten opzichte van het oorspronkelijke voorstel uit 2022. Deze aangepaste definities zorgen voor meer duidelijkheid over de toepassing van de bepalingen in de EHDS. De Engelstalige definities worden meegegeven, aangezien dit op dit ogenblik de meest accurate versie van de wetgeving is.

6.2.6.2.1 Persoonlijke elektronische gezondheidsgegevens

Het kader definieert **elektronische gezondheidsgegevens** als zowel persoonlijke als niet-persoonlijke gezondheidsdata in elektronische vorm. Meer specifiek worden **persoonlijke elektronische gezondheidsgegevens** omschreven als: *"data concerning health and genetic data, processed in an electronic form."*[219] *Deze term is aldus ruimer dan de notie 'persoonsgegevens' in de AVG.*[220]

6.2.6.2.2 Niet-persoonlijke elektronische gezondheidsgegevens

Niet-persoonlijke elektronische gezondheidsgegevens worden gedefinieerd als: “"electronic health data other than personal electronic health data, including both data that have been anonymised so that they no longer relate to an identified or identifiable natural person (the 'data subject') and data that have never related to a data subject.”[221]

6.2.6.2.3 Primair gebruik van elektronische gezondheidsgegevens

Volgens de verordening betekent het **primaire gebruik** van elektronische gezondheidsgegevens: "the processing of electronic health data for the provision of healthcare, in order to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription,

[216] *Op basis van artikel 6.1.c) AVG (wettelijke verplichting die op de verwerkingsverantwoordelijke rust).*

[217] *Wat het primaire gebruik van elektronische gezondheidsgegevens betreft moet gekeken worden naar artikel 6.1 AVG. Hier wordt geen uitdrukkelijke rechtsgrond in de EHDS voorzien.*

[218] *Zie artikel 1 EHDS.*

[219] *Artikel 2(2)(a) EHDS.*

[220] *C., Baartmans, & W., Steenbruggen. (2023). Een Europese Unie voor zorgdata: so close yet so far, Computerrecht (NL), 2023(3), p. 220.*

[221] *Artikel 2(2)(b) EHDS.*

dispensation and provision of medicinal products and medical devices, as well as for relevant social, administrative or reimbursement services.”[222]

6.2.6.2.4 Secundair gebruik van elektronische gezondheidsgegevens

Het **secundaire gebruik** van elektronische gezondheidsgegevens wordt gedefinieerd als: “the processing of electronic health data for purposes set out in Chapter IV of this Regulation, other than the initial purposes for which they were collected or produced.”[223]

Enkele relevante toegelaten doeleinden zijn de volgende:

> “Scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefitting end-users, such as patients, health professionals and health administrators, including:
>
> - development and innovation activities for products or services;
> - training, testing and evaluation of algorithms, including in medical devices, in vitro diagnostic medical devices, AI systems and digital health applications;”[224]

> “Improvement of the delivery of care, of the optimization of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.”[225]

Er worden ook enkele doeleinden uitdrukkelijk opgesomd als verboden doeleinden voor secundair gebruik, met name activiteiten die conflicteren met de ethische voorschriften zoals bepaald in het nationale recht.[226]

6.2.6.2.5 Houder van gezondheidsgegevens

Volgens artikel 2(2)(t) van de EHDS wordt een **houder van gezondheidsgegevens** gedefinieerd als: “any natural or legal person, public authority, agency or other body in the healthcare or the care sectors, including reimbursement services where necessary, as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors, developing or manufacturing wellness applications, performing research in relation to the healthcare or care sectors or acting as a mortality registry, as well as any Union institution, body, office or agency”[227]

Als een entiteit onder deze definitie valt en beschikt over ten minste een van de minimumcategorieën elektronische gezondheidsgegevens die zijn vastgesteld in artikel 51 van de EHDS, is de betreffende entiteit verplicht een beschrijving van de gegevensverzamelingen te verstrekken aan instanties die toegang hebben tot gezondheidsgegevens en de gegevens op verzoek aan hen beschikbaar te stellen. De EHDS voorziet in een specifieke procedure die hieronder verder wordt toegelicht. Bepaalde categorieën houders van gezondheidsgegevens, zoals individuele onderzoekers, natuurlijke personen of rechtspersonen die micro-ondernemingen vormen, kunnen echter worden vrijgesteld van de verplichtingen voor secundair gebruik.[228]

---

[222] *Artikel 2(2)(d) EHDS.*

[223] *Artikel 2(2)(e) EHDS; artikel 54 EHDS verbiedt expliciet bepaalde types van secundair gebruik van elektronische gezondheidsgegevens (bv. wanneer producten of diensten schadelijk kunnen zijn voor personen, de volksgezondheid, of samenlevingen in het algemeen (para. (e)), of wanneer de activiteiten in strijd zijn met ethische bepalingen uit hoofde van het nationale recht (para. (e ter)).*

[224] *Artikel 53(1)(e) EHDS.*

[225] *Artikel 53(1)(f) EHDS.*

[226] *Artikel 54, lid 2, (e) EHDS.*

[227] *Artikel 2(2)(t) EHDS.*

[228] *Artikel 50 EHDS.*

6.2.6.2.6 Gebruiker van gezondheidsgegevens

Een gebruiker van gezondheidsgegevens, d.w.z. een entiteit die deelneemt aan de Europese ruimte voor gezondheidsgegevens door toegang te krijgen tot de gegevens, kan elke natuurlijke of rechtspersoon zijn die de aanvraagprocedure voor toegang tot de gegevens met succes heeft doorlopen. Meer specifiek wordt een gebruiker van gezondheidsgegevens die toegang vraagt tot gegevens voor secundair gebruik gedefinieerd als "*a natural or legal person, including Union institutions, bodies or agencies, which has been granted lawful access to electronic health data for secondary use pursuant to a data permit, data request or an access approval by an authorized participant in Health Data @ EU."*[229]

6.2.6.3 Gegevenstoegang en categorieën elektronische gezondheidsgegevens voor secundair gebruik

6.2.6.3.1 Categorieën ven elektronische gezondheidsgegevens

De EHDS stelt een lijst op met **minimumcategorieën van elektronische gezondheidsgegevens** die houders van gezondheidsgegevens beschikbaar moeten stellen **voor secundair gebruik**.[230] Met name de volgende soorten elektronische gezondheidsgegevens moeten worden gedeeld:

- elektronische gezondheidsgegevens uit *electronic health records* (EHR's);
- gegevens over factoren die van invloed zijn op de gezondheid, waaronder sociaal-economische, milieu- en gedragsdeterminanten van gezondheid;
- geaggregeerde gegevens over de behoeften aan gezondheidszorg, de middelen die aan gezondheidszorg worden toegewezen, de verstrekking van en de toegang tot gezondheidszorg, de uitgaven voor en de financiering van de gezondheidszorg;
- gegevens over ziekteverwekkers, met gevolgen voor de menselijke gezondheid;
- administratieve gegevens over gezondheidszorg, waaronder gegevens over verstrekkingen, declaraties en vergoedingen;
- genetische, epigenomische en genomische gegevens over de mens;
- andere menselijke moleculaire gegevens zoals proteomische transcriptomische, metabolomische, lipidomische en andere omische gegevens;
- automatisch gegenereerde persoonlijke elektronische gezondheidsgegevens via medische apparatuur;
- gegevens van wellness toepassingen;
- gegevens over beroepsstatus, specialisatie en instelling van gezondheidswerkers die betrokken zijn bij de behandeling van een natuurlijke persoon;
- bevolkingsgebonden registers van gezondheidsgegevens (volksgezondheidsregisters);
- **gegevens uit medische registers** en mortaliteitsregisters;
- **gegevens uit klinische proeven**, klinische studies en klinische onderzoeken die respectievelijk onder Verordening (EU) 536/2014, Verordening [SOHO], Verordening (EU) 2017/745 en Verordening (EU) 2017/746 vallen;
- andere gezondheidsgegevens van **medische hulpmiddelen**;
- gegevens uit registers voor geneesmiddelen en medische hulpmiddelen;
- gegevens uit onderzoekscohorten, vragenlijsten en enquêtes met betrekking tot gezondheid, na de eerste publicatie van resultaten;
- gezondheidsgegevens van biobanken en aanverwante databanken.

[229] *Zie artikel 2(2)(u) EHDS. Volgens artikel 61 (3) EHDS is het de plicht van een gebruiker van gezondheidsgegevens om natuurlijke personen niet opnieuw te identificeren of proberen te identificeren aan de hand van de verkregen gegevens.*

[230] *Zie artikel 51 EHDS.*

6.2.6.3.2 Lidstaten

Naast de bovengenoemde categorieën biedt de EHDS de lidstaten de mogelijkheid om op grond van nationale wetgeving extra categorieën elektronische gezondheidsgegevens toe te voegen die beschikbaar moeten worden gesteld voor secundair gebruik binnen de EHDS.[231] Hoewel dit waarschijnlijk zal leiden tot een gefragmenteerde aanpak in de verschillende EU-landen, wordt erkend dat ook andere soorten gegevens van belang kunnen zijn. Bovendien mogen de lidstaten strengere toegangsregels invoeren voor bepaalde soorten gevoelige gegevens, zoals genetische gegevens. De lidstaten mogen strengere maatregelen en aanvullende waarborgen invoeren om de gevoeligheid van de te delen gegevens te beschermen.

6.2.6.3.3 Toegang tot gegevens en de Health Data Access Body

De EHDS voorziet in een aanvraagprocedure voor gebruikers van gezondheidsgegevens zoals onderzoekers en andere belanghebbenden die toegang willen tot elektronische gezondheidsgegevens voor secundair gebruik.[232] Als zij toestemming krijgen, wordt hun toegang verleend tot de hierboven genoemde gevraagde categorieën, waarbij het beginsel van gegevensminimalisatie en doelbinding in acht wordt genomen.[233] Het verzoek om toegang wordt beoordeeld door **de Health Data Access Body (HDAB)** *(instantie voor de toegang tot gezondheidsgegevens)*.[234] Meer in het bijzonder is het de verantwoordelijkheid van het HDAB (overeenkomstig de taak die aan hen is toegewezen volgens artikel 57, lid 1, onder a), van de EHDS) om te beslissen over verzoeken om toegang tot gegevens, om toestemming te verlenen en om gegevensvergunningen af te geven. Ook kan een vereenvoudigde toegangsprocedure voor vertrouwde houders van gezondheidsgegevens worden omgezet.[235]

In het algemeen moet een natuurlijke of rechtspersoon die toegang tot de gewenste gegevens wil verkrijgen, een **verzoek om toegang tot gegevens**[236] voor de in artikel 53 van de EHDS vastgestelde doeleinden indienen bij het HDAB. In dit verband zal de Europese Commissie de modellen uiteenzetten om de toegang tot gegevens te bevorderen.[237] Als de aanvraag voor toegang tot de gegevens wordt goedgekeurd, worden de elektronische gezondheidsgegevens in een geanonimiseerd of gepseudonimiseerd formaat beschikbaar gesteld. In het geval dat toegang tot gepseudonimiseerde gegevens wordt gevraagd, moeten gebruikers van gezondheidsgegevens rechtvaardigen waarom de verwerking niet kan worden voortgezet met behulp van geanonimiseerde gegevens en een beschrijving geven van hoe het gebruik van gepseudonimiseerde gegevens (die persoonsgegevens zijn in overeenstemming met de AVG) zou voldoen aan de toepasselijke nationale en EU-wetgeving inzake gegevensbescherming en privacy.[238] Het HDAB moet een positief besluit nemen en toegang tot gegevens verlenen (in de vorm van een gegevensvergunning) als aan alle vereisten van artikel 67 van de EHDS, die hieronder verder zullen worden uitgewerkt, is voldaan. In het bijzonder vraagt het HDAB na de afgifte van de gegevensvergunning de gegevens onmiddellijk op bij de houder van de gezondheidsgegevens. HDAB stelt de gegevens dan in beginsel ter beschikking van de gebruiker van het gezondheidsgegevensbestand binnen twee maanden nadat het deze van de houder heeft ontvangen.[239]

---

[231] *Artikel 51 EHDS.*

[232] *Zie artikelen 67 en 68 EHDS.*

[233] *Volgens artikel 66 EHDS mag het orgaan voor toegang tot gezondheidsgegevens alleen toegang verlenen tot dergelijke elektronische gezondheidsgegevens die toereikend en relevant zijn en beperkt zijn tot wat nodig is in verband met het doel.*

[234] *Elke lidstaat wijst een of meer instanties voor toegang tot gezondheidsgegevens aan om de krachtens de EHDS toegewezen taak uit te voeren (d.w.z. overeenkomstig artikel 57-59 EHDS). De lidstaten moeten ervoor zorgen dat de aangewezen Health Data Access Body de personele en financiële middelen krijgt om haar taak uit te voeren. Indien de nationale wetgeving de beoordeling door ethische instanties vereist, moeten deze instanties hun deskundigheid ter beschikking stellen van de Health Data Access Body (zie artikel 55, 55(2) EHDS).*

[235] *Artikel 72 EHDS.*

[236] *Zie artikel 67 EHDS.*

[237] *Artikel 69, 70 EHDS. Artikel 70 EHDS deelt mee dat deze modellen moeten volgen twee jaar na de inwerkingtreding van de verordening, d.w.z. waarschijnlijk begin 2027.*

[238] *Zie artikel 67(2)(e) EHDS; In artikel 67(2)van de EHDS zijn de eisen of informatie vastgelegd die in de toepassing voor gegevenstoegang moeten worden opgenomen.*

[239] *Artikel 68, lid 7, van de EHDS.*

Over het algemeen wordt de gegevensvergunning afgegeven voor de duur die nodig is om het doel te bereiken, maar niet langer dan tien jaar.[240]

Bij het verlenen van toegang tot (persoonlijke en niet-persoonlijke) elektronische gezondheidsgegevens in overeenstemming met de afgegeven gegevensvergunning, mag het HDAB dit alleen doen via een **beveiligde verwerkingsomgeving**, met technische en organisatorische maatregelen en beveiligings- en interoperabiliteitsvereisten. Om een veilige verwerkingsomgeving tot stand te brengen, stelt de EHDS bepaalde voorwaarden en beveiligingsmaatregelen waaraan moet worden voldaan. Hoewel artikel 73 van de EHDS een aantal van die maatregelen bevat om een veilige verwerkingsomgeving te faciliteren, wordt van de Europese Commissie verwacht dat zij door middel van uitvoeringshandelingen voorziet in de technische, organisatorische, informatiebeveiligings-, vertrouwelijkheids-, gegevensbeschermings- en interoperabiliteitsvereisten voor beveiligde verwerkingsomgevingen.[241]

6.2.6.3.4 Vereisten voor toegang tot gegevens

Zoals in het vorige deel is aangegeven, zal een HDAB alleen een **gegevensvergunning** afgeven als de deelnemer aan de gegevensruimte (namelijk de gebruiker van gezondheidsgegevens) cumulatief voldoet aan de vereisten van artikel 67 van de EHDS. In het bijzonder is bepaald in artikel 67(1) van de EHDS dat:

- toegang alleen kan worden verleend als het in de aanvraag voor gegevenstoegang beschreven doel [242] overeenstemt met een of meer van de in artikel 53, lid 1, van de EHDS, genoemde doeleinden;
- toegang alleen wordt verleend als de gevraagde elektronische gezondheidsgegevens **noodzakelijk, adequaat en evenredig zijn** in verhouding tot het doel of de doeleinden die door de gebruiker van gezondheidsgegevens in de toepassing voor gegevenstoegang zijn aangegeven. Hierbij wordt rekening gehouden met het beginsel van minimale gegevensverwerking en doelbinding (dat vereist dat alleen die persoonsgegevens in aanmerking worden genomen die toereikend en ter zake dienend zijn en beperkt zijn tot wat noodzakelijk is in verband met het doel) in artikel 66 van de EHDS;
- met name in het geval van het gebruik van **gepseudonimiseerde gegevens** de aanvragers van gegevens moeten aantonen dat ze voldoen aan een rechtsgrondslag[243] van artikel 6, lid 1, van de AVG en aantonen dat er voldoende rechtvaardiging is dat het verwachte doel niet kan worden bereikt met geanonimiseerde gegevens;
- aanvragers van gegevens gekwalificeerd moeten zijn **met betrekking tot de beoogde** doeleinden van het gebruik van gegevens en beschikken over de juiste deskundigheid, met inbegrip van beroepskwalificaties op het gebied van gezondheidszorg, zorg, volksgezondheid, onderzoek, in overeenstemming met de ethische praktijk en de toepasselijke wet- en regelgeving;
- aanvragers aantonen dat er **voldoende technische en organisatorische maatregelen zijn genomen om misbruik** van elektronische gezondheidsgegevens **te voorkomen en de rechten en belangen** van de houder van de gegevens en de betrokken natuurlijke personen te beschermen;
- de informatie over de beoordeling van de **ethische aspecten** van de verwerking, indien van toepassing, in overeenstemming is met het nationale recht;
- indien een aanvrager gebruik wenst te maken van een uitzondering op grond van artikel 71, lid 4, betreffende het recht om af te zien van secundair gebruik van natuurlijke personen, moeten de toelichtingen worden verstrekt die vereist zijn door het nationale recht dat op grond van dat artikel is vastgesteld;
- de aanvrager van gezondheidsgegevens aan alle andere vereisten van hoofdstuk IV voldoet.

---

[240] Artikel 68, lid 12, EHDS.

[241] Artikel 73, lid 5, van de EHDS.

[242] Volgens artikel 69 EHDS.

[243] In overweging 52 EHDS wordt met name verwezen naar artikel 6, lid 1, onder a), c), e of f), AVG.

Naast de opgesomde vereisten zal de betrokken HDAB ook rekening houden met bepaalde **risico's** alvorens een gegevensvergunning af te geven, namelijk risico's voor de nationale defensie, veiligheid, openbare veiligheid en openbare orde, alsook risico's van ondermijning van vertrouwelijke gegevens in overheidsdatabanken van regelgevende instanties.[244] Als deze risico's voldoende zijn gemitigeerd en aan de vereisten van artikel 68, lid 1, EHDS is voldaan, geeft het HDAB een gegevensvergunning af. Anders, als niet wordt voldaan aan de eisen van de EHDS, zal het HDAB de aanvraag weigeren. Als de gegevensvergunning moet worden bijgewerkt, moet de gebruiker van gezondheidsgegevens een verzoek tot wijziging indienen op grond van artikel 68, lid 13, EHDS. Om toegang te krijgen tot elektronische gezondheidsgegevens voor secundair gebruik, kunnen HDAB's kosten in rekening brengen.[245]

6.2.6.3.5 Doel

HDAB's verlenen alleen voor bepaalde doeleinden toegang tot elektronische gezondheidsgegevens voor secundair gebruik. De EHDS-regeling somt in artikel 53 van de EHDS de doeleinden op waarvoor gebruikers deze gegevens mogen verwerken of gebruiken, namelijk:

- het algemeen belang op het gebied van de **volksgezondheid en de gezondheid op het werk**, zoals activiteiten ter bescherming tegen **ernstige grensoverschrijdende bedreigingen van de gezondheid en het toezicht op de volksgezondheid of activiteiten ter waarborging van een hoog niveau van kwaliteit en veiligheid van de gezondheidszorg**, met inbegrip van de veiligheid van de patiënt, en van geneesmiddelen of medische hulpmiddelen (lid 1, onder a);
- **beleidsvorming en regelgevende activiteiten** ter ondersteuning van overheidsinstanties of instellingen, agentschappen en organen van de Unie, met inbegrip van regelgevende instanties, in de gezondheids- of zorgsector bij de uitvoering van hun taken die in hun mandaten zijn omschreven (lid 1, onder b);
- **statistieken**, zoals nationale, multinationale en officiële statistieken op Unieniveau zoals gedefinieerd in Verordening (EU) nr. 223/2009 met betrekking tot de gezondheids- of zorgsector (lid 1, onder c);
- **onderwijs- of onderwijsactiviteiten** in de gezondheids- of zorgsector op het niveau van het beroeps- of hoger onderwijs (lid 1, letter d);
- **wetenschappelijk onderzoek in verband met de gezondheids- of zorgsector**, dat bijdraagt tot de volksgezondheid of de evaluatie van gezondheidstechnologie, of dat een hoog kwaliteits- en veiligheidsniveau van de gezondheidszorg, van geneesmiddelen of medische hulpmiddelen waarborgt, met als doel de eindgebruikers, zoals patiënten, gezondheidswerkers en gezondheidsbeheerders, ten goede te komen, met inbegrip van (lid 1, onder e):
  - ontwikkelings- en innovatieactiviteiten voor producten of diensten;
  - het opleiden, testen en evalueren van algoritmen, onder meer in medische hulpmiddelen, medische hulpmiddelen voor in-vitrodiagnostiek, AI-systemen en digitale gezondheidstoepassingen
- het **verbeteren van de zorgverlening, het optimaliseren van de behandeling en het verlenen van gezondheidszorg**, op basis van de elektronische gezondheidsgegevens van andere natuurlijke personen (lid 1, sub h).

De toegang tot de eerste drie doeleinden (lid 1, onder a) tot en met c)) is voorbehouden aan openbare lichamen en instellingen, organen en instanties van de Unie.[246] Bovendien moeten gebruikers van gezondheidsgegevens elektronische gezondheidsgegevens voor secundair gebruik verwerken op basis en in overeenstemming met de gegevensvergunning of het gegevensverzoek. In artikel 54 van de EHDS schetst de verordening bepaalde doeleinden waarvoor het secundaire gebruik van elektronische gezondheidsgegevens verboden is (bv. als producten of diensten schade kunnen toebrengen aan personen, de volksgezondheid of de samenleving als geheel).

---

[244] Artikel 68(1) EHDS.

[245] Zie artikel 62 EHDS.

[246] Artikel 53, lid 2, EHDS.

6.2.6.3.6 Gegevens beschermd door IE-rechten en bedrijfsgeheimen

De EHDS volgt de algemene veronderstelling dat alle elektronische gezondheidsgegevens, met inbegrip van dergelijke elektronische gezondheidsgegevens die worden beschermd door intellectuele eigendomsrechten en handelsgeheimen, beschikbaar moeten worden gesteld voor secundair gebruik in overeenstemming met de EHDS-verordening.[247] De houder van gezondheidsgegevens informeert het verantwoordelijke HDAB en identificeert alle elektronische gezondheidsgegevens die inhoud of informatie bevatten die worden beschermd door intellectuele-eigendomsrechten of handelsgeheimen en/of die vallen onder het regelgevingsrecht inzake gegevensbescherming als bedoeld in artikel 10, lid 1, van Richtlijn 2001/83/EG of artikel 14, lid 11, van Verordening (EG) nr. 726/2004. De houder van de gezondheidsgegevens moet dan aangeven om welke delen van de datasets het gaat en motiveren waarom de gegevens in kwestie specifieke bescherming behoeven.[248] Naar aanleiding van de ontvangen informatie zal het betrokken HDAB vervolgens moeten beslissen over alle passende en evenredige maatregelen (met inbegrip van juridische, organisatorische en technische) en deze moeten nemen om deze rechten te beschermen.[249] Het HDAB kan de toegang tot bepaalde elektronische gezondheidsgegevens afhankelijk stellen van wettelijke, organisatorische en technische maatregelen, die ook contractuele overeenkomsten tussen houders en gebruikers van gezondheidsgegevens kunnen omvatten. In dit verband moet de Europese Commissie niet-bindende modelcontractbepalingen voor dergelijke regelingen ontwikkelen.[250] Indien nodig kan het HDAB de toegang tot dergelijke gegevens weigeren indien het verlenen van toegang tot elektronische gezondheidsgegevens voor secundair gebruik een ernstig risico zou inhouden dat niet op bevredigende wijze kan worden aangepakt om te beschermen tegen een inbreuk op de intellectuele-eigendomsrechten, handelsgeheimen of het regelgevingsrecht inzake gegevensbescherming als bedoeld in artikel 10, lid 1, van Richtlijn 2001/83/EG of artikel 14, lid 11, van Verordening (EG) nr. 726/2004.[251]

6.2.6.3.7 Plichten voor gebruikers van gezondheidsgegevens

Artikel 61 van de EHDS-verordening stelt bepaalde plichten vast voor gebruikers van gezondheidsgegevens. Zodra zij toegang hebben gekregen tot de gegevens, hebben zij de gegevens niet meer tot hun beschikking. De bepaling bepaalt onder meer dat het voor gebruikers van gezondheidsgegevens verboden is om bij de verwerking van gegevens binnen de beveiligde verwerkingsomgeving toegang te verlenen tot of anderszins ter beschikking te stellen aan **derden die niet in de gegevensvergunning zijn genoemd.** Bovendien mogen gebruikers van gezondheidsgegevens de natuurlijke personen waarop de elektronische gezondheidsgegevens betrekking hebben en die zij hebben verkregen op basis van de gegevensvergunning, het gegevensverzoek of het besluit tot goedkeuring van de toegang door een bevoegde deelnemer aan Health Data EU, **niet opnieuw identificeren of proberen te heridentificeren**. Bovendien is het interessant om op te merken dat de EHDS een vorm van **wederkerigheidsoverweging** heeft geïntegreerd.
Gebruikers van gezondheidsgegevens moeten namelijk **de resultaten of output van het secundaire gebruik van elektronische gezondheidsgegevens, met inbegrip van informatie die relevant is voor de verstrekking van gezondheidszorg, openbaar maken binnen 18 maanden na voltooiing van de verwerking van elektronische gezondheidsgegevens in de beveiligde omgeving of nadat zij het antwoord op het in artikel 69 bedoelde gegevensverzoek hebben ontvangen** (resultaten of output bevatten alleen anonieme gegevens (!)).[252]

---

[247] *Zie artikel 52 EHDS.*

[248] *Zie artikel 52, lid 2, EHDS; De informatie wordt verstrekt wanneer de beschrijvingen van de datasets overeenkomstig artikel 60, lid 3, EHDS, aan de Health Data Access Body worden meegedeeld, of uiterlijk wanneer zij een verzoek van de Health Data Access Body ontvangt.*

[249] *Artikel 52 bis, lid 3 tot en met 3 EHDS.*

[250] *Artikel 52 bis, lid 4, EHDS.*

[251] *Artikel 52 bis, lid 5, EHDS.*

[252] *Artikel 61(4) EHDS.*

6.2.6.3.8 Rechten van particulieren in het kader van secundair gebruik

Opt-out-mechanisme

Met de laatste wetswijziging kwam onder meer de invoering van een **opt-outmechanisme** op het niveau van de lidstaten. Patiënten moeten de mogelijkheid hebben om af te zien van het gebruik van hun gezondheidsgegevens door een beroepsbeoefenaar in de gezondheidszorg (primair gebruik) of verder gebruik (secundair gebruik).[253]

Specifiek wat dit laatste betreft, zullen personen het recht hebben om af te zien van de verwerking van persoonlijke elektronische gezondheidsgegevens voor secundair gebruik.[254] Natuurlijke personen hoeven geen redenen op te geven over waarom zij zich willen afmelden en zij kunnen dit op elk moment doen. Het is aan de lidstaten om te zorgen voor een toegankelijk en gemakkelijk te begrijpen opt-out-mechanisme. Zodra een persoon gebruik maakt van zijn of haar recht tot opt-out, mogen de persoonlijke elektronische gezondheidsgegevens niet beschikbaar worden gesteld of anderszins worden verwerkt op grond van de gegevensvergunning volgens artikel 68 van de EHDS of gegevensverzoek volgens artikel 69 van de EHDS. Het recht op opt-out mag echter geen invloed hebben op de verwerking die is toegestaan voordat de betrokkene gebruik maakte van zijn recht op opt-out.[255]

Bovendien kunnen de lidstaten op grond van de nationale wetgeving uitzonderingen vaststellen voor het beschikbaar stellen van gegevens, ongeacht het recht op opt-out. Een dergelijke uitzondering[256] zou bijvoorbeeld kunnen gelden voor openbare lichamen of instellingen, organen of instanties van de Unie met een mandaat voor de uitvoering van taken op het gebied van de volksgezondheid en uitsluitend met het oog op wetenschappelijk onderzoek, om gewichtige redenen van algemeen belang en de in artikel 53, lid 1, onder a) tot en met c), van de EHDS bedoelde doeleinden.

Recht op informatie

De wetgevers kwamen overeen om gebruikers van gezondheidsgegevens te verplichten het HDAB te informeren over bevindingen die door onderzoek zijn ontdekt en die van invloed kunnen zijn op de gezondheid van patiënten.[257] HDAB's die door gebruikers van gezondheidsgegevens op de hoogte zijn gesteld van een belangrijke bevinding in verband met de gezondheid van een persoon, stellen vervolgens de houder van de gezondheidsgegevens op de hoogte, die vervolgens (in overeenstemming met de krachtens het nationale recht vast te stellen vereisten) de persoon of zijn of haar behandelende gezondheidswerker moet informeren. Natuurlijke personen kunnen echter ook het recht hebben om te verzoeken niet van dergelijke bevindingen op de hoogte te worden gebracht.[258] Voor de ontwikkeling van het huidige project is dat eveneens een aspect om op te volgen en mogelijk te maken in de toekomst.

6.2.6.4 Governance-infrastructuur voor secundair gebruik

De EHDS zal verschillende governance-infrastructuren opzetten, zowel op nationaal als op internationaal niveau, om de succesvolle omzetting van een Europese ruimte voor gezondheidsgegevens te vergemakkelijken.

Op **nationaal niveau** zal de uitwisseling van elektronische gezondheidsgegevens worden bevorderd via een netwerk van HDAB's. Zoals hierboven uiteengezet, zullen HDAB's een cruciale rol spelen bij de toegang tot elektronische gezondheidsgegevens voor secundair gebruik. HDAB's zijn openbare organen die in elke EU-lidstaat moeten worden benoemd of opgericht. In het kader van internationale samenwerking, zullen deze HDAB's met elkaar moeten samenwerken.

---

[253] *Bepaalde secundaire vormen van gebruik kunnen nog steeds bij wijze van uitzondering worden toegestaan voor doeleinden van algemeen belang, beleidsvorming, statistiek en onderzoek in het algemeen belang (ibid.). Zie ook artikel 71, overweging 57 EHDS.*

[254] *Artikel 71 EHDS.*

[255] *Artikel 71, lid 2, EHDS.*

[256] *Artikel 71, lid 4, EHDS.*

[257] *Ibid; zie ook artikel 61, lid 5, EHDS.*

[258] *Artikel 58, lid 3, EHDS.*

Op **internationaal niveau** moeten het **HealthData@EU**-initiatief en de **EHDS-raad** het delen van elektronische gezondheidsgegevens voor secundair gebruik bevorderen. HealthData@EU is in het leven geroepen om grensoverschrijdend secundair gebruik te bevorderen.[259] Daartoe wijst elke lidstaat één **nationaal contactpunt aan voor secundair gebruik van elektronische gezondheidsgegevens**.
Het nationale contactpunt zal een organisatorische en technische toegangspoort vormen om het gebruik van elektronische gezondheidsgegevens in een grensoverschrijdende context te vergemakkelijken, aangezien het zal aansluiten op de infrastructuur voor secundair gebruik van elektronische gezondheidsgegevens (HealthData@EU). Volgens de EHDS kunnen derde landen of internationale organisaties geautoriseerde deelnemers worden wanneer zij voldoen aan de relevante EHDS-regels en toegang verlenen aan gegevensgebruikers uit de EU.[260]

Het Europees Comité voor de ruimte voor gezondheidsgegevens (EHDS-raad) is een bestuursorgaan op hoog niveau dat moet worden opgericht om de samenwerking en de uitwisseling van informatie tussen de lidstaten en de Commissie te vergemakkelijken.[261] De EHDS-raad zal bestaan uit twee vertegenwoordigers per lidstaat, één vertegenwoordiger voor primair gebruik en één voor secundair gebruik. De raad zal ook samenwerken met andere relevante nationale autoriteiten, deskundigen en waarnemers en hen uitnodigen om hun vergaderingen bij te wonen. Agentschappen kunnen in bepaalde omstandigheden worden uitgenodigd.

6.2.6.5 Handhaving

Met het oog op de uitvoering van succesvolle handhavingsprocedures[262] in het kader van de EHDS zullen HDAB's in dit verband een leidende rol spelen. HDAB's houden toezicht op de naleving door gebruikers van gezondheidsgegevens en houders van gezondheidsgegevens van de vereisten van deze verordening.[263] Zij hebben het recht om van houders van gezondheidsgegevens en gebruikers van gezondheidsgegevens alle nodige informatie te vragen om de naleving te verifiëren. Als een gebruiker of houder van gezondheidsgegevens niet aan de vereisten voldoet, stelt het verantwoordelijke HDAB hen in kennis van die bevindingen en neemt het passende maatregelen. Houders/gebruikers van gezondheidsgegevens kunnen binnen maximaal vier weken hun mening geven. Als de niet-naleving betrekking heeft op een inbreuk in verband met persoonsgegevens in de zin van de AVG, zal het HDAB de toezichthoudende autoriteit op de hoogte stellen.

In geval van **niet-naleving door een gebruiker van gezondheidsgegevens** kan het HDAB de toestemming intrekken en de betrokken verwerking zonder onnodige vertraging stopzetten en passende maatregelen nemen. Als onderdeel van een dergelijke maatregel kan het HDAB ook, indien nodig, de gebruiker van gezondheidsgegevens uitsluiten of een procedure starten om deze uit te sluiten in overeenstemming met de nationale wetgeving van elke toegang binnen de EHDS in het kader van secundair gebruik voor een periode van maximaal 5 jaar.[264]

In geval van **niet-naleving door een houder van gezondheidsgegevens** kan het HDAB de houder van de gegevens een boete/dwangsom opleggen wanneer de houder bepaalde gegevens achterhoudt met de kennelijke bedoeling het gebruik van elektronische gezondheidsgegevens te belemmeren of de termijn niet na te leven voor iedere dag dat zij zich niet in regel stellen.[265] In geval van herhaalde inbreuken kunnen HDAB's gegevenshouders uitsluiten van het indienen van verzoeken om toegang tot gegevens van maximaal 5 jaar (terwijl ze nog steeds verplicht zijn om gegevens beschikbaar te stellen).

[259] *Zie artikel 75, lid 4, EHDS.*

[260] *Artikel 75, lid 5 EHDS.*

[261] *Artikel 92 EHDS.*

[262] *De algemene voorwaarden voor het opleggen van boetes zijn vastgelegd in artikel 64 EHDS.*

[263] *Artikel 57, lid 1, onder a), ii), artikel 63 EHDS.*

[264] *Artikel 63.3 EHDS.*

[265] *Artikel 63.4 EHDS.*

6.2.6.6 Slotoverwegingen

Rekening houdend met de opgesomde doeleinden zal de Vlaamse Health Data Space zonder twijfel secundair gebruik beogen conform de EHDS-verordening; het verbeteren van de zorgverlening, het in kaart brengen van trends en preventieve gezondheidszorg stimuleren. Ook de Data4PHM use case in het bijzonder valt hier zeker onder. De volwaardige uitwerking van een gegevensruimte zoals beoogd in de EHDS-verordening vereist echter ook de uitwerking van het luik rond primair gegevensgebruik. Dit aspect vereist nog verder onderzoek, ook op technisch en governance vlak.

De implementatie van de EHDS-verordening binnen de Vlaamse context biedt kansen, maar legt ook een aantal structurele tekortkomingen en uitdagingen bloot. De verordening dient nog verder geïmplementeerd te worden door nationale wetgeving, bijvoorbeeld om eventuele uitzonderingen op het recht op opt-out te concretiseren. Dit zal ook voor het huidige project belangrijk zijn om volledig te begrijpen hoe de EHDS geïmplementeerd moet worden in België, maar op moment van het schrijven zijn de intenties van de (Belgische) wetgever nog niet bekend. De **implementatiewetgeving** kan zo immers concreet de werkingssfeer van de Health Data Space beïnvloeden.

Daarnaast is ook het aanwijzen van een **HDAB** interessante materie.[266] Zoals uit hierboven blijkt, heeft het HDAB een veelheid aan bevoegdheden. Wie deze instantie moet zijn en of deze reeds kan worden opgericht in het kader van het huidige project is een interessante vraag. Het is bovendien mogelijk dat er meerdere HDAB's worden aangeduid. Indien dit het geval is, zal er echter ook een coördinerende HDAB moeten zijn. Dit kadert natuurlijk ook samen in het overkoepelende debat over de geografische afbakening van het huidige project. Indien er één grote federale health data space wordt beoogd, kunnen er misschien wel per gemeenschap HDAB's worden aangewezen. Het zal interessant zijn om te kijken welke entiteit deze bevoegdheden op zich neemt en of in het huidige Health Data Space-project al een instantie kan worden opgericht die aan de wettelijke vereisten zoals vooropgesteld in de EHDS tegemoet komt.

Ten slotte, zijn er nog een aantal bemerkingen ten aanzien van de EHDS-verordening:

> Zo is een opvallende leemte in de huidige verordening het gebrek aan specifieke aandacht voor gezondheidsgegevens van kinderen. De verwerking van **gegevens van minderjarigen** vereist extra waarborgen vanwege hun verhoogde kwetsbaarheid. Het ontbreken van duidelijke richtlijnen hierover in de EHDS-verordening roept vragen op over hoe de Health Data Space dergelijke bescherming kan integreren in haar werking en of er überhaupt differentiatie moet worden gemaakt?

> Zoals reeds aangehaald in 6.2.4.1 Relevante definities, is de juridische definitie van **geanonimiseerde gegevens** niet de meest duidelijke. De verordening biedt op dit ogenblik onvoldoende duidelijkheid over de eisen rondom anonimisering, met name voor genetische gegevens. Voor deze categorie van gegevens is volledige anonimisering vaak technisch onhaalbaar door hun inherente unieke karakter. Nu de tekst finaal is, kan dit gezien worden als een gemiste kans om hierover meer duidelijkheid te verschaffen.

> Een ander knelpunt betreft **de implementatie van het opt-outmechanisme**. De EHDS-verordening vereist dat lidstaten duidelijkheid verschaffen over hoe en op welk niveau dit mechanisme toegepast moet worden. Dit roept vragen op over de verantwoordelijkheid van Vlaamse instellingen en hoe dit mechanisme kan worden geïntegreerd zonder de kernprincipes van gegevensbescherming te ondermijnen.

> De **interactie tussen de EHDS en de DGA blijft onduidelijk**, met name met betrekking tot DISPs die in het kader van de DGA zijn opgericht. Het is essentieel om te verduidelijken hoe deze entiteiten zich verhouden tot de Health Data Space, om conflicten in regelgeving te vermijden.

[266] *Artikel 55 EHDS.*

6.2.7 Dataverordening

6.2.7.1 Inleiding

De Dataverordening[267], die op 11 januari 2024 in werking is getreden, vormt een belangrijke mijlpaal in de regulering van gegevensbeheer binnen de Europese Unie. Deze wetgeving is van toepassing op **zowel persoonlijke als niet-persoonlijke gegevens** en definieert gegevens in brede zin als "*elke digitale weergave van handelingen, feiten of informatie en elke compilatie van dergelijke handelingen, feiten of informatie, ook in de vorm van geluids-, visuele of audiovisuele opnames*."[268] Afgeleide informatie van deze gegevens moet worden uitgesloten van het toepassingsgebied.

De Dataverordening is ontworpen om duidelijkheid te scheppen over wie waarde kan creëren uit data. Dit wordt bereikt door het vaststellen van regels voor het gebruik van gegevens die worden gegenereerd door *Internet-of-Things*-apparaten. Daarnaast bevat de wetgeving maatregelen om misbruik van contractuele ongelijkheden bij het delen van gegevens te beperken.

Een ander belangrijk aspect is de mogelijkheid voor overheidsinstanties om toegang te krijgen tot gegevens die worden beheerd door private entiteiten, mits dit gebeurt voor specifieke doeleinden van algemeen belang. Tot slot bevordert de Dataverordening de interoperabiliteit door nieuwe regels in te voeren die klanten in staat stellen naadloos over te schakelen tussen verschillende data-verwerkingsdienstverleners.

Kortom, de verordening voorziet in drie soorten van gegevensdeling:

1. Informatie over het verbonden product of de gerelateerde dienst aan de gebruiker hiervan (business to consumer);
2. Informatie van de houders van gegevens aan de ontvangers van gegevens (business to business);
3. Informatie van houders van gegevens aan publieke sector lichamen wanneer er zich een situatie van uitzonderlijke noodzaak voordoet (business to government).[269]

Hoewel zowel de DGA als de Dataverordening zich richten op gegevensbeheer, hebben ze een verschillend doel. De DGA faciliteert vrijwillige gegevensdeling door middel van mechanismen zoals gegevens-bemiddelingsdiensten, terwijl de Dataverordening zich richt op toegangsrechten en verplichtingen voor gegevenshouders, met name binnen een commerciële omgeving.

6.2.7.2 Relevante definities en toepassingsgebied

De Dataverordening richt zich op een breed scala aan actoren binnen de EU, waaronder:

- **Aanbieders/fabrikanten van verbonden producten en gerelateerde diensten** die op de EU-markt worden aangeboden, evenals gebruikers van dergelijke verbonden producten of diensten;
- **Gegevenshouders** die gegevens beschikbaar stellen aan ontvangers binnen de EU;[270]
- **Gegevensontvangers** in de EU die deze gegevens ontvangen;[271]

---

[267] *Verordening (EU) 2023/2864 van het Europees Parlement en de Raad betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data en tot wijziging van Verordening (EU) 2017/3294 en Richtlijn (EU) 2020/1828 van 13 december 2023 (hierna: Dataverordening).*

[268] *Artikel 2, lid 1, Dataverordening.*

[269] *Biasin, E. (19 mei 2022). The Data Act will concern eHealth apps and Medical Devices. CiTiP Blog.*

[270] *Artikel 2, lid 13, Dataverordening definieert een gegevenshouders als "een natuurlijke persoon of rechtspersoon die overeenkomstig deze verordening, het toepasselijke Unierecht of het overeenkomstig het Unierecht vastgestelde nationale recht, het recht of de verplichting heeft gegevens te gebruiken en ter beschikking te stellen, waaronder — in gevallen waar dat contractueel is overeengekomen — productgegevens of gegevens van een gerelateerde dienst die deze natuurlijke of rechtspersoon heeft opgevraagd of gegenereerd tijdens de verlening van een gerelateerde dienst.".*

[271] *Artikel 2, lid 14, Dataverordening definieert een gegevensontvanger als "een natuurlijke of rechtspersoon die handelt voor doeleinden die verband houden met diens handels-, bedrijfs-, ambachts- of beroepsactiviteit, die niet de gebruiker van een verbonden product of gerelateerde dienst is en aan wie gegevens beschikbaar worden gesteld door de gegevenshouder, met inbegrip van een derde op verzoek van de gebruiker aan de*

- **Overheidsinstanties en EU-instellingen**, agentschappen of organen die toegang vragen tot gegevens wanneer er een uitzonderlijke behoefte[272] is in het kader van een publieke taak;[273]
- **Leveranciers van dataverwerkingsdiensten**[274] die dergelijke diensten aanbieden aan klanten in de EU.

Een **verbonden product** refereert naar een goed dat gegevens over het gebruik of de omgeving ervan verkrijgt, genereert of verzamelt, en dat productgegevens kan doorgeven via een elektronische communicatiedienst, fysieke verbinding of apparaattoegang, en waarvan de hoofdfunctie niet het opslaan, verwerken of doorgeven van gegevens namens anderen dan de gebruiker is.[275] Dergelijke verbonden producten komen hoe langer hoe meer voor in de samenleving en kunnen ook relevante gezondheidsgegevens genereren. Een voorbeeld is een sporthorloge of medische meetapparatuur. Het is waarschijnlijk dat op termijn ook dergelijke gegevens in een health data space terecht komen.

Gerelateerde diensten zijn andere digitale diensten dan een elektronische communicatiedienst, waaronder software, die op het moment van aankoop, huur of lease zodanig met het product verbonden zijn, dat de afwezigheid ervan het verbonden product zou beletten een of meer van zijn functies uit te voeren, of die vervolgens door de fabrikant of een derde met het product worden verbonden om functies aan het product toe te voegen, of de functies van het verbonden product te updaten of aan te passen.[276] Deze gerelateerde diensten zijn bijvoorbeeld via een applicatie (bijkomende) data kunnen raadplegen die door het product gegenereerd zijn.

De **gebruiker** is de natuurlijke persoon of rechtspersoon die een verbonden product in eigendom heeft, of aan wie contractueel tijdelijke rechten zijn overgedragen om dat verbonden product te gebruiken, of die gerelateerde diensten ontvangt.[277] Het lijkt erop dat dit patiënten kunnen zijn die gebruik maken van bepaalde medische apparatuur, bijvoorbeeld bij hen thuis, maar ook artsen die deze tijdens de behandeling van een patiënt gebruiken. Het is met andere woorden mogelijk dat een gebruiker onder de Dataverordening overlapt met entiteiten in de Health Data Space.

gegevenshouder of in overeenstemming met een wettelijke verplichting uit hoofde van Unierecht of overeenkomstig het Unierecht vastgestelde nationale wetgeving."

[272] Dit is in het geval er zich een "algemene noodsituatie" voordoet, wat in artikel 2, lid 29, Dataverordening wordt omschreven als "een in de tijd beperkte uitzonderlijke situatie, zoals een noodsituatie op het gebied van de volksgezondheid, een noodsituatie die voortvloeit uit natuurrampen, of een door de mens veroorzaakte grote ramp, met inbegrip van een groot cyberveiligheidsincident, dat negatieve gevolgen heeft voor de bevolking van de Unie, van een lidstaat of van een deel daarvan, met een risico op ernstige en blijvende gevolgen voor de levensomstandigheden of de economische stabiliteit, de financiële stabiliteit of een aanzienlijke en onmiddellijke verslechtering van de economische activa in de Unie of in de betrokken lidstaat, en die wordt vastgesteld of officieel wordt afgekondigd overeenkomstig de relevante Unie- of nationaalrechtelijke procedures."

[273] Artikel 2, lid 27, Dataverordening definieert organen van de Unie als "instellingen, organen en instanties van de Unie die zijn opgericht bij of op grond van handelingen die zijn vastgesteld op basis van het Verdrag betreffende de Europese Unie, het VWEU of het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie;" en artikel 2, lid 28, Dataverordening definieert overheidsinstantie als "nationale, regionale en lokale autoriteiten van de lidstaten, publiekrechtelijke instellingen van de lidstaten of samenwerkingsverbanden bestaande uit één of meer van dergelijke autoriteiten of één of meer van dergelijke instellingen."

[274] Artikel 2, lid 8, Dataverordening definieert een dataverwerkingsdienst als "een digitale aan een klant aangeboden dienst die alomtegenwoordige en on-demand netwerktoegang mogelijk maakt tot een gedeelde pool van configureerbare, schaalbare en elastische computer capaciteit van gecentraliseerde, gedistribueerde of sterk gedistribueerde aard, die snel ter beschikking kan worden gesteld en worden vrijgegeven met minimale beheersinspanningen of tussenkomst van een dienstverlener."

[275] Artikel 2, lid 5, Dataverordening.

[276] Artikel 2, lid 6, Dataverordening.

[277] Artikel 2, lid 12, Dataverordening.

6.2.7.3 Situatie van uitzonderlijke noodzaak

Hoofdstuk V omschrijft de verplichting tot gegevensdeling aan overheidsinstanties, de Commissie, de Europese Centrale Bank en organen van de Unie op grond van uitzonderlijke noodzaak.
Zo een situatie kan zich voordoen:

a) Indien de gevraagde gegevens noodzakelijk zijn om te reageren op een algemene noodsituatie en de overheidsinstanties, de Commissie, de Europese Centrale Bank of het orgaan van de Unie niet in staat is dergelijke gegevens tijdig en doeltreffend op een andere manier en in gelijkwaardige omstandigheden te verkrijgen;

b) In niet onder punt a) vallende omstandigheden en uitsluitend voor niet-persoonsgebonden gegevens, indien:
   - een overheidsinstantie, de Commissie, de Europese Centrale Bank of een orgaan van de Unie handelt op grond van het Unie- of nationale recht en specifieke gegevens heeft geïdentificeerd waarvan het ontbreken haar/het ervan weerhoudt een bij wet opgelegde specifieke taak van algemeen belang te vervullen, zoals het opstellen van officiële statistieken of beperking van of herstel na een algemene noodsituatie, en
   - de overheidsinstantie, de Commissie, de Europese Centrale Bank of het orgaan van de Unie alle andere middelen waarover zij/het beschikt om dergelijke gegevens te verkrijgen heeft uitgeput, met inbegrip van de aankoop van de gegevens op de markt door markttarieven aan te bieden of door gebruik te maken van bestaande verplichtingen om gegevens beschikbaar te stellen of de vaststelling van nieuwe wetgevingsmaatregelen die de tijdige beschikbaarheid van de gegevens kunnen waarborgen.[278]

Micro- en kleine ondernemingen worden vrijgesteld van deze verplichting.[279]

6.2.7.4 Slotoverwegingen

De Dataverordening is een horizontaal kader dat van toepassing is op alle sectoren, inclusief de gezondheidszorg.[280] Hoewel de verordening duidelijke regels biedt voor gegevensbeheer en -deling, blijven er op een aantal punten onduidelijkheden bestaan met betrekking tot de uitvoering, vooral in de context van gezondheidsgegevens en medische apparatuur.

> In de gezondheidssector richt de Dataverordening zich vooral op de rechten en verplichtingen van gebruikers en houders van medische en gezondheidsgerelateerde apparaten.[281] Dit heeft enkele belangrijke implicaties:
   - **Uitgebreide rechten voor gebruikers/patiënten**: gebruikers van medische apparaten hebben recht op toegang tot en het delen van zowel persoonlijke als niet-persoonlijke gegevens. Deze rechten gaan verder dan de rechten die worden geboden onder de AVG, waarmee een nieuwe dimensie aan patiëntengegevensbeheer wordt toegevoegd.

[278] *Artikel 15, lid 1, Dataverordening.*

[279] *Artikel 15, lid 2, Dataverordening.*

[280] *Overweging 14 Dataverordening benadrukt dat verbonden producten in alle onderdelen van de economie en de samenleving te vinden zijn, waaronder particuliere, civiele of commerciële infrastructuur, voertuigen, gezondheids- en lifestyleapparatuur, schepen, vliegtuigen, huishoudelijke apparatuur en consumptiegoederen, medische en gezondheidsapparatuur of landbouw- en industriële machines.*

[281] *Zie overweging 14 Dataverordening.*

> In principe vallen **afgeleide gegevens** niet onder het toepassingsgebied van de Dataverordening.[282] In werkelijkheid is niet altijd goed te onderscheiden tussen gegenereerde gegevens, die wel door de Dataverordening worden gevat, en meer afgeleide gegevens. Het is niet glashelder waar het verschil precies ligt tussen louter gegenereerde gegevens en gegevens die reeds een bewerking/transformatie hebben ondergaan en daardoor afgeleide gegevens zijn, die dan eventueel zelfs beschermd kunnen worden door het intellectuele eigendomsrecht.

> De rolverdeling blijkt niet altijd even duidelijk te zijn; wie wordt gedefinieerd als de houder van de gegevens afkomstig van medische apparatuur? Is dit de gezondheidsbeoefenaar bijvoorbeeld, en zijn de fabrikanten van medische apparatuur de houders van gezondheidsgegevens betreffende patiënten? Een gelijkaardige onduidelijkheid doet zich voor rond het begrip 'gebruiker', waar dit afhankelijk van het gehanteerde perspectief de patiënt kan zijn, maar soms ook een ziekenfonds (bv. wanneer een bepaald apparaat aan de patiënt wordt verschaft via het ziekenfonds dat het apparaat uitleent). Afhankelijk van de omstandigheden, kunnen **de rollen (en verantwoordelijkheden)** variëren onder de Dataverordening. In een gezondheidscontext blijkt niet glashelder te zijn wie onder welke hoedanigheid valt.
    - Hier komt bij dat de **begrippen van de AVG niet altijd duidelijk toepasbaar zijn op de actoren** van de Dataverordening. De termen gegevenshouder en gegevensgebruiker in de Dataverordening verschillen van de begrippen "verwerkingsverantwoordelijke," "verwerker" en "betrokkene" in de AVG. Hoewel een gegevensgebruiker in sommige gevallen overeen kan komen met een "betrokkene" (bijvoorbeeld een patiënt die een medisch apparaat gebruikt), is dit niet altijd het geval. Dit kan verwarring veroorzaken bij de toepassing van beide verordeningen.

> **Verplichting tot gegevensdeling bij uitzonderlijke nood**: bij publieke noodsituaties, zoals gezondheidscrises of grote natuurrampen, moeten gegevens gratis beschikbaar worden gesteld aan overheidsinstanties. Deze verplichting, vastgelegd in Hoofdstuk V van de Dataverordening, roept vragen op over hoe deze gegevensdeling praktisch en juridisch wordt geïmplementeerd in de gezondheidszorg. In het bijzonder wanneer het gaat om sensitieve gezondheidsgegevens, moet omzichtig worden omgesprongen met een dergelijke overdracht van gegevens.

Hoewel de Dataverordening een krachtig instrument is voor het bevorderen van datatoegang en innovatie in de gezondheidszorg, blijven er vragen bestaan over de praktische uitvoering en interactie met bestaande regelgevingen zoals de AVG. Voor een effectieve toepassing is verdere verduidelijking nodig, zowel op juridisch als operationeel vlak. Dit is essentieel om te voorkomen dat de overlappende kaders leiden tot verwarring of inefficiënties in de omgang met gezondheidsgegevens.

Het is belangrijk te benadrukken dat in het kader van de Health Data Space de complexiteit van de Dataverordening minder speelt. Dit komt doordat in deze fase van het project er nog niet gekeken werd om het toepassingsveld van de Dataverordening te incorporeren in de Health Data Space, al kan dit uiteraard in de toekomst veranderen. Voor secundair gebruik is de regel momenteel ook dat - zoveel als mogelijk - de gegevens die gebruikt worden, volledig geanonimiseerd zijn en specifiek worden ingezet voor onderzoeks-doeleinden. Hiervoor vallen veel van de specifieke rechten en verplichtingen van de Dataverordening, zoals die met betrekking tot persoonlijke gegevens, buiten beschouwing.

Binnen de Health Data Space kunnen (op termijn) actoren zoals leveranciers van dataverwerkingsdiensten een belangrijke rol spelen in de context van de Dataverordening. Bijvoorbeeld:

> Dataproviders: leveranciers van dataverwerkingsdiensten kunnen fungeren als dataproviders binnen de Health Data Space. Ze maken geanonimiseerde gegevens beschikbaar voor secundair gebruik, zoals wetenschappelijk onderzoek of populatiebeheer, binnen de kaders van de Dataverordening.

[282] *Zie bijvoorbeeld overweging 15 Dataverordening.*

> Toepasselijkheid van de wetgeving: hoewel de Health Data Space-participanten onder de Dataverordening kunnen vallen, richt de wetgeving zich vooral op hun specifieke activiteiten en verantwoordelijkheden, en niet op de Health Data Space zelf. Dit betekent dat de Health Data Space *an sich* niet rechtstreeks wordt beïnvloed door de verplichtingen van de Dataverordening.

De Dataverordening heeft dus vooral betrekking op de actoren binnen de data-infrastructuur en minder op de structuur of het functioneren van de Health Data Space als geheel. Wel kan nagedacht worden of de Health Data Space op termijn de gegevensstromen die ontstaan in het kader van de Dataverordening kan faciliteren, door bijvoorbeeld toegang tot haar infrastructuur te verlenen in het geval van een uitzonderlijke noodzaak.[283]

6.2.8 Richtlijn inzake open data en het hergebruik van overheidsinformatie

De richtlijn inzake open data en het hergebruik van overheidsinformatie (PSI)[284] is sinds juli 2018 van kracht en vereist verdere implementatie door de lidstaten. De omzetting in nationale wetgeving moest uiterlijk op 16 juli 2021 voltooid zijn. Deze richtlijn is een essentieel instrument om de interne markt te versterken en is opgebouwd rond twee kernprincipes: **transparantie** en **eerlijke concurrentie**.

De richtlijn beoogt het stimuleren van innovatie en economische groei door het hergebruik[285] van overheidsinformatie eenvoudiger te maken. De belangrijkste bepalingen omvatten:

> Het stimuleren van publicatie van dynamische gegevens[286] en gebruik van API's[287];
  - Overheidsinstanties worden aangemoedigd om dynamische gegevens (realtime gegevens)[288] beschikbaar te maken en het gebruik van Application Programming Interfaces (API's) te ondersteunen. Dit vergemakkelijkt de toegang tot een integratie van gegevens in nieuwe toepassingen en diensten.

> Een beperking van kosten voor hergebruik;
  - Overheidsinstanties mogen geen kosten in rekening brengen voor het hergebruik van gegevens, behalve de marginale kosten voor verspreiding.[289] Dit beperkt uitzonderingen die voorheen werden toegestaan, wat de toegankelijkheid van overheidsinformatie vergroot.

> Een uitbreiding van het toepassingsgebied;
  - Gegevens van overheidsbedrijven: de richtlijn is van toepassing op gegevens in het bezit van overheidsbedrijven, met een specifieke reeks regels. Dit geldt uitsluitend voor gegevens die deze bedrijven beschikbaar stellen voor hergebruik (zij zijn hier niet toe verplicht in hoofde van de PSI[290]).

---

[283] *Artikel 15 Dataverordening.*

[284] *Richtlijn (EU) 2019/1024 inzake open data en het hergebruik van overheidsinformatie van 20 juni 2019 (hierna: PSI).*

[285] *De term hergebruik wordt gedefinieerd in artikel 2, 11) PSI als "het gebruik door natuurlijke personen of rechtspersonen van documenten die in het bezit zijn van: a) openbare lichamen voor andere commerciële of niet-commerciële doeleinden dan het oorspronkelijk doel binnen de publieke taak waarvoor de documenten zijn geproduceerd, met uitzondering van de uitwisseling van documenten tussen openbare lichamen uitsluitend met het oog op de vervulling van hun openbare taken, of; b) overheidsondernemingen voor andere commerciële of niet-commerciële doeleinden dan het oorspronkelijke doel van dienstverlening in het algemeen belang waarvoor de documenten zijn geproduceerd, met uitzondering van de uitwisseling van documenten tussen overheidsondernemingen en openbare lichamen uitsluitend met het oog op de vervulling van de openbare taken van openbare lichamen."*

[286] *Overweging 31 en artikel 5(5) PSI.*

[287] *Overweging 32 en artikel 5(5) PSI.*

[288] *'Dynamische gegevens' wordt in artikel 2, 8) PSI gedefinieerd als: "documenten in digitale vorm die frequent of in real time worden geactualiseerd, met name wegens hun volatiliteit of omdat ze snel verouderd zijn; gegevens die door sensoren zijn gegenereerd, worden doorgaans als dynamische gegevens beschouwd."*

[289] *Overweging 36 en artikel 6(1), tweede lid, PSI.*

[290] *Overweging 26 PSI.*

- Onderzoeksgegevens[291] die voortkomen uit overheidsfinanciering vallen ook onder de richtlijn. Lidstaten worden aangemoedigd om beleid te ontwikkelen voor **open toegang** tot door de overheid gefinancierde onderzoeksgegevens. Dit omvat ook het vergemakkelijken van hergebruik van gegevens die al zijn opgenomen in open repositories.

> Transparantie en exclusieve regelingen: de richtlijn versterkt de transparantievereisten bij publiek-private overeenkomsten waarbij overheidsinformatie betrokken is. Het gebruik van exclusieve regelingen, die toegang tot bepaalde informatie beperken, wordt verder beperkt om eerlijke concurrentie te waarborgen.

In artikel 10 wordt uiteengezet dat de lidstaten de beschikbaarheid van onderzoeksgegevens ondersteunen middels nationale beleidsmaatregelen en relevante acties om met overheidsmiddelen gefinancierde[292] onderzoeksgegevens beschikbaar te stellen ("**openaccessbeleid**"[293]). Dit dient te verlopen in overeenstemming met de "open door standaardinstellingen" ("**open by default**") en de FAIR-beginselen (zie sectie 6.2.8 Richtlijn inzake open data en het hergebruik van overheidsinformatie).[294] In dat verband worden problemen met betrekking tot intellectuele eigendomsrechten, bescherming en vertrouwelijkheid van persoonsgegevens, beveiliging en rechtmatige handelsbelangen in aanmerking genomen in overeenstemming met het beginsel "zo open als mogelijk, zo gesloten als nodig".

Onderzoeksgegevens zijn bovendien herbruikbaar voor commerciële of niet-commerciële doeleinden, voor zover die gegevens met overheidsmiddelen zijn gefinancierd en onderzoekers, onderzoeksinstellingen of organisaties die onderzoek financieren ze al openbaar hebben gemaakt via een institutionele of thematische databank.[295] In dat verband moet rekening worden gehouden met rechtmatige handelsbelangen, activiteiten inzake kennisoverdracht en reeds bestaande intellectuele eigendomsrechten.

Hier komt bovenop dat Hoofdstuk II van de DGA voorwaarden stelt aan het hergebruik van publieke data, d.w.z. de data gehouden door openbare lichamen in de publieke sector die beschermd zijn op basis van (i) commerciële confidentialiteit, (ii) statistische confidentialiteit, (iii) intellectuele eigendomsrechten, of (iv) het gegevensbeschermingsrecht in zoverre dit buiten het toepassingsgebied van de PSI valt. Normaliter zijn deze gegevens niet publiek toegankelijk en daarom ook niet vatbaar voor hergebruik op basis van de PSI.[296]

Hoewel de richtlijn voornamelijk gericht is op overheidsinstanties, ontstaan er uitdagingen bij de toepassing op onderzoek, vooral door de mix van nationale en Europese wetgevingen die daarop van toepassing zijn. Daarnaast is de richtlijn van toepassing op informatie die reeds "**publiek toegankelijk**" is, maar er gelden strike beperkingen op intellectuele eigendomsrechten. Deze beperkingen omvatten:

> Een verbod op het uitoefenen van het ***sui generis-recht*** op databanken door publieke instellingen (zie 6.2.10.2 Het sui generis-recht van toepassing op databanken);

> Beperkingen op auteursrechten en andere intellectuele eigendomsrechten om hergebruik van gegevens te waarborgen.

---

[291] De term "onderzoeksgegevens" wordt in artikel 2(9) PSI gedefinieerd als "andere documenten in digitale vorm dan wetenschappelijke publicaties, die worden verzameld of geproduceerd tijdens wetenschappelijke onderzoeksactiviteiten en die als bewijs in het onderzoeksproces worden gebruikt, of waarvan binnen de onderzoeksgemeenschap algemeen wordt erkend dat ze noodzakelijk zijn om onderzoeksresultaten te valideren." In de Wet van 4 mei 2016 inzake open data en het hergebruik van overheidsinformatie wordt hier in artikel 2, 14° aan toegevoegd dat om als onderzoeksgegevens te kwalificeren de gegevens minstens voor de helft moten zijn gefinancierd met overheidsmiddelen en deze reeds openbaar zijn gemaakt via een institutionele of thematische databank.

[292] Deze onderzoeken kunnen al dan niet mede gefinancierd zijn door entiteiten uit de particuliere sector (zie overweging 28 PSI).

[293] Overweging 27 PSI bepaalt het volgende: "Openaccessbeleid heeft met name tot doel onderzoekers en het grote publiek zo vroeg mogelijk in het verspreidingsproces toegang te verschaffen tot onderzoeksgegevens en het gebruik en hergebruik daarvan te vergemakkelijken. Open access draagt bij tot een betere kwaliteit, tot het beperken van de behoefte aan duplicatie van onderzoek, tot snellere wetenschappelijke vooruitgang en tot de strijd tegen wetenschappelijk bedrog, en komt in het algemeen de economische groei en innovatie te goede."

[294] Zie ook artikel II.62/1 Bestuursdecreet van 7 december 2018.

[295] Artikel 10(2) PSI.

[296] Zie overweging 7 DGA.

De richtlijn heeft als doel een opentoegangsbeleid te bevorderen binnen de lidstaten, met name voor onderzoeksgegevens. Dit beleid draagt bij aan:

> Het stimuleren van innovatie door bredere toegang tot overheidsinformatie;
> Het vergroten van de transparantie van overheidsactiviteiten;
> Het bevorderen van eerlijke concurrentie door exclusieve regelingen te minimaliseren.

Een belangrijk onderdeel van de richtlijn betreft de identificatie en beschikbaarstelling van **hoogwaardige datasets**[297]. Dit zijn datasets die vanwege hun economische en maatschappelijke waarde bijzondere aandacht krijgen en breed beschikbaar moeten zijn. Een uitvoeringsverordening vanaf 2023 definieert een lijst van hoogwaardige gegevensreeksen binnen zes thematische categorieën. Deze datasets zijn in het bezit van openbare lichamen en overheidsbedrijven en vallen onder de documenten waarop de richtlijn van toepassing is. De zes categorieën zijn:[298]

- Geospatiaal, bv. geografische kaarten, kadastergegevens of informatie over administratieve grenzen;
- Aardobservatie en milieu, bv. informatie over natuurlijke hulpbronnen, luchtkwaliteit of klimaatverandering;
- Meteorologisch, bv. weersvoorspellingen of historische weersgegevens;
- Statistieken, bv. bevolkingscijfers, economische gegevens;
- Bedrijven en bedrijfseigendom, bv. informatie over bedrijfsregistraties, eigendomsstructuren en faillissementen;
- Mobiliteit, bv. data over verkeersstromen, openbaar vervoer en logistieke netwerking.

6.2.8.1 Nationale implementatie

De omzetting van de richtlijn in België verloopt via verschillende kanalen en maatregelen:[299]

> Federaal
  - Wet inzake het hergebruik van overheidsinformatie van 4 mei 2016.
  - KB tot bepaling van de behandelingsprocedure en -termijnen voor een aanvraag voor hergebruik van overheidsinformatie alsook het toezicht op de verplichting om bestuursdocumenten beschikbaar te stellen van 29 oktober 2007.
  - KB betreffende de samenstelling en werkwijze van de Commissie voor de toegang tot en het hergebruik van bestuursdocumenten van 29 april 2008.

> Vlaams
  - Bestuursdecreet van 7 december 2018.
  - Besluit van de Vlaamse Regering betreffende het hergebruik van overheidsinformatie bij de diverse departementen binnen de Vlaamse ministeries en bij de intern verzelfstandigde agentschappen zonder rechtspersoonlijkheid van 19 juli 2007.
  - Besluit van de Vlaamse Regering tot oprichting van de beroepsinstantie inzake openbaarheid van bestuur en het hergebruik van overheidsinformatie van 19 juli 2007.
  - Ministerieel besluit met betrekking tot vastlegging van de modellicentie inzake hergebruik van overheidsinformatie van 8 oktober 2007.

> Beroepsinstantie inzake openbaarheid van bestuur en hergebruik van overheidsinformatie. Afdeling hergebruik van overheidsinformatie van 8 oktober 2007.

---

[297] Dit begrip wordt in artikel 2, 10) PSI gedefinieerd als "documenten waarvan het hergebruik belangrijke voordelen biedt voor de samenleving, het milieu en de economie, met name vanwege hun geschiktheid voor het ontwikkelen van diensten met toegevoegde waarde en van toepassingen, en voor het scheppen van nieuwe, hoogwaardige en fatsoenlijke banen, en vanwege het aantal potentiële begunstigden van op basis van die datasets ontwikkelde diensten of toepassingen met toegevoegde waarde."

[298] Overweging 66 en Bijlage I PSI.

[299] Europese Commissie. (12 december 2012). Implementation of the PSI Directive in Belgium.

De richtlijn is van toepassing op onderzoeksgegevens op grond van de voorwaarden van artikel 10.[300] **Dit dient kosteloos te kunnen gebeuren.**[301] Andere documenten van onderzoeksinstellingen en organisaties die onderzoek financieren vallen hier niet onder, inclusief documenten van organisaties die zijn opgericht voor de overdracht van onderzoeksresultaten.[302]

Zoals besproken in sectie 6.2.7 Dataverordening behandelt de richtlijn inzake open data meerdere aspecten. **Een van de belangrijkste bepalingen in de context van de Health Data Space is de verplichting tot hergebruik van onderzoeksgegevens.** Deze verplichting geldt voor gegevens die voortkomen uit onderzoeken die grotendeels door de overheid worden gefinancierd. Het is echter belangrijk op te merken dat deze verplichting specifiek rust op de *data consumers*, en niet zozeer op de Health Data Space zelf. Het is uiteraard wel mogelijk om bij de opzet van een Health Data Space rekening te houden met de verplichtingen die voortspruiten uit de PSI.

6.2.9 Verordening betreffende een kader voor het vrije verkeer van niet-persoonsgebonden gegevens

Als onderdeel van de EU-strategie voor de digitale eengemaakte markt moet een vrij verkeer van gegevens in de hele EU tot stand worden gebracht om de opslag, verwerking en (grensoverschrijdende) uitwisseling van niet-persoonsgebonden gegevens door zowel industriële belanghebbenden als overheidsinstanties te vergemakkelijken. Verschillende obstakels hebben de mobiliteit van gegevens binnen de EU echter belemmerd. De Europese Commissie heeft met name vier uitdagingen voor het vrije verkeer van gegevens vastgesteld, namelijk de uitvoering van gegevenslokalisatiebeperkingen die door overheidsinstanties op nationaal niveau zijn omgezet (1), belemmeringen voor het verkeer van gegevens tussen IT-systemen (2), rechtsonzekerheid als gevolg van een complex lappendeken van EU-wetgeving (3) en het gebrek aan vertrouwen dat wordt gecreëerd door veiligheidsrisico's die gepaard gaan met grensoverschrijdende gegevensuitwisseling (4).[303]

In dit verband heeft de EU-wetgever de verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens (FFNPDR)[304] in de EU omgezet. De verordening is in mei 2019 in werking getreden en is sindsdien rechtstreeks van toepassing in alle EU-lidstaten. Het vormt een aanvulling op de AVG in die zin dat de FFNPDR van toepassing is op de verwerking van elektronische **niet-persoonsgebonden gegevens**[305], dus andere gegevens dan persoonsgegevens zoals gereguleerd in het EU-kader voor gegevensbescherming. Door dit samen te doen, creëren zij een alomvattend kader voor het vrije verkeer van persoonsgebonden en niet-persoonsgebonden gegevens, en bevorderen zij zo de omzetting van een Europese gegevensruimte.

Op basis van de FFNDR kunnen niet-persoonlijke gegevens zonder beperkingen in de hele EU worden opgeslagen en gebruikt. Het rechtskader van de FFNDPR omvat met name de volgende kenmerken in overeenstemming met de bestaande bepalingen die van toepassing zijn op het vrije verkeer en de overdraagbaarheid van persoonsgegevens:

[300] *Artikel 1(1)(c) PSI.*

[301] *Artikel 6(6)(b) PSI en artikel II.62/2 Bestuursdecreet 7 december 2018.*

[302] *Artikel 1(2)(l) PSI.*

[303] *Europese Commissie. (19 september 2017). Digital Single Market. Free Flow of non-personal data.*

[304] *Verordening (EU) 2018/1807 van het Europees Parlement en de Raad betreffende een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie van 14 november 2018 (hierna: FFNPDR).*

[305] *Zie artikel 3, lid 1, van de FFNPDR.*

- De FFNPDR creëert een kader dat de lidstaten verhindert gegevenslokalisatiebeperkingen in te voeren om het vrije verkeer van gegevens over de grenzen heen te waarborgen. Als EU-lidstaten bestaande beperkingen hebben of van plan zijn deze in te voeren, zijn zij verplicht deze aan de Commissie mee te delen;
- Het kader zorgt ervoor dat gegevens beschikbaar zijn voor regelgevend toezicht en de uitvoering van hun taken, zodat overheidsinstanties toegang tot gegevens kunnen behouden voor toezichtsdoeleinden;
- De verordening bevordert de ontwikkeling van gedragscodes voor clouddiensten ter ondersteuning van de verandering van aanbieder van clouddiensten voor professionele gebruikers.[306]

De niet-persoonsgebonden gegevens kunnen naar oorsprong worden gecategoriseerd als:

- Ten eerste; gegevens die oorspronkelijk geen betrekking hadden op een geïdentificeerde of identificeerbare natuurlijke persoon, zoals gegevens over weersomstandigheden die worden gegenereerd door sensoren die op windturbines zijn geïnstalleerd of gegevens over onderhoudsbehoeften voor industriële machines;
- Ten tweede; **gegevens die in eerste instantie persoonsgegevens waren, maar later geanonimiseerd zijn.** Het 'anonimiseren' van persoonsgegevens is iets anders dan pseudonimiseren, aangezien goed geanonimiseerde gegevens niet aan een specifieke persoon kunnen worden toegeschreven, ook niet door het gebruik van aanvullende gegevens en dus niet-persoonsgebonden gegevens zijn.[307]

Tegen deze achtergrond heeft de wetgever richtsnoeren gegeven voor **het gebruik van gemengde datasets**.[308] Gemengde datasets omvatten persoonlijke, zoals gegevens over gezondheid, en niet-persoonlijke gegevens, zoals anonieme of geaggregeerde gegevens. Het onderverdelen van beide gegevenstypen die in één dataset zijn opgeslagen (bijvoorbeeld in elektronische medische dossiers) kan soms moeilijk zijn en verwarring scheppen op het gebied van de toepasselijke wetgeving. De FFNPDR beschouwt use cases als deze en verduidelijkt dit:

- Als een dataset persoonsgegevens en niet-persoonsgebonden gegevens bevat, is de FFNPDR van toepassing op het deel van de dataset dat niet-persoonsgebonden gegevens bevat en is de AVG van toepassing op het persoonsgegevensgedeelte van de dataset op voorwaarde dat zowel niet-persoonsgebonden gegevens als persoonsgegevens niet onlosmakelijk met elkaar verbonden zijn;
- Als beide soorten gegevens (d.w.z. persoonsgegevens en niet-persoonsgebonden gegevens) onlosmakelijk met elkaar verbonden zijn, dan is de AVG met al zijn rechten en plichten van toepassing op de gehele gemengde dataset, zelfs als het persoonsgegevensgedeelte slechts een klein deel van de hele dataset uitmaakt.

Noch de FFNPDR, noch de AVG definieert het concept van "onlosmakelijk verbonden" in hun kader.
De Europese Commissie heeft echter richtsnoeren uitgevaardigd voor het gebruik van gemengde datasets waarin zij dit concept verder verduidelijkt[309]. Een dataset kan bijvoorbeeld worden beschouwd als onlosmakelijk met elkaar verbonden of "het scheiden van de twee zou onmogelijk zijn of door de verwerkingsverantwoordelijke als economisch inefficiënt of technisch niet haalbaar worden beschouwd".[310]

---

[306] Europese Commissie. (29 mei 2019). Mededeling van de Commissie aan het Europees Parlement en de Raad. Richtsnoeren over de verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie, COM(2019) 250 final.

[307] Ibid.

[308] Zie artikel 2, lid 2, FFNPDR.

[309] Europese Commissie. (29 mei 2019). Mededeling van de Commissie aan het Europees Parlement en de Raad. Richtsnoeren over de verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie, COM(2019) 250 final.

[310] Ibid.

6.2.10 Intellectuele eigendomsrechten

Met de explosie in wetgeving die zich de afgelopen jaren heeft voorgedaan, kunnen er tal van andere verordeningen en richtlijnen van toepassing zijn. Met name de AI-regelgeving kan relevant worden wanneer AI-toepassingen, zoals door AI gegenereerde dashboards, worden geïntegreerd in de context van gegevensruimten. Andere relevante aspecten hebben betrekking op de toepassing van intellectuele eigendomsrechten en cyberbeveiligingsvereisten, die inherent met elkaar verbonden zijn. Daarom zullen in de komende paragrafen geselecteerde juridische overwegingen verder worden uitgewerkt om een leidraad te bieden aan partners.

6.2.10.1 Auteursrecht

Het auteursrecht biedt bescherming aan de manier waarop gegevens in een databank zijn georganiseerd.[311] Deze bescherming geldt alleen als de structuur van de databank **origineel** is. Dat betekent dat de keuzes en rangschikking van de inhoud voortkomen uit een **creatieve inspanning** van de maker.[312]
Arbeid en investeringen in de samenstelling van een databank volstaan niet om originaliteit aan te tonen. Het is vereist dat de wijze van ordening niet uitsluitend gebaseerd is op technische of logische voorschriften, maar ook op creatieve keuzes van de auteur die een persoonlijke stempel drukken op de structuur. Een klassiek voorbeeld is een telefoongids, die doorgaans niet als origineel wordt beschouwd omdat het alfabetisch ordenen van namen en nummers een logische aanpak is. Daarentegen kan een gids wél origineel zijn wanneer gegevens worden gestructureerd op basis van unieke criteria, zoals een indeling naar expertise of locatie. De bepalingen XI.186 tot en met XI.188 van het Wetboek Economisch Recht (WER) regelen de bescherming van databanken aan de hand van het auteursrecht.

Naast de structuur kan ook **de inhoud van een databank** auteursrechtelijk beschermd zijn, mits de afzonderlijke elementen zelf origineel zijn. Zo kunnen foto's in een catalogus van beeldhouwwerken beschermd zijn door auteursrecht, op voorwaarde dat ze een creatieve inspanning van de maker tonen. In dat geval is toestemming van de auteur nodig voor gebruik van deze elementen.

Een **dataset met gegevens** valt doorgaans niet onder de bescherming van het auteursrecht. Dit geldt ook voor datasets die gezondheidsgegevens bevatten. **Gezondheidsgegevens zijn immers een objectieve weergave van feiten of gezondheidstoestanden, en niet het resultaat van een originele en creatieve inspanning.** Met andere woorden, een dataset met gezondheidsgegevens komt in principe niet in aanmerking voor auteursrechtelijke bescherming.

Als een databank niet origineel is, kan deze eventueel wel nog beschermd worden via het ***sui generis*-recht,** dat een apart juridisch kader biedt voor de bescherming van databanken. Dit *sui generis*-recht beslaat de bescherming van databanken voor wat betreft het samenbrengen van de gegevens die ze bevat.[313]

---

[311] *Artikel XI.186 Wetboek Economisch Recht: "Databanken die door de keuze of de rangschikking van de stof een eigen intellectuele schepping van de auteur vormen, worden als zodanig door het auteursrecht beschermd. De bescherming van databanken op grond van het auteursrecht geldt niet voor de werken, de gegevens of de elementen zelf en laat bestaande rechten op de werken, gegevens of andere elementen vervat in de databank onverlet."*

[312] *FOD Economie. (24 maart 2022). Bescherming van Databanken door Het Auteursrecht.*

[313] *A. Decourriere, Les bases de données, in Droits intellectuels : contentieux de la validité et de la contrefaçon, 83e ed., Ser. Pratique du droit, Wolters Kluwer Belgium, 2020, p. 545-553.*

6.2.10.2 Het sui generis-recht van toepassing op databanken

Richtlijn 96/9/EG[314] creëert een bescherming voor het samenstellen van databanken[315], wanneer de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van **een substantiële investering**.[316] Dit werd voornamelijk gedaan met de insteek grote investeringen te doen renderen.[317] Het recht komt enkel toe aan de maker van de databank.[318] De **maker van een databank** is "*de persoon die het initiatief neemt en het risico draagt van de investering*"**.**[319] In tegenstelling tot het auteursrecht sluit deze definitie specifiek onderaannemers uit van de term "maker."
Hiernaast vermeldt de richtlijn ook de **auteur van een databank**, als zijnde "*de natuurlijke persoon of groep van natuurlijke personen die de databank heeft gecreëerd of, waar de wetgeving van de lidstaten dit toestaat, de rechtspersoon die door die wetgeving als rechthebbende wordt aangewezen."*[320]
Zij differentieert dus tegen de entiteit die het financiële risico liep tijdens de creatie en de eigenlijke maker van de databank.
Ten slotte vermeldt de richtlijn de **rechtmatige gebruikers.** Dit zijn personen die toegang hebben tot een databank volgens wettelijke voorwaarden. Zij genieten van bepaalde rechten en uitzonderingen zoals omschreven in de richtlijn.[321]

Een databank wordt in de richtlijn omschreven als een verzameling van werken, gegevens of andere zelfstandige elementen met elektronische middelen of anderszins toegankelijk.[322] Het is aan de maker van de databank om te beslissen of er vervolgens een permanente of tijdelijke reproductie, geheel of gedeeltelijk, een vertaling, bewerking, schikking en iedere andere verandering, een openbare verspreiding of kopie, of een mededeling, voorstelling of demonstratie voor het publiek kan plaatsvinden.[323] Er bestaan uitzonderingen op dit recht, met name wanneer een opvraging voor particuliere doeleinden van een niet-elektronische databank plaatsvindt, ter illustratie bij onderwijs of voor wetenschappelijk onderzoek met bronvermelding en voor zover door het niet-commerciële doel gerechtvaardigd, in het kader van de openbare veiligheid of een administratieve of gerechtelijke procedure.[324]
Er bestaat dus **een uitzondering voor het gebruik van een databank, wanneer dit gebeurt voor doeleinden van onderzoek,** wat van belang is in het kader van de Health Data Space. Moest er dus een *sui generis*-recht bestaan op de databank zelf, dan staat dit niet het gebruik voor wetenschappelijk onderzoek in de weg. Er bestaat een uitzondering op het toekennen van het *sui generis*-recht voor openbare lichamen in de publieke sector opdat het hergebruik van informatie niet raakt aan de bepalingen ingevoerd door de Open Data Richtlijn (zie sectie 6.2.7 Dataverordening).[325]

---

[314] *Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken (hierna: databankenrichtlijn).*

[315] *Het begrip databank dient ruim geïnterpreteerd te worden volgens het Hof van Justitie van de Europese Unie. (9 november 2024). Fixtures Marketing Zaak (C-46/02, ECLI:EU:C:2004:694). para. 28-32 en A. Decourriere, Les bases de données, in Droits intellectuels : contentieux de la validité et de la contrefaçon, 83e ed., Ser. Pratique du droit, Wolters Kluwer Belgium, 2020, p. 547.*

[316] *Artikel 7(1) Databankrichtlijn.*

[317] *Overweging 12 Databankenrichtlijn.*

[318] *A. Decourriere, Les bases de données, in Droits intellectuels : contentieux de la validité et de la contrefaçon, 83e ed., Ser. Pratique du droit, Wolters Kluwer Belgium, 2020, p. 550.*

[319] *Overweging 41 Databankenrichtlijn.*

[320] *Artikel 4(1) Databankenrichtlijn.*

[321] *Zie bijvoorbeeld artkel 6(1) Databankenrichtlijn.*

[322] *Artikel 1(2) Databankenrichtlijn.*

[323] *Artikel 5 Databankenrichtlijn.*

[324] *Artikel 9 Databankenrichtlijn.*

[325] *Artikel 1(6) PSI.*

De rechtspraak van het **Hof van Justitie van de Europese Unie (HvJEU)** heeft de potentiële reikwijdte van de *sui generis*-bescherming van databanken aanzienlijk ingeperkt. Het Hof heeft bepaald dat deze bescherming niet van toepassing is op databanken die worden gecreëerd als een bijproduct van de hoofdactiviteit van een organisatie.[326]

Voorbeelden van databanken die hierdoor buiten de reikwijdte van de *sui generis*-bescherming vallen:

- Automatisch gegenereerde datasets, zoals machine-generated data;
- Data afkomstig van IoT-apparaten;
- Gegevenspools of *data lakes*;
- Databanken die worden gecreëerd als onderdeel van een hoofdactiviteit, zoals **patiëntendossiers** die worden gegenereerd tijdens de gezondheidszorg.

De huidige beperkingen in de Databankenrichtlijn, met name in relatie tot de *sui generis*-bescherming, hebben geleid tot de oproep voor een **wettelijke verfijning**. Dit is noodzakelijk om de EU-wetgeving, inclusief de Databankenrichtlijn, beter af te stemmen op nieuwe regelgeving zoals de **European Health Data Space (EHDS)**. De EHDS-regelgeving vereist een moderne interpretatie van databankbescherming om te voldoen aan de behoeften van een datagedreven gezondheidszorgsysteem.

6.2.10.3 Bedrijfsgeheimen

Bedrijfsgeheimen worden nog op enkele bijkomstige manieren beschermd. Zo voorziet de EU-Richtlijn bedrijfsgeheimen[327] in het recht om op te treden tegen de onrechtmatige overname, diefstal, gebruik of openbaarmaking van onrechtmatig verkregen bedrijfsgeheimen en bestaat er ook een Richtlijn betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie. Dit wordt ook gereflecteerd in de artikelen XI.332/1 e.v. WER. Indien partijen bijkomende beschermingsmaatregelen willen installeren, kunnen zij bovendien een beroep doen op *non-disclosure agreements* of NDA's die voorkomen dat bedrijfsgeheimen publiek gemaakt worden.

Een bedrijfsgeheim wordt in de richtlijn omschreven als informatie die aan de volgende voorwaarden cumulatief voldoet:

> De informatie is geheim in die zin dat zij, in haar geheel dan wel in de juiste samenstelling en ordening van haar bestanddelen, niet algemeen bekend is bij of gemakkelijk toegankelijk is voor personen binnen de kringen die zich gewoonlijk bezighouden met de desbetreffende soort informatie;

> De informatie bezit handelswaarde omdat zij geheim is, en;

> De informatie is door de persoon die rechtmatig daarover beschikt, onderworpen aan redelijke maatregelen, gezien de omstandigheden, om deze geheim te houden.

6.2.10.4 IE-rechten in de EHDS

De EHDS-verordening biedt expliciet ruimte voor de bescherming van intellectuele eigendomsrechten (zie 6.2.5.3 Nationale implementatie). In overweging 60 worden juridische, organisatorische en technische maatregelen beschreven die kunnen worden ingezet om intellectuele eigendomsrechten en bedrijfs-geheimen te waarborgen. Voorbeelden hiervan zijn standaardovereenkomsten voor elektronische toegang tot gezondheidsgegevens en speciale verplichtingen in gegevensvergunningen met betrekking tot dergelijke rechten. De verordening erkent het belang van deze rechten en integreert waarborgen in haar kader.

---

[326] *Hof van Justitie van de Europese Unie. (9 november 2004). British Horseracing Board Ltd. V. William Hill Organization Ltd. (Zaak C-203/02, ECLI:EU:C:2004:695).*

[327] *Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan van 8 juni 2016.*

Elektronische gezondheidsgegevens die worden beschermd door intellectuele eigendomsrechten, bedrijfsgeheimen en/of die vallen onder het wettelijke recht op gegevensbescherming van artikel 10, lid 1, van Richtlijn 2001/83/EG[328] of artikel 14(11) van Verordening (EG) 726/2004[329], worden in de EHDS-verordening beschikbaar gesteld voor secundair gebruik in overeenstemming met de in deze verordening uiteengezette beginselen. In dit verband is het volgende van toepassing:[330]

- De houders van gezondheidsgegevens brengen de Health Data Access Body (HDAB) op de hoogte van elektronische gezondheidsgegevens die door een van bovenstaande regimes beschermd worden, en identificeren deze. Zij geven aan om welke delen van de gegevensreeksen het gaat en motiveren waarom de gegevens de specifieke bescherming nodig hebben die de gegevens genieten.
  Deze informatie wordt verstrekt wanneer de HDAB overeenkomstig artikel 60(3) van de EHDS-verordening in kennis wordt gesteld van de gegevensbankbeschrijvingen voor de gegevensreeksen die in haar bezit zijn, of uiterlijk naar aanleiding van een verzoek van de HDAB.
- De HDAB's nemen alle specifieke passende en evenredige maatregelen, met inbegrip van juridische, organisatorische en technische maatregelen, die zij nodig achten om de bescherming van bovenstaande regimes te vrijwaren. Het is aan de HDAB's om te bepalen of dergelijke maatregelen noodzakelijk en passend zijn.
- Bij het afgeven van gegevensvergunningen kunnen de HDAB's de toegang tot bepaalde elektronische gezondheidsgegevens afhankelijk maken van juridische, organisatorische en technische maatregelen. Dergelijke maatregelen kunnen contractuele regelingen tussen houders en gebruikers van gezondheidsgegevens omvatten om gegevens te delen die door intellectuele-eigendomsrechten of bedrijfsgeheimen beschermde informatie of inhoud bevatten. De Commissie ontwikkelt en beveelt niet-bindende modelcontractbepalingen voor dergelijke regelingen aan;
- Indien het verlenen van toegang tot elektronische gezondheidsgegevens voor secundaire doeleinden een ernstig risico met zich meebrengt dat een inbreuk zou worden gemaakt op een van de bovenstaande regimes, en dat risico kan niet op bevredigende wijze worden aangepakt, dan weigert de HDAB de gebruiker van de gezondheidsgegevens de toegang. De HDAB stelt de gebruiker van de gezondheidsgegevens in kennis van deze weigering en legt uit waarom geen toegang kan worden verleend. Houders en gebruikers van gezondheidsgegevens hebben het recht een klacht in te dienen overeenkomstig artikel 81 van de EHDS-verordening.

Ten slotte werpt de compromistekst van 2024 van de EHDS-verordening op dat aggregatietechnieken om persoonsgegevens te anonimiseren minder getest zijn voor niet-persoonsgebonden gegevens die bijvoorbeeld bedrijfsgeheimen bevatten, zoals in de verslaggeving over klinische proeven en klinisch onderzoek.[331] Bijkomend is de handhaving van inbreuken op bedrijfsgeheimen buiten de Unie moeilijker bij gebreke aan een toereikende internationale beschermingsnorm.[332] Deze soorten gegevens vallen dan onder artikel 5(13) van de DGA.

[328] Richtlijn 2001/83/EG tot vaststelling van een communautair wetboek betreffende geneesmiddelen voor menselijk gebruik van 6 november 2001.

[329] Verordening (EU) 726/2004tot vaststelling van communautaire procedures voor het verlenen van vergunningen en het toezicht op geneesmiddelen voor menselijk en diergeneeskundig gebruik en tot oprichting van een Europees Geneesmiddelenbureau van 31 maart 2004.

[330] Artikel 52 EHDS.

[331] Overweging 64 EHDS (compromistekst).

[332] Ibid.

6.2.10.5 Data ownership

Een fundamenteel filosofisch vraagstuk ligt besloten in het concept van *data ownership*.[333]
Bedrijven hebben enorme winsten geboekt met persoonsgegevens, maar dit roept soms de vraag op of zij recht hebben op deze opbrengsten als de data eigenlijk aan anderen toebehoort.[334] Een mogelijke benadering om dit fenomeen aan te pakken, is de idee van *data ownership*. Hierbij wordt geprobeerd een deel van de winsten terug te laten vloeien naar de betrokkenen, aangezien het hun persoonsgegevens zijn.[335]
Het is echter belangrijk te benadrukken dat deze discussie nog steeds theoretisch van aard is: in de praktijk bestaat er geen juridisch eigendomsrecht over data. In de AVG bestaat er bijvoorbeeld geen gelijkaardig concept. Hoewel het niet volledig van tafel is, blijft de praktische uitvoering ervan bijzonder complex. Bovendien betwijfelen sommigen of data als product überhaupt een duurzaam of succesvol model kan vormen.[336] Vanwege deze uitdagingen wordt aangeraden om voorlopig voorzichtig om te gaan met de term *data ownership* in het kader van de Health Data Space. Het concept heeft namelijk nog geen stabiele basis gevonden in de academische literatuur en verdere verfijning is nodig.

6.2.10.6 Afgeleide rechten

Hierboven wordt gesteld dat zowel het auteursrecht als het *sui generis*-recht, zoals vastgelegd in Richtlijn 96/9/EG, geen belemmering vormen voor het gebruik van databanken voor wetenschappelijke doeleinden. Binnen de context van het secundair gebruik in de de Vlaamse Health Data Space zijn er daarom geen juridische beperkingen op het gebruik van de data zelf.

Dit neemt echter niet weg dat er aandacht besteed moet worden aan de interactie tussen intellectuele eigendomsrechten en de Health Data Space. Een belangrijk aandachtspunt is wat er gebeurt met de resultaten van uitgevoerd onderzoek. Deze resultaten kunnen bijvoorbeeld in de vorm van een rapport of zelfs een uitvinding worden gegoten, die wél onder het auteursrecht of andere intellectuele eigendoms-rechten kunnen vallen. Een mogelijkheid is dat hier naar analogie met de EHDS-verordening wordt gehandeld, namelijk dat gegevensgebruikers verplicht zijn om de resultaten of output van het secundaire gebruik van elektronische gezondheidsgegevens, met inbegrip van informatie die relevant is voor de verstrekking van gezondheidszorg, openbaar te maken binnen 18 maanden na voltooiing van de verwerking van elektronische gezondheidsgegevens in de beveiligde omgeving of nadat zij antwoord op het in artikel 69 van de EHDS bedoelde gegevensverzoek hebben ontvangen, al gaat het hier enkel om anonieme gegevens.[337] Met het oog op het verder ontplooien tot een volwaardige health data space in de zin van de EHDS, zou dit uiteraard een logische stap zijn. Het is dan ook essentieel om binnen de Vlaamse Health Data Space duidelijke afspraken te maken over de verdeling van dergelijke rechten tussen de verschillende participanten. Dit voorkomt toekomstige geschillen en zorgt voor een eerlijke en transparante samenwerking.

6.2.11 Het gebruik van AI

Kunstmatige intelligentie (AI) is inmiddels een onmisbaar onderdeel van de gezondheidszorg geworden. AI wordt op verschillende manieren ingezet, zoals:

- Het genereren van datasets, bijvoorbeeld door het creëren van synthetische data;
- Het analyseren van datasets om resultaten af te leiden;
- Het trainen van AI-modellen met gezondheidsgegevens, bijvoorbeeld om medische diagnoses te stellen.

[333] *P. Hummel, M. Braun & P. Dabrock. (2020). Own Data? Ethical reflections on Data Ownership. Philosophy & Technology, (34), 545-572.*
[334] *A., Tanner, A. (2017). Our bodies, our data. How companies make billions selling our medical records. Beacon Press.*
[335] *J., Asswad, & J., Marx Gómez, (2021). Data Ownership: A Survey. Information, 12(11), 465.*
[336] *C., Ducuing, Data as a Contested Commodity (15 maart 2024).*
[337] *Artikel 61(4) EHDS.*

Het gebruik van AI brengt echter uitdagingen en risico's met zich mee, zoals ethische dilemma's, potentiële schendingen van privacy, en de noodzaak aan transparantie en betrouwbaarheid. Om deze risico's aan te pakken, heeft de Europese Commissie de **AI-verordening** (AIA)[338] ontwikkeld, die recent is goedgekeurd. Deze verordening heeft als doel om een kader te scheppen voor het veilige en verantwoorde gebruik van AI, met specifieke aandacht voor gezondheidsgerelateerde toepassingen.

De AI-verordening richt zich op de volgende kerndoelen:

- **Aanpakken van AI-specifieke risico's:** het identificeren en reguleren van risico's die ontstaan door AI-toepassingen.
- **Verbod op AI-praktijken met onaanvaardbare risico's:** bijvoorbeeld systemen die manipulatief of discriminerend zijn.
- **Regulering van hoog-risico AI-toepassingen:** het opstellen van duidelijke eisen voor AI-systemen die een hoog risico met zich meebrengen, zoals medische toepassingen.
- **Verplichtingen voor aanbieders en gebruikers van hoog-risico AI-systemen:** het vastleggen van specifieke verplichtingen voor fabrikanten en andere betrokken partijen.
- **Conformiteitsbeoordeling vóór vermarkting:** een verplichte controle om te garanderen dat AI-systemen voldoen aan de gestelde eisen voordat ze worden geïmplementeerd of op de markt worden gebracht.
- **Handhaving na vermarkting:** het monitoren van AI-systemen om te zorgen dat deze ook na ingebruikname aan de regelgeving blijven voldoen.
- **Governancestructuur opzetten:** het oprichten van een bestuursstructuur op zowel Europees als nationaal niveau om toezicht en naleving te waarborgen.

Hoewel de AI-verordening vaak wordt gepresenteerd als een instrument om fundamentele rechten en vrijheden te beschermen, is het in essentie **productwetgeving**. Dit betekent dat de verordening zich primair richt op de technische en operationele eisen voor AI-systemen. In de gezondheidssector sluit deze wetgeving aan bij bestaande productregelgeving, zoals de **Verordening betreffende medische hulpmiddelen (Medical Device Regulation, MDR)**. De MDR, die al van toepassing is in de gezondheidszorg, reguleert medische hulpmiddelen zoals instrumenten, apparaten, software, implantaten, reagentia, materialen of andere producten die door fabrikanten specifiek zijn ontworpen voor medische doeleinden bij mensen. Deze verordening bevat gedetailleerde eisen voor de veiligheid, kwaliteit en prestaties van dergelijke producten.[339]

De AI-verordening bouwt (onder meer) voort op dit kader door aanvullende eisen te stellen aan AI-systemen die worden ingezet als medische hulpmiddelen. Dit omvat onder meer de waarborging van transparantie, robuustheid en ethiek binnen AI-gedreven medische technologie.

Het kan zijn dat Health Data Space-participanten gebruik maken van een niet door hen ontworpen AI-systeem. Dit maakt hen mogelijk **gebruikers** in de zin van artikel 3(4) AIA. Anderzijds kan het ook zijn dat de uitkomst van het onderzoek resulteert in een AI-systeem of -model dat mede getraind is aan de hand van een via de Health Data Space verkregen dataset. Indien het resultaat van dergelijk onderzoek ook daadwerkelijk vermarkt wordt[340], dan kan de data consumer of user eventueel gekwalificeerd worden als **aanbieder van een hoog risico AI-systeem**. Het is dus van belang aandacht te hebben voor het gebruik van AI in het kader van de Health Data Space, want mogelijks is de AI-verordening wel degelijk van toepassing.

---

[338] *Verordening (EU) 2024/1689 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 van 13 juni 2024 (verordening artificiële intelligentie) (hierna: AIA).*

[339] *Artikel 2(1) MDR.*

[340] *Zie artikel 2(1)(a) AIA.*

6.2.11.1 Toepassing van de AI-verordening

Er bestaat een algemene uitzondering in de AI-verordening, waardoor de verplichtingen niet van toepassing zijn wanneer de ontwikkeling of het gebruik van een AI-systeem uitsluitend plaatsvindt voor **wetenschappelijke onderzoeksdoeleinden**.[341] In de praktijk betekent dit dat veel AI-toepassingen mogelijk buiten het toepassingsgebied van de verordening vallen. De exacte reikwijdte van deze uitzondering is echter nog niet volledig duidelijk.

De Engelstalige tekst van de AI-verordening specificeert dat het moet gaan om "*AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development*". Dit suggereert dat als een AI-systeem of -model voor meerdere doeleinden is ontwikkeld – bijvoorbeeld ook voor commerciële toepassingen – de uitzondering niet van toepassing is. Dit blijft zo, zelfs als de gebruiker het systeem uitsluitend voor wetenschappelijke doeleinden inzet. Dit vormt een potentieel probleem, vooral bij **general-purpose AI models (GPAIM)**. Vanwege hun aard zijn GPAIM immers ontworpen voor een breed scala aan toepassingen en niet uitsluitend voor één specifiek doel. Hun waarde ligt juist in hun veelzijdigheid.

De definitie van GPAIM in artikel 3(63) van de AI-verordening verduidelijkt dit slechts deels. GPAIM wordt omschreven als "*an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications,* ***except AI models that are used for research, development or prototyping activities before they are placed on the market****."* Hoewel de definitie opnieuw een uitzondering voor onderzoeksdoeleinden vermeldt, lijkt deze in de praktijk weinig impact te hebben. Dit komt omdat het moment waarop de verordening daadwerkelijk van toepassing wordt, pas de vermarkting van het model is. Voor die tijd kwalificeert een ontwikkelaar niet als "aanbieder" onder de AI-verordening, en gebruikers kunnen het model niet gebruiken, omdat het nog niet beschikbaar is.

De praktische reikwijdte van de onderzoeksuitzondering blijft onduidelijk. Hoewel de wetgever lijkt te hebben beoogd dat GPAIM onder deze uitzondering vallen, laat de huidige formulering ruimte voor twijfel. Dit werpt de vraag op of AI-systemen met een breed scala aan toepassingen daadwerkelijk van deze uitzondering kunnen profiteren, ondanks de intentie van de wetgever. Daarnaast blijft het onzeker of AI-systemen en -modellen met een beperkter toepassingsbereik, zoals commercieel inzetbare systemen, ook mogen worden gebruikt voor **"uitsluitend wetenschappelijke onderzoeksdoeleinden"** zonder buiten de uitzondering te vallen.

Deze discussie uit de weg gaand, moet natuurlijk worden benadrukt dat het werkveld van de AI-verordening voornamelijk hoog riciso AI-systemen betreft. Een AI-systeem moet dus eerst als hoog risico worden gekwalificeerd vooraleer de verplichtingen van toepassing zijn. Er zijn twee manieren waarop dit kan gebeuren:

- Het AI-systeem is bedoeld om te worden gebruikt als veiligheidscomponent van een product of het AI-systeem is zelf een product dat valt onder de in bijlage I opgenomen harmonisatiewetgeving van de Unie; en voor het product waarvan het AI-systeem de veiligheidscomponent op grond van punt 1) vormt of voor het AI-systeem als product zelf moet een conformiteitsbeoordeling door een derde partij worden uitgevoerd met het oog op het in de handel brengen of in gebruik stellen van dat product op grond van de in bijlage I van de AIA opgenomen harmonisatiewetgeving van de Unie.[342]
- Het AI-systeem valt onder de lijst opgenomen in bijlage III van de AI-verordening.[343]

[341] *Artikel 2(4) AIA.*

[342] *Artikel 6(1) AIA.*

[343] *Artikel 6(2) AIA.*

Voor de context van de Health Data Space is de volgende harmonisatiewetgeving uit Bijlage I mogelijk van tel, aangezien deze systemen mogelijk in een gezondheidscontext worden gebruikt:

> Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van **radioapparatuur** en tot intrekking van Richtlijn 1999/5/EG.
> Verordening (EU) 2016/426 van het Europees Parlement en de Raad betreffende **persoonlijke beschermingsmiddelen** en tot intrekking van Richtlijn 89/686/EEG van de Raad van 9 maart 2016;
> **Verordening medische hulpmiddelen**.[344]

De relevante toepassingen uit Bijlage III van de AI-verordening zijn wellicht de volgende, aangezien deze systemen mogelijk in een gezondheidscontext worden gebruikt:

> Toegang tot en gebruik van essentiële particuliere en publieke diensten en uitkeringen:[345]
  - AI-systemen die bedoeld zijn om door of namens overheidsinstanties te worden gebruikt om te beoordelen of natuurlijke personen in aanmerking komen voor essentiële overheidsuitkeringen en -diensten, **waaronder gezondheidsdiensten**, of om dergelijke uitkeringen en diensten te verlenen, te beperken, in te trekken of terug te vorderen.
  - AI-systemen die bedoeld zijn om noodoproepen van natuurlijke personen te evalueren en te classificeren of om te worden gebruikt voor het inzetten of het bepalen van prioriteiten voor de inzet van hulpdiensten, onder meer van politie, brandweer en ambulance, alsook van systemen voor de triage van patiënten die dringend medische zorg behoeven.

In artikel 6 van de AI-verordening worden nog bijkomstige uitzonderingen opgenomen waardoor AI-systemen toch niet als hoog risico worden aangemerkt.
De AI-verordening zal komende jaren geleidelijk aan van toepassing worden. Een aantal aspecten dienen te worden geïmplementeerd in nationale wetgeving. Zo moeten bijvoorbeeld overeenkomstig artikel 70 van de AI-verordening een aanmeldende autoriteit en een markttoezichtautoriteit worden aangesteld als nationale bevoegde autoriteiten. Hoe deze bevoegdheden concreet zullen worden verdeeld met het oog op de uit te voeren conformiteitsbeoordelingen, is momenteel een aspect dat wordt onderzocht door meerdere instellingen in het Vlaamse/Belgische landschap.[346]

Eventueel interessant om in het oog te houden is ook de notie van de **legal sandboxes** die door de AI-verordening nieuw leven in is geblazen. Dit laat toe om AI-toepassingen in *real world*-omstandigheden uit te testen. Hoewel de Health Data Space voornamelijk retroactief onderzoek beoogt, kan op termijn ook gekeken worden naar alternatieve manieren van onderzoek.

De AI-verordening zal vermoedelijk niet van toepassing zijn op AI-toepassingen die worden gebruikt in een onderzoekscontext, dankzij de uitzondering voor onderzoek. De omvang van deze uitzondering is echter niet geheel duidelijk. Bovendien vermelden andere wetgevende instrumenten, zoals de AVG, meerdere onderzoeksvelden naast *wetenschappelijk* onderzoek, zoals ook historisch of statistisch onderzoek. In de AI-verordening wordt dit niet gedaan, waardoor de vraag gesteld kan worden of deze vormen van onderzoek doelbewust zijn uitgesloten van de uitzondering.

---

[344] Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad.

[345] Bijlage III, punt 5, (a) en (d), AIA.

[346] Begin 2025 zal een visienota door het Kenniscentrum Data & Maatschappij worden gepubliceerd dat dieper ingaat op enkele aspecten van de AI-verordening. Het vraagstuk over welke autoriteiten welke bevoegdheden opnemen wordt hier onder meer breed in besproken.

Wanneer een AI-systeem of -model dat voortkomt uit onderzoek wordt onderworpen aan een conformiteitsbeoordeling (zie Bijlage I) of op de markt wordt gebracht (zie Bijlage III), zullen de verplichtingen van de AI-verordening wél van toepassing worden op de aanbieder. Het is daarom verstandig om al in de vroege stadia van het onderzoek rekening te houden met mogelijke toekomstige toepassingen van het systeem of model. Dit maakt het mogelijk om vanaf het begin te anticiperen op bepaalde verplichtingen uit de AI-verordening, zoals documentatievereisten, en zo eventuele aanpassingen in latere fasen te minimaliseren.

6.2.12 FAIR principles

Een belangrijk uitgangspunt binnen het beheer van onderzoeksgegevens is het gebruik van de FAIR-principes.[347] Deze principes richten zich op het mogelijk maken van ontdekking, evaluatie en hergebruik van gegevens in uiteenlopende contexten. FAIR staat voor vier kernkenmerken van goed beheerde onderzoeksgegevens, namelijk dat de gegevens:

- **Findable** (vindbaar) zijn,
- **Accessible** (toegankelijk) zijn,
- **Interoperable** (interoperabel) zijn, en
- **Reusable** (herbruikbaar) zijn.

Het is belangrijk op te merken dat FAIR-data niet hetzelfde zijn als open data. Open data moeten vrij beschikbaar zijn op het internet zonder financiële, juridische of technische barrières. Voor FAIR-data geldt enkel dat ze toegankelijk moeten zijn. Dit betekent niet dat de data openbaar moeten zijn, maar dat er duidelijke en toegankelijke richtlijnen bestaan voor hoe toegang kan worden verkregen, indien toegestaan. Hieronder gaan we dieper in op de vier kenmerken.

De eerste voorwaarde om data herbruikbaar te laten zijn, is ervoor zorgen dat ze **vindbaar** zijn. Hiervoor is het cruciaal om **kwalitatieve metadata** te voorzien. In deze metadata moet er minimaal beschreven zijn waarover de data gaat, en onder welke omstandigheden de data geconsulteerd kunnen worden. Dit houdt in dat er voldoende informatie voorhanden moet zijn over het project waarin de data verzameld werd, een samenvatting van de procedure, contactgegevens, enz. De metadata moet vindbaar zijn voor zowel mensen als machines. Dat houdt in dat er in de metadata (en in de data zelf) gebruikgemaakt moet worden van zowel de juiste semantische standaarden (SNOMED-CT, LOINC, ICD9-10-11, zie hoofdstuk 8.5 Datastandaarden) als van *unique and persistent identifiers*. Dit is een unieke en voor altijd bestaande code, waardoor machines in staat zijn om de juiste data items te vinden.

Per definitie is *alle metadata* verplicht vindbaar voor elke burger, met enkele uitzonderingen wanneer het gaat over bijvoorbeeld militaire metadata. De metadata moet ook te allen tijde beschikbaar blijven, zelfs wanneer een project afgelopen is en de data zelf niet meer beschikbaar is. Dat de metadata vindbaar is, betekent echter niet noodzakelijk dat ook de *data* vindbaar en/of toegankelijk is. Data is ook FAIR wanneer er duidelijk gemaakt wordt in de metadata wie, wanneer, onder welke voorwaarden en hoe men **toegang** kan krijgen tot de data.

Als derde pijler in de FAIR data principes, worden aanbevelingen gedaan om de **interoperabiliteit** van data zoveel mogelijk te boosten. Dit houdt in dat alle voorgeschreven **domeinspecifieke standaarden** zoveel mogelijk gevolgd moeten worden, waardoor data en metadata interoperabel worden. Dit betreft niet enkel semantische standaarden, maar ook standaarden voor dataopslag, metadata standaarden en standaarden voor datatransfer. Binnen het gezondheidszorgdomein zijn hier vandaag de dag nog maar weinig afspraken rond geformuleerd. In de toekomst kunnen standaarden als OMOP, OPENEHR, FHIR en andere, mogelijke pistes vormen om de interoperabiliteit van data te bevorderen. Bovenop standaarden vereisen de FAIR

[347] *Zie ook Go4Fair, z.d.*

data principes ook dat men zoveel mogelijk werkt met linked data, *unique and persistent identifiers* en andere technieken die de **machineleesbaarheid** van data en metadata optimaliseren.

Als laatste vereisen de FAIR data principes dat er **zoveel mogelijk informatie en documentatie** wordt gepubliceerd, waardoor eender welke (her)gebruiker van de data in staat zou moeten zijn te evalueren of de desbetreffende data herbruikbaar is voor zijn of haar use case. Dit houdt in dat details zoals primaire doelstellingen, potentieel secundaire doelstellingen, gevolgde procedures, ethische commissieaanvragen, gebruikersvoorwaarden, een preview van de data, enz. ter beschikking gesteld worden.

Hoewel de FAIR-principes al enkele jaren worden toegepast, blijkt in de praktijk dat ze vaak niet strikt worden nageleefd. Nochtans kunnen enkele van deze principes met relatief beperkte inspanningen zorgen voor een aanzienlijke verbetering in de vindbaarheid, toegankelijkheid, interoperabiliteit en herbruikbaarheid van data.
Voor de data4PHM use case werd een analyse uitgevoerd om het huidige niveau van FAIR-compliance van een specifieke databron in kaart te brengen. Op basis hiervan werden concrete verbetermogelijkheden voorgesteld om de databron verder te optimaliseren. Deze info is te vinden in hoofdstuk 9.3 Fair data en metadata.

6.3 HET SAMENSPEL VAN WETGEVING

Een van de belangrijkste vastgestelde *lacunes* naar aanleiding van het gevoerde onderzoek blijkt hoe lastig het samenspel van alle verschillende toepasselijke wetgevende normen te zijn. Hoe verordeningen gelijktijdig op eenzelfde context van toepassing zijn, blijkt niet altijd duidelijk.

Hoe actoren, mede zoals ze worden gedefinieerd in de EHDS-verordening, worden gekwalificeerd in de AVG bijvoorbeeld, is niet geheel helder. De Health Data Space omvat zowel primair als secundair gebruik van gegevens (zie 6.2.4.1 Relevante definities voor meer informatie over deze begrippen). Indien instanties die dergelijk onderzoek uitvoeren aan bepaalde voorwaarden voldoen, kunnen zij Health Data Space-participanten worden en op deze manier toegang verzoeken tot datasets waarop onderzoek kan worden uitgevoerd. Het is aan de data consumer in de Health Data Space om een aanvraag in te dienen bij de dataprovider waarvan zij een dataset wensen. Het is dus de data consumer die het doel en de middelen van de gegevensverwerking bepaalt, zoals welke onderzoeksdoeleinden worden nagestreefd en met welke gegevens – als deze al verkregen worden via de Health Data Space – het onderzoek zal worden uitgevoerd. De Health Data Space fungeert in deze interactie als het technische platform en verbindingskader waarbinnen deze gegevensoverdrachten kunnen plaatsvinden.

De Health Data Space zelf beslist echter niet over het doel of de middelen van de verwerking; zij faciliteert enkel de overdracht door enerzijds actoren met elkaar in contact te brengen en anderzijds het praktisch mogelijk te maken om de overdracht van gegevens te doen plaatsvinden. De Health Data Space fungeert als het kader waarin datadelen kan plaatsvinden (zie hiervoor ook de opmaak van een usage policy die plaatsvindt in het kader van het huidige project).

De Health Data Space dient dus naar alle waarschijnlijkheid niet als verwerkingsverantwoordelijke te worden beschouwd onder de AVG, indien er toch persoonsgegevens zouden worden verwerkt.
De **dataproviders** die deelnemen aan de Health Data Space stellen zelf concrete doeleinden voor het datadelen en zijn daarom **verwerkingsverantwoordelijke**. Dit is in analogie met overweging 55 van de EHDS-verordening.[348] Hierin wordt verduidelijkt dat de *health data holder*, *health data access bodies* en de *health data users*, allen, op hun beurt, aanschouwd worden als verwerkingsverantwoordelijken voor een specifiek deel van de verwerking en respectievelijk naar hun rollen hierin.

[348] *Er kan ook verwezen worden naar artikel 8 Decreet tot oprichting van het platform Vitalink van 8 juli 2022.*

Zo is de *health data holder* verwerkingsverantwoordelijke voor de volgende verwerkingsactiviteiten:

- voor de verstrekking van de gevraagde persoonlijke elektronische gezondheidsgegevens aan het Health Data Access Body;
- voor de verwerking van persoonlijke elektronische gezondheidsgegevens in verband met de verstrekking ervan aan de health data user op grond van een gegevensvergunning of gegevensverzoek.

De *health data holder* moet worden gekwalificeerd als verwerker ten aanzien van de volgende verwerkingsactiviteiten:

- verwerker voor de *health data user* bij het verstrekken van gegevens via een beveiligde verwerkingsomgeving.

De *Health Data Access Body* is verwerkingsverantwoordelijke voor de verwerking van elektronische gezondheidsgegevens bij het voorbereiden van de gegevens en het ter beschikking stellen ervan aan de gezondheidsgegevensgebruiker. Het is dan weer verwerker namens de *health data user* voor de verwerking die de *health data user* uitvoert op grond van een gegevensvergunning in de beveiligde verwerkingsomgeving alsook voor de verwerking om een antwoord op een gegevensverzoek te generen.

De *health data user*, ten slotte, is verwerkingsverantwoordelijke voor de verwerking ven persoonlijke elektronische gezondheidsgegevens in gepseudonimiseerde vorm in de beveiligde verwerkingsomgeving op grond van zijn gegevensvergunning.

Bij de beoordeling van de rol van de Health Data Space onder de AVG is een belangrijke nuance op zijn plaats, aangezien de Health Data Space mogelijk beperkingen oplegt aan het gebruik van haar diensten en infrastructuur. Zo kan de Health Data Space bepaalde doeleinden zoals strikt commercieel onderzoek, uitsluiten in haar usage policy. Daarnaast verplicht de Health Data Space participanten om technische middelen, zoals een connector, te installeren om toegang tot de infrastructuur te verkrijgen.

Deze inmenging met zowel de doeleinden waarvoor gegevens worden gebruikt als de technische uitvoering (i.e. de middelen), roept vragen op over de kwalificatie. Enerzijds zou de Health Data Space kunnen worden beschouwd als een gezamenlijke verwerkingsverantwoordelijke, omdat haar ingrepen de beslissings-bevoegdheid van Health Data Space-participanten ten aanzien van hun verwerkingsactiviteiten kan beïnvloeden, zowel op juridisch als technisch vlak. Anderzijds kan worden beargumenteerd dat de Health Data Space enkel optreedt als aanbieder van diensten. In dat geval is zij hoogstens een verwerker, aangezien participanten zelf beslissen om gebruik te maken van de diensten en akkoord gaan met de bijbehorende voorwaarden. Hier komt dan weer verandering in wanneer participanten niet meer vrij, maar verplicht zijn om gebruik te maken van de Health Data Space, zoals bij primaire verwerkingen die gebeuren in het kader van de gezondheidszorg zoals beschreven in de EHDS-verordening. Dan gaat dezelfde redenering, waarbij participanten louter vrije dienstafnemers zijn, niet meer op. Hoe de verantwoordelijkheden en rollen dan verdeeld worden, is nog onbeantwoord.

Deze overweging onderstreept een breder spanningsveld in de gelijktijdige toepassing van de Data Governance Act, de EHDS-verordening en de AVG. De exacte verhouding tussen deze instrumenten in de praktijk is complex en onduidelijk. Verwacht wordt dat een *white paper* van CiTiP, gepland voor het late voorjaar van 2025, dieper zal ingaan op deze kwesties. Een fundamentele vraag is of de rolverdeling onder de AVG voldoende flexibiliteit biedt voor nieuwe entiteiten zoals data spaces. Naarmate gegevensketens langer worden en actoren zoals de Health Data Space of databemiddelingsdiensten opkomen, kan het noodzakelijk zijn om na te denken over een meer genuanceerde rolverdeling binnen de AVG. Zo zou een "verwerkingsverantwoordelijke-light"-rol kunnen worden overwogen voor entiteiten die gegevensdeling faciliteren, zonder volledige verantwoordelijkheid over de inhoudelijke verwerking te dragen.

Hoewel deze discussie academisch relevant is, volgt het huidige project de rolverdeling zoals hierboven geschetst. De participanten zijn dus verwerkingsverantwoordelijke ten aanzien van hun eigen verwerkingsactiviteiten, waarbij de Health Data Space vooralsnog geen rol onder de AVG opneemt, vanwege het feit dat zij geen (geanonimiseerde) persoonsgegevens verwerkt op dit ogenblik. De Health Data Space verwerkt wel gegevens bij het opstellen en beschikbaar maken van diens catalogus met metadata. Ten aanzien van deze activiteit is zij dus wel verwerkingsverantwoordelijke. Momenteel wordt deze pragmatische visie toegepast, maar vooralsnog blijft onduidelijk wie welke verantwoordelijkheden op zich neemt, en zal de verdere uitwerking van de juridische kaders cruciaal zijn voor een robuuste en werkbare toepassing van de EHDS binnen de Vlaamse context. Daarnaast is ook van belang wie de Health Data Access Body in de Belgische context zal zijn. Dit kan een entiteit zijn die kadert binnen de Health Data Space, die vervolgens ten aanzien van haar eigen activiteiten als verwerkingsverantwoordelijke moet worden beschouwd.

Het is bovendien mogelijk dat er **gezamenlijke verwerkingsverantwoordelijken** bestaan binnen de context van de Health Data Space. Een dergelijke situatie kan zich voordoen wanneer meerdere data users of consumers dezelfde dataset opvragen of gezamenlijk onderzoek uitvoeren. In dat geval dragen zij gezamenlijk de verantwoordelijkheid voor de verwerking van de gegevens. Het is dan aan de betrokken verwerkingsverantwoordelijken om een onderlinge overeenkomst op te stellen die hun respectieve verantwoordelijkheden regelt. Indien gewenst, zou de Health Data Space een template kunnen aanbieden om dit proces te vergemakkelijken. Deze overeenkomst dient op verzoek te kunnen worden voorgelegd aan de governance authority, opdat deze controle kan uitoefenen wanneer noodzakelijk.

6.4 ETHISCHE PRINCIPES

Naast de consideraties die moeten worden genomen naar aanleiding van wetgeving, zijn er ook tal van ethische aspecten die in rekening moeten worden gehouden bij het uitvoeren van een project.
De bescherming van de mensenrechten staat centraal, ook bij de opkomst van technologieën zoals kunstmatige intelligentie (AI), multi-computation en het genereren van synthetische gegevens.
Idealiter geeft wetgeving reeds gevolg aan ethische opvattingen, waardoor de juridische bepalingen reeds ethische overwegingen ten uitvoer leggen. Een voorbeeld hiervan is de AVG, waarin ethische elementen zoals transparantie, verantwoordingsplicht en de bescherming van digitale rechten een centrale rol spelen. Ook het principe van toestemming speelt een sleutelrol bij het waarborgen van de autonomie en waardigheid van individuen.

De wetgeving dient dus als een startpunt, waarna er moet gekeken worden naar ethische waarden en aanvullende richtlijnen om verder dan de wet te gaan met betrekking tot het ethisch kader. De wetgeving, hoe vooruitziend deze ook tracht te zijn, kan immers nooit met alle nieuwe ontwikkelingen en technologische vooruitgang rekening houden. Ethische principes dienen als richtinggevende normen, maar ook als grenzen aan de ontwikkeling van toepassing van technologieën. Tegelijkertijd dient er te worden benadrukt dat “ethisch zijn” niet voortkomt uit het afvinken van verplichte criteria en dat hier niet automatisch een ethisch verantwoorde technologie uit voort zou komen. Ethisch handelen vereist een voortdurende iteratie en herziening van de gebruikte methoden en toepassingen. Het houdt in dat ethische waarden en houdingen worden geïntegreerd in de ontwikkelingsfase. Dit niet enkel ten aanzien van het verantwoord verwerken van persoonsgegevens, maar ten aanzien van een algemene bescherming voor de mensrenrechten.

In dit verband zijn er enkele ‘leidraden’, zoals de vier biomedische principes in ethiek door BEAUCHAMP en CHILDRESS en de verklaring van Taipei, die naar voren worden geschoven om ethisch onderzoek te faciliteren. Ook in de relaties tussen arts en patiënt spelen veel ethische overwegingen mee.
De onderstaande aangehaalde principes richten zich echter op onderzoek (of secundaire verwerkingsactiviteiten) in het kader van de Health Data Space. De Verklaring van Helsinki wordt niet nader besproken, aangezien deze (klinisch) onderzoek met mensen betreft en dit in het kader van het huidige project niet als relevant werd beschouwd.

6.4.1 De vier biomedische principes in ethiek door Beauchamp en Childress

De vier biomedische ethische principes die zijn ontwikkeld door BEAUCHAMP en CHILDRESS[349] zijn richtingaangevend wat betreft het voeren van wetenschappelijk onderzoek. Daar waar wetgeving zwijgt, zorgen de principes voor extra ondersteuning.

De principes klinken als volgt:

PRINCIPE	OMSCHRIJVING	UITING IN DE PRAKTIJK
Weldadigheid (*beneficence*)	Het principe van weldadigheid voorziet in het actief bijdragen aan het welzijn en de welvaart van anderen en het beschermen van de rechten en vrijheden van anderen.[350]	Beschermen van de menselijke veiligheid en het algemeen belang (bv. kwaliteitscontrole en verbeteringsmaatregelen);[351] Toewijzen van verantwoordelijkheid en het stimuleren van aansprakelijkheid (bv. door te zorgen voor menselijk toezicht wanneer AI wordt gebruikt).[352]
Onschadelijkheid (*non-maleficence*)	Dit principe omvat de verplichting om anderen geen schade toe te brengen en geen risico's te creëren ten nadele van anderen.[353]	Regelgeving en cyberveiligheidsvoorwaarden adequaat te implementeren;[354] De authenticiteit en integriteit van gegevens te waarborgen door middel van een mechanisme voor toegangscontrole.[355]
Respect voor autonomie	Respect voor iemands autonomie houdt in dat de keuzes van een individu worden gerespecteerd en dat er niet wordt ingegrepen in iemands besluitvormingsproces.[356]	Dit is een principe dat in de gezondheidszorg veelvuldig voortkomt. Het is bijvoorbeeld aan de patiënt om de uiteindelijke beslissingen in zijn/haar dossier te nemen, waar de arts slechts als een adviserende entiteit tussenkomt. Hiervoor moet men transparant zijn (het is bijvoorbeeld niet voldoende om alleen algemene informatie aan de patiënt te geven, maar het moet geïndividualiseerd zijn). Advies op maat moet via de arts aan de patiënt worden meegedeeld, zodat deze kan begrijpen hoe en waarom zijn gegevens worden gebruikt gedurende het onderzoek.[357]

[349] *T.L. Beauchamp & J.F. Childress (2013) Principles of Biomedical Ethics, 7th Edition.*

[350] *Ibid, p. 202-205.*

[351] *World Health Organization (WHO). (28 juni 2021). Ethics and governance of artificial intelligence for health – WHO Guidance, p. 26.*

[352] *Ibid, p. 28.*

[353] *T.L. Beauchamp & J.F. Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 150-155.*

[354] *World Health Organization (WHO). (28 juni 2021). Ethics and governance of artificial intelligence for health – WHO Guidance, p. 26.*

[355] *G., Verhenneman, A., Vedder. (30 juni 2015). 'WITDOM "Empowering privacy and security in non-trusted environments", D6.1 – Legal and Ethical framework and privacy and security principles', p. 44.*

[356] *T.L. Beauchamp & J.F. Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 103-107.*

[357] *European Union Agency for Cybersecurity (ENISA). (Juni 2023). Cybersecurity and privacy in AI - Medical imaging diagnosis, p. 19.*

PRINCIPE	OMSCHRIJVING	UITING IN DE PRAKTIJK
Rechtvaardigheid	Het principe van rechtvaardigheid vereist om anderen eerlijk te behandelen en gelijke en rechtvaardige kansen te bieden aan iedereen.[358]	Gegevens te verwerken op een manier die de patiënt zou verwachten (bv. het gebruik voor het opsporen van een specifieke ziekte zou te verwachten zijn, terwijl mogelijke negatieve effecten uiteraard niet als zodanig kunnen worden beschouwd).[359] Inclusiviteit en rechtvaardigheid te beschermen (onderzoekers moeten zich bijvoorbeeld bewust zijn van en rekening houden met mogelijke vooroordelen bij het voeren van onderzoek om ongelijkheden in de gezondheidszorg te voorkomen).[360]

Uit deze principes schrijden dus concrete richtlijnen voort (dit is de derde kolom in het bovenstaande kader) die moeten worden meegenomen bij het uitvoeren van wetenschappelijk onderzoek. De principes richten zich in beginsel dus op wetenschappelijk onderzoek, maar uiteraard zijn deze niet alleenstaand en dienen zij te worden toegepast in de wettelijke kaders die veel van deze aspecten reeds verplichten.
De Health Data Space moet deze beginselen promoten en faciliteren ten aanzien van de secundaire verwerkingsactiviteiten die plaatsvinden in het kader van de Health Data Space. Indien er wetenschappelijk onderzoek plaatsvindt, voor welk uiteindelijk doeleinde dan ook (dit kan preventieve gezondheidszorg zijn, maar ook gepersonaliseerde geneeskunde of epidemiologisch onderzoek), dienen deze beginselen, waar relevant, te worden meegenomen en toegepast.

6.4.2 Verklaring van Taipei

Los van de principes die van toepassing zijn tijdens het uitvoeren van onderzoek, zijn er ook ethische overwegingen die de resultaten van onderzoek beheersen. Zo werd een Verklaring van Taipei[361] aangenomen door de WORLD MEDICAL ASSOCIATION (WMA). Dit volgde na de eerder genomen Verklaring van Helsinki[362] die zich richt op de ontwikkeling en digitalisering van onderzoek. De Verklaring van Taipei houdt rekening met het potentieel dat grote verzamelingen gegevens en menselijke specimens met zich meebrengen voor de ontwikkeling van nieuwe onderzoeksstrategieën en voorspellende modellen.
Dit kadert in de big data-hype, die zich uiteraard ook in het onderzoeksveld afspeelt. Dergelijke databases brengen immers ook bepaalde risico's met zich mee. Het is bedoeld om een evenwicht te bereiken tussen de rechten van individuen met betrekking tot hun deelname aan onderzoek, vertrouwelijkheid en privacyregels, terwijl het potentieel van gezondheidsgegevens wordt erkend als een krachtig instrument om kennis te vergroten. Het risico van dergelijke biobanken en de veelheid van gezondheidsgegevens stamt niet noodzakelijk uit wetenschappelijk onderzoek voort, maar lijkt veelal te liggen in het commerciële, administratieve of politieke gebruik van dergelijke gegevens. De verklaring treedt daarom ook buiten het toepassingsgebied van de medische context en raakt meer dan enkel de relatie arts-patiënt, waar de arts uiteraard reeds een zekere verantwoordelijkheid ten aanzien van zijn patiënten heeft.[363]

[358] *T.L. Beauchamp & J.F. Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 249-277.*

[359] *European Union Agency for Cybersecurity (ENISA). (Juni 2023). Cybersecurity and privacy in AI - Medical imaging diagnosis, p. 19.*

[360] *World Health Organization (WHO). (28 juni 2021). Ethics and governance of artificial intelligence for health – WHO Guidance, p. 29.*

[361] *World Health Association (WMA). (4 juni 2020). Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks (Hierna: Verklaring van Taipei).*

[362] *Hier wordt niet dieper op ingegaan omdat deze Verklaring eerder van toepassing is op het effectief uitvoeren van klinische proeven dan op het retroactief uitvoeren van onderzoek op gegevens, zoals wat beoogd wordt in de Health Data Space.*

[363] *Verklaring van Taipei.*

Allereerst is de Verklaring van Taipei van mening dat gezondheidsonderzoek een gemeenschappelijk “goed” is dat in het belang van zowel individuele patiënten, als de samenleving in het algemeen, is.[364]
Hierop bouwend bevat de Verklaring ethische overwegingen met betrekking tot gezondheidsdatabases en biobanken, aangezien onderzoek, gezondheidsdatabases en biobankgerelateerde activiteiten moeten bijdragen aan het welzijn van de samenleving, met name de belangen van de volksgezondheid.[365]
Prima facie kan worden opgemerkt dat een dergelijke visie overlapt met de opzet van de Health Data Space.

De Verklaring richt zich ook op de arts-patiëntrelatie door de arts als de “hoeder van data” te beschouwen, waardoor deze specifieke ethische en wettelijke verplichtingen heeft die zorgen voor de bescherming van de patiëntgegevens. Onder meer de rechten op autonomie, privacy en vertrouwelijkheid proberen de patiënt controle te geven over diens persoonsgegevens en biologisch materiaal.[366] Vertrouwelijkheid, zoals ook blijkt uit de bevraging bij spelers in het veld in het kader van het opzetten van een Health Data Space, is een cruciaal element om het vertrouwen en de integriteit in gezondheidsdatabanken te behouden.[367]
Het verzamelen, opslaan en gebruiken van gegevens van deelnemers die toestemming kunnen geven, moet vrijwillig zijn en moet worden verzameld voor bepaald onderzoek, in overeenstemming met de specifieke, vrije en geïnformeerde toestemming die is neergelegd in de Verklaring van Helsinki.[368] Indien de gegevens voor meervoudig en onbepaald gebruik in een gezondheidsdatabank worden opgeslagen, is de toestemming alleen geldig indien de betrokkene voldoende is geïnformeerd over de in punt 12 van de verklaring genoemde aspecten, met inbegrip van het doel van de gezondheidsdatabank of de biobank, de risico's en lasten van de opslag en verzameling van de gegevens, de regels voor de toegang tot de gegevens, enzovoort. Ook indien onderzoek wordt uitgevoerd op basis van het gerechtvaardigd belang overeenkomstig artikel 6.1.*f)* van de AVG, en niet op basis van de toestemming overeenkomstig artikel 6.1.*a)* van de AVG, moet de oorspronkelijke patiënt afdoende geïnformeerd worden. Het verkrijgen van de toestemming kadert echter meer in een context waar het initiële onderzoek ook werd uitgevoerd op basis van de toestemming. Hiervoor speelt de verklaring van Helsinki[369] een belangrijke rol als ethische ondersteuning bij het verkrijgen van de nodige toestemmingen van de patiënt/proefpersoon.

Wellicht leiden sommige verwerkingen in het kader van de Health Data Space tot gezondheidsdatabanken. Om betrouwbaar te zijn, moeten deze worden beheerd door interne en externe mechanismen, zoals de bescherming van de rechten van individuen (bescherming van individuen), het handhaven van transparantie, relevante informatie over databases moet beschikbaar zijn voor het publiek (transparantie), het raadplegen en betrekken van individuen en hun gemeenschappen (participatie en inclusie), en toegankelijk zijn voor en reageren op alle belanghebbenden (verantwoordingsplicht).[370] Alle professionals die bijdragen aan of werken met gezondheidsdatabanken en biobanken moeten adequate governanceregelingen treffen.[371]
Dergelijke governanceregelingen moeten alle elementen omvatten die zijn opgesomd in sectie 21 van de verklaring, zoals het doel van de database vastleggen, de aard van de opgeslagen gezondheidsgegevens bepalen, regelingen voor de bewaartermijn en de vernietiging van de gegevens of het materiaal; enzovoort. De in de Verklaring opgenomen voorschriften zijn vrij oppervlakkig van aard, dus het zal aan de houder/maker van een dergelijke databank zijn om over te gaan tot concrete uitvoering hiervan. Het spreekt dan ook voor zich dat een in de verklaring opgenomen verplichting is dat gezondheidsdatabanken worden beheerd onder de verantwoordelijkheid van naar behoren gekwalificeerde beroepsbeoefenaren die de naleving van de verklaring kunnen garanderen.[372]

[364] *Verklaring van Taipei, sectie 5.*

[365] *Ibid, sectie 8.*

[366] *Ibid, sectie 9.*

[367] *Ibid, sectie 10.*

[368] *Ibid, sectie 11.*

[369] *World Health Association (WMA). (Oktober 2013). Declaration of Helsinki – Medical research involving human participants.*

[370] *Verklaring van Taipei, sectie 20.*

[371] *Ibid, sectie 22.*

[372] *Ibid, sectie 23.*

In het kader van de Health Data Space moet vooreerst besproken worden “onder wie” dergelijke databanken zich situeren. In principe verwerkt de Health Data Space immers zelf geen gegevens en gebeuren overdrachten aan de hand van geïnstalleerde connectoren. Het resultaat van onderzoek zal dan ook bij data consumers (of in dit geval wellicht data users) komen te liggen. Deze “afgeleide gegevens” die volgen uit het uitvoeren van onderzoek op via de Health Data Space verkregen gegevens, zullen in werkelijkheid immers vaak bruikbaar zijn voor andere actoren. Vanuit de ingesteldheid dat wetenschappelijk onderzoek in het algemeen belang is en dat het resultaat hieruit gemeen goed is, dienen dergelijke databanken ook door anderen, te worden hergebruikt. Los van de vereisten die reeds zijn opgenomen in de wetgeving (zie hiervoor bijvoorbeeld de richtlijn inzake open data in sectie 6.2.7 Dataverordening), kan dit dus steeds een opzet zijn van de Health Data Space, waarbij deze Health Data Space participanten bepaalde resultaten moeten delen met anderen. De EHDS-verordening weerspiegelt trouwens ook een dergelijke ingesteldheid (zie sectie 6.2.5.3 Nationale implementatie).

7 GOVERNANCE

7.1 SITUERING EN DEFINITIEVAN GOVERNANCE

Historisch gezien wordt governance vooral binnen de context van gouvernementeel bestuur gepercipieerd. In die zin staat governance synoniem voor het (goed) bestuur door een overheid, waarbij in het bijzonder aandacht wordt besteed aan haar regelgevend karakter (Vlaamse Overheid, 2024). De hierboven beschreven opkomst van data spaces brengt niet enkel technologische uitdagingen met zich mee, maar doet ook de aandacht toenemen voor het bestuur van complexe ecosystemen, én het beheer van (grote hoeveelheden) data. Het is pas door beide aspecten met elkaar te verzoenen, dat men aan 'data space governance' kan doen.

Om tegemoet te komen aan de vele vragen rond het opzetten en beheren van data spaces, richtte de EU het **Data Space Support Centre (DSSC)**[373] op. Naast **kennisdeling** over de technische bouwblokken, biedt DSSC ook informatie aan over governance binnen een Europese data space, waarbij rekening wordt gehouden met de specifieke legale context binnen Europa (bv. door middel van de Data Act, Data Governance Act ...). Maar waar er vandaag, onder andere dankzij DSSC, reeds veel informatie beschikbaar is over data space governance, is deze vaak erg complex of zelfs ongekend bij het bredere ecosysteem.

Zowel gesprekken met stakeholders als desk research tonen aan dat het concept governance niet goed ingeburgerd is. Hoewel de partijen wel van governance gehoord hebben en weten dat het belangrijk is, blijkt men vaak weinig inzicht te hebben in welke domeinen, taken en verantwoordelijkheden onder data space governance vallen. Ook de sterke verwevenheid van governance met *business* en *legal* bemoeilijkt een concrete invulling van het concept in een health data space.

Voordat we dieper in de methodologie en voorgestelde governance-aanpak duiken, wordt hieronder eerst een beknopt theoretisch kader geschetst omtrent wat governance is en waarom dit een essentiële voorwaarde is voor ***vertrouwen*** in een data space.

7.1.1 Wat is data space governance?

Data space governance steunt op twee pijlers: het **beheren van het ecosysteem** (i.e. de organisatorische governance met focus op rollen, verantwoordelijkheden en onderlinge relaties) en het **beheren van data en data-uitwisseling** (data governance). DSSC definieert de twee pijlers als volgt:

> "(1) *Organisational governance:* identifying key decision points and options for establishing inclusive governance and transparent rules and roles [...] to guide the participants to organise the data space and achieve their goals.
> (2) *Data sharing governance*: establishing common rules that promote effective and reliable data sharing processes and introduces different ways to organise data transactions within a data space [...] Clear data sharing rules are essential for building trust between data space participants and directly reflect the functionality of the data space." (DSSC, 2024)

Het einddoel van beide vormen van governance is, in lijn met haar oorspronkelijke betekenis, dan ook hetzelfde: **het ondersteunen van beslissingen ten voordele van goed bestuur**, en dit door middel van zowel heldere regels als duidelijke definiëring van rollen en verantwoordelijkheden.

[373] https://dssc.eu/

Deze holistische benadering van governance, die zowel het organisatorische als data sharing aspect dekt, sluit goed aan bij de noden die leven binnen het (Vlaamse) gezondheidsecosysteem. Om die reden zal de rest van dit hoofdstuk rond governance verder bouwen op dit DSSC-framework, tenzij anders aangegeven:

> *"Data space governance verwijst naar een geheel aan principes, beleid, regels en procedures die het mogelijk maken om op een veilige, faire en transparante manier data te delen in een data space. Het is een kader dat vertrouwen en verantwoordelijkheid creëert tussen provider, consumers en andere stakeholders in een data space ecosysteem."*

7.1.2 Waarom governance: het belang van vertrouwen

Een data space is in de eerste plaats een data ecosysteem waarbinnen partners aan waardecreatie[374] doen. Of die waarde nu van financiële, maatschappelijke of reputationele aard is, een samenwerking kan slechts duurzaam zijn wanneer de verschillende actoren elkaar vertrouwen (DSSC, 2024).

> *"Without trust and longterm [sic] collaboration any effort toward making a [data space] accessible is doomed to fail. That's why well-designed governance principles, processes and tools, will be essential to deliver the benefits of a connected data space." (Fritzenkötter, et al., 2022)*

Dit sentiment, waarbij **vertrouwen een *conditio sine qua non* vormt voor het goed functioneren van een data space**, blijkt vandaag sterk gedragen binnen het gezondheidsecosysteem. Tegelijkertijd vormt het gebrek aan vertrouwen één van de grootste barrières voor het uitwisselen van data, en al zeker voor de uitwisseling van (persoonlijke) gezondheidsdata (zie sectie 7.3.5.5 Solid). Een succesvolle health data space zal hieraan dus moeten tegemoetkomen. En alhoewel dit zeker een uitdaging vormt, is het ook een uitgelezen opportuniteit om via goed onderbouwde governancekeuzes *vertrouwen* te creëren, en zo positie in te nemen binnen het ecosysteem als voorkeurspartner voor datadeling.

Vertrouwen binnen een data space zal groeien op basis van gedeelde positieve ervaringen. Tegelijkertijd moet een data space al het mogelijke doen om vertrouwen te stimuleren door wat DSSC omschrijft als:

> *"Compliance with a set of rules to support decision-making parties in performing their risk assessment to determine the level of trust. This can be verified through a technology framework that provides information on transparency, security, controllability, and interoperability." (DSSC, 2024)*

Dit betekent dat het opzetten van **een governancestructuur en framework de allereerste stap is bij de implementatie van een health data space**. De oprichters van de data space zullen enerzijds het speelveld aan beleidsondersteunende regels waarbinnen haar participanten opereren moeten **bepalen**, en anderzijds een aantal technologische middelen moeten inschakelen om deze **regels af te dwingen.** De eerste van deze twee assen wordt ook wel het **governance framework** genoemd – het geheel aan interne regels, processen, vereisten, procedures en principes die de dagelijkse werking van de data space ondersteunen. Daarnaast moet men ook voorzien dat deze set aan regels (technisch) geïmplementeerd en afgedwongen kan worden. Deze taken vallen onder het zogenaamde **trust framework**, waarin de nodige technische specificaties en voorwaarden ter implementatie en operationalisering gedefinieerd worden (DSSC, 2024). Het trust framework maakt doorgaans deel uit van het technische en architecturale luik en is dus out of scope voor dit hoofdstuk.

Bovenstaande paragraaf illustreert de complexiteit van *governance*, aangezien een succesvolle data space governance-strategie telkens kennis samenbrengt uit verschillende domeinen. Enkel door deze kruisbestuiving kunnen de regels zoals opgesteld binnen het governance framework afgestemd worden op het wettelijk kader (*legal*), de zakelijke afspraken en contracten (*business*) en technisch geïmplementeerd

[374] *Waardecreatie is het proces waarbij producten, diensten of ideeën worden ontwikkeld die tegemoetkomen aan de behoeften van klanten, stakeholders of de samenleving, waardoor er economische, sociale of milieuwinst wordt gerealiseerd.*

worden binnen het trust framework (*technisch*). Een goede data space governance is dus enkel mogelijk wanneer governance als het **kruispunt wordt gezien waarop verschillende expertises samenkomen om middels samenwerking en vertrouwen het kader te scheppen voor waardecreatie op lange termijn.**

7.1.3 Governance binnen de context van het domein gezondheid

Datadeling brengt een aantal complexe vraagstukken met zich mee. Zo is er het lopend maatschappelijk-ethisch debat rond ***data ownership***, waarbij er een kloof is ontstaan tussen de (economische) waarde van het exploiteren van (persoons)data enerzijds, en het gebrek aan zeggenschap over en compensatie voor het gebruik van deze data anderzijds (Vlaamse Overheid, 2024). Dit spanningsveld heeft reeds tot verschillende initiatieven geleid die data ownership terug bij het individu leggen, zoals *Solid* (zie sectie 7.3.5.5 Solid). Binnen de gezondheidscontext profileren bestaande netwerken en ziekenhuizen zich bovendien ook steeds meer als data owner, wat het debat nog complexer maakt.

Daarbovenop zijn thema's zoals de omgang met **gevoelige persoonsdata** en het bewaken van **privacy** nog pertinenter aanwezig binnen het gezondheidsecosysteem dan in de bredere maatschappelijke context. **Transparantie** omtrent correct datagebruik speelt dan ook een cruciale rol in het al dan niet (willen) delen van gezondheidsdata binnen het gezondheidsecosysteem.

Een goed doordachte governance-strategie van een health data space moet dus een (gedeeltelijk) antwoord formuleren op deze complexe context. Daarvoor moet reeds in de **ontwerpfase** van de data space rekening worden gehouden met de relevante maatschappelijke en ethische debatten op vlak van gezondheidszorg. Op basis van deze debatten moeten de **regels** van het governance framework worden opgesteld en **verankerd** in het trust framework en de architectuur. Alle beleidskeuzes, regels, technische designkeuzes en operationele processen moeten daarbij nauwgezet op elkaar **afgestemd** worden zodat een data space structuur kan ontstaan waarbinnen gevoelige gezondheidsdata veilig, transparant en fair gedeeld kunnen worden zonder aan wendbaarheid en efficiëntie in te boeten. Finaal draagt een weldoordachte governance-strategie zo bij tot een health data space met een duidelijke **meerwaarde** voor het ecosysteem én de maatschappij.

7.2 DE BOUWBLOKKEN VAN GOVERNANCE

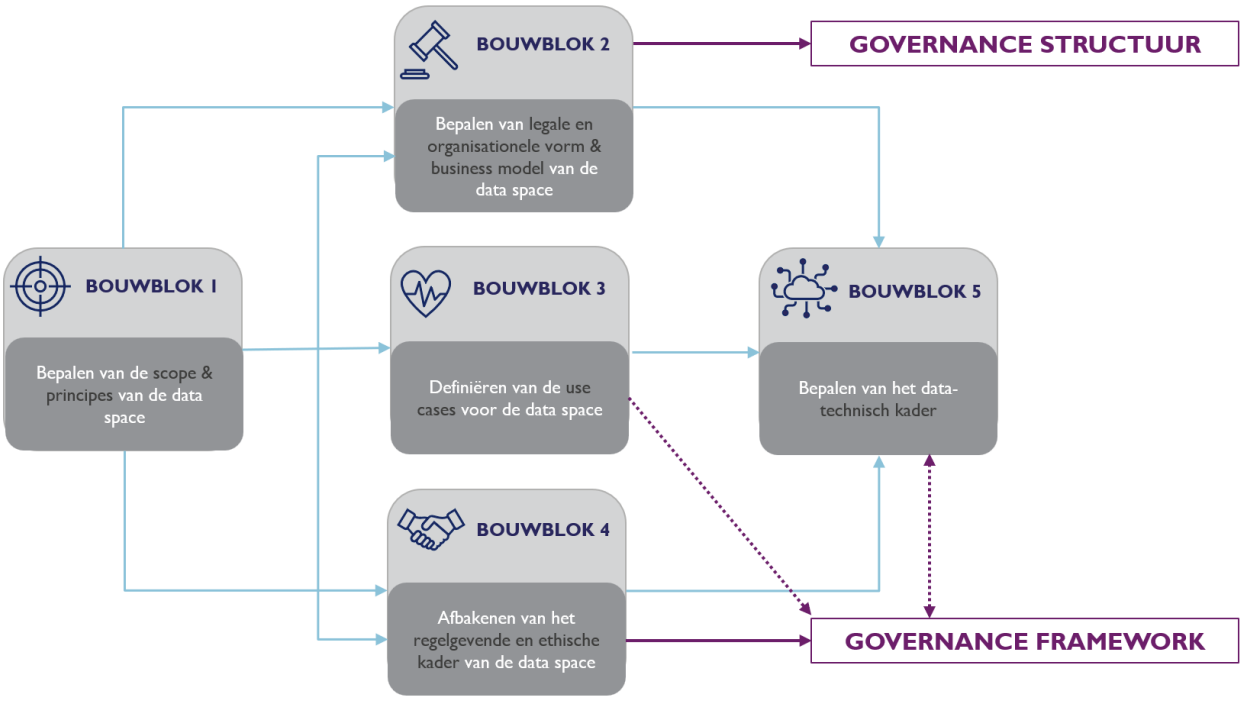
Uit bovenstaande introductie werd duidelijk dat governance een complex gegeven is dat aan erg veel domeinen raakt (denk aan regel- en wetgeving, business-strategie, ethiek, technische componenten ...), en dat bovendien onderhevig is aan de complexiteit van de gezondheidscontext.
De onderzoeksvraag ***"hoe moet een governance structuur en governance framework eruit zien in een health data space?"*** werd daarom beantwoord door een continue wisselwerking tussen desk research enerzijds en validatie met verschillende partners uit het ecosysteem anderzijds.

Tijdens de desk research werden een aantal reeds bestaande governance frameworks en structuren binnen data spaces en andere datadelingsinitiatieven in Vlaanderen, België en Europa onderzocht (zie bijlage 6.A.). In het merendeel van de gevallen ging het om data spaces die niet aan het gezondheidsdomein gerelateerd zijn. De onderzochte structuren en frameworks varieerden van reeds gerealiseerde, feitelijke structuren tot louter academische oefeningen (zie ook sectie 7.3.5 Alternatieve governance structuur en keuzes).
DSSC bleef, net als voor de rest van dit vooronderzoek, de belangrijkste (theoretische) bron van informatie.

Op basis van de gemaakte analyses, werden een aantal uitdagingen en best practices gedistilleerd die systematisch afgetoetst werden bij het health ecosysteem of gezondheidsecosysteem of kortweg *ecosysteem*. Dit ecosysteem omvat een breed scala aan stakeholders die gericht zijn op het bevorderen van toegankelijkheid, kwaliteit en efficiëntie in de gezondheidszorg. Deze gesprekken leverden ook informatie op omtrent de belangrijkste actoren en stakeholders binnen het gezondheidsecosysteem, wat de go-to-market strategie mee kon voeden (zie hoofdstuk 10 Go-to-marketstrategie - Roadmap - Actieplan).

Finaal werden de inzichten uit de desk research en de validatieoefening gebundeld in **zes thematische governance bouwblokken**. Deze bouwen verder op het stappenplan zoals voorgesteld door DSSC (DSSC, 2024), maar diepen het verder uit **aan de hand van gerichte vragen of keuzeopties** die tegemoetkomen aan de relevante vraagstukken binnen het gezondheidsecosysteem. Door deze bouwblokken (en de bijhorende vragen) te toetsen aan een aantal relevante potentiële partners voor een health data space, kon uiteindelijk ook een voorstel geformuleerd worden tot een relevante governance structuur en framework.

Hieronder gaan we dieper in op elk van de verschillende bouwblokken die nodig zijn om *governance in een health data space* te installeren. Voor elk bouwblok wordt kort geschetst wat voor type onderwerpen en vragen (of keuzeopties) erin aan bod komen, en wordt vervolgens de vertaalslag gemaakt naar de feedback die vanuit het ecosysteem werd gegeven. Deze feedback blijft hier steeds theoretisch en capteert enkel de wensen en verwachtingen van het ecosysteem, los van hoe toepasbaar of realistisch deze zijn. Voor een meer concrete suggestie naar wat de health data space finaal zou kunnen aanbieden, verwijzen we graag naar de hoofdstukken 7.3 Governance structuur van een health data space en 7.4 Governance framework van een health data space.



Figuur 11: De relaties tussen de governance bouwblokken

7.2.1 Bouwblok 0: Conceptueel ontwerp

Nog voor men kan starten met een data space, moet men zich ervan verzekeren dat de mogelijke data space actoren dezelfde taal spreken. Door op voorhand een overeenkomst te hebben omtrent de gebruikte terminologie en concepten, kunnen latere discussies vermeden worden. Deze preliminaire "*stap 0*" dient dus om de **concepten en definities binnen de data space vast te leggen met de relevante partners**.
Het is een voorbereidende - maar essentiële – stap die idealiter **resulteert in een glossary** (of lexicon), waarin alle termen verankerd worden. Binnen de context van dit vooronderzoek werd een aanzet gedaan naar een bruikbare glossary (zie hoofdstuk **Fout! Verwijzingsbron niet gevonden.**). Deze kan in latere fases van het onderzoek verder uitgebreid en verdiept worden. Voor de rest van dit hoofdstuk worden de relevante definities en termen omtrent governance steeds gekaderd in de inleidende teksten zelf.

7.2.2 Bouwblok 1: Scope en principes

De eerste echte stap bij het oprichten van een data space is het definiëren van de **strategische richting**. Dit bouwblok consolideert vragen omtrent de missie en visie van de data space, de **scope** die men ambieert, de **meerwaarde** die de data space brengt voor het ecosysteem en de **principes** die centraal zullen staan. In aanvulling wordt ook de toegevoegde waarde die de data space heeft om deze te bereiken geformuleerd. Door deze 'rode draad' van in den beginne duidelijk te omschrijven, kan men toekomstige beslissingen omtrent het bestuur en de werking van de data space hier consequent op enten.
De strategische lijn kan zo doorgetrokken worden naar het businessmodel, de organisatorische structuur, de legale en operationele regels en processen, en de data-technische designkeuzes die in de volgende bouwblokken aan bod komen.

7.2.2.1 Missie, visie en scope volgens het ecosysteem

De visie stipuleert waarom de data space bestaat. Voor het ecosysteem is dit helder: de data space moet voor zowel het individu als de maatschappij een verbeterd **welzijn** en een hogere kwaliteit van preventieve en curatieve **gezondheidszorg** realiseren. Ze kan dit doen door betere **zorg**, **onderzoek** en **beleidsbeslissingen** te ondersteunen, die gebaseerd zijn op inzichten gegenereerd uit de **decentrale** en **transparante** datadeling tussen gezondheidsactoren. Dit leidt tot gepersonaliseerde zorg, snellere innovatie en een effectiever beheer van de volksgezondheid. Daarbij wordt ook verwezen naar de voordelen van data space technologie, die toelaat om deze datadeling met respect voor ethisch-legale en technische kwesties, zoals data **ownership, privacy** en nutteloze duplicaten van data, te laten plaatsvinden.

De **scope** legt de krijtlijnen vast waarbinnen de visie gerealiseerd kan worden. Hier stelt het ecosysteem duidelijk dat de data in een health data space ingezet moeten worden voor **zorgkundige**, **wetenschappelijke of beleidsmatige doeleinden**. Dit houdt in dat zorgverleners, zorginstellingen, overheidsinstanties, onderzoeks- en onderwijsinstellingen, patiënten en burgers gezien worden als stakeholders in een health data space. Een finaliteit die op eender welke manier **discriminatie of polarisatie** in de hand werkt is een absolute 'no go'.

Rond het **commercieel** gebruik van gezondheidsdata zijn de meningen meer verdeeld. Hierbij blijkt de specifieke finaliteit bepalend te zijn: commercieel gebruik dat raakt aan discriminatie wordt resoluut afgewezen (denk bijvoorbeeld aan het opstellen van duurdere verzekeringspolissen op basis van het aantal zorgbehoevenden in een bepaalde regio), maar commercieel gebruik dat ook beleidsmatige voordelen oplevert, is niet per se problematisch (bijvoorbeeld omdat een cijfergedreven *go-to-market* plan beter kan inspelen op bestaande beleids- en zorgnoden). Commerciële partijen zullen voor hun datatoegang dus steeds op *use case*-basis geëvalueerd moeten worden, en data providers moeten kunnen vertrouwen op een degelijk identificatie- en autorisatiesysteem om die validatie uit te kunnen voeren.

Verder moet de data space in eerste instantie vooral ten dienste van **Vlaanderen** en/of **België** staan, al moeten mogelijkheden op het vlak van cross-border en cross-domein integratie wel van in den beginne voorzien worden. Dit betekent ook dat de data space conform de (EU-)**aanbevelingen** moet worden opgezet, en rekening moet houden met initiatieven als de EHDS of de IDSA, of met regels zoals die rond GPDR, standaarden (bijvoorbeeld OMOP/DCAT) of de FAIR principes.

7.2.2.2 Meerwaarde volgens het ecosysteem

Wanneer men kijkt naar de **meerwaarde** die een health data space kan bieden voor haar ecosysteem, ziet men in de eerste plaats **maatschappelijke voordelen** die de globale gezondheidssector ten goede komen. Zo moet een health data space leiden tot:

> Minder **versnippering** van gezondheidsdata, onder andere door het (opgelegd) gebruik van standaarden.

> Een verbetering van de **kwaliteit**, **beschikbaarheid** en **interoperabiliteit** van gezondheid- en welzijnsdata, en volledigere inzichten uit die data.
> Een verhoogde inzetbaarheid van de data, onder meer door het aanbieden van **services** zoals visualisaties van gecombineerde data waardoor data voor veel stakeholders écht herbruikbaar worden.
> Een toegenomen **datasoevereiniteit**, met waarborg van de **privacy** van persoonsgebonden data, omdat data aan de bron kunnen blijven.
> Meer **transparantie** omtrent het gebruik van data (bijvoorbeeld door de betere registratie van transacties).
> Opportuniteiten om **gezondheid holistisch** te benaderen, enerzijds door data binnen de data space te delen, alsook door te connecteren met andere data spaces. Bijvoorbeeld: een data space die data deelt omtrent fietsgebruik, water- en luchtkwaliteit, de aan- of afwezigheid van groen en industrie, enzovoort, kan een interessante meerwaarde zijn voor gezondheidsinzichten.
> Nauwere **samenwerking** tussen de verschillende zorgactoren en beleidsniveaus (Vlaams, Belgisch, Europees).

Op langere termijn ziet men potentieel ook meer **economische winsten**, onder andere door een toegenomen **efficiëntie** (tijdswinst) en een daling in de **kosten** die gepaard gaan met onderzoek, onder andere via vereenvoudigde administratieve procedures, het gebruik van een gedeelde infrastructuur en services, en een duurzaam samenwerkings- en businessmodel.

7.2.2.3 Principes volgens het ecosysteem

Het ecosysteem wijst herhaaldelijk op de cruciale rol van **vertrouwen** binnen een health data space. De belangrijkste driver hierbij is **transparantie,** waarbij men onder andere een open communicatiestijl aanhoudt en geen informatie achterhoudt. Dit laatste wil niet zeggen dat elk detail aan eender wie gecommuniceerd moet worden, maar wel dat alle *relevante* informatie steeds beschikbaar moet zijn. Zo moeten gegevens omtrent de werking en kosten van de data space, het gebruik van data, en de bestaande data space participanten transparant worden gecommuniceerd. De data provider moet steeds weten welke partijen zijn of haar (geaggregeerde) data hebben verwerkt, met welk doel, etc. Een data consumer moet perfect kunnen achterhalen hoe de dataset tot stand kwam.[375] Samengevat is het motto: *alles transparant delen, zonder te verdrinken in details*.

Verder stelt het ecosysteem nog een aantal bijkomende mechanismes of procedures voor die het vertrouwen in een health data space kunnen bolsteren:

> Procedures voor de omgang met een data-lek of een andere vorm van **vertrouwensbreuk**, bijvoorbeeld bij het oneigenlijk gebruik van de data of de inzichten die eruit voortvloeien.
    - De health data space kan reeds van in het begin een **DPO** (of een ander, gelijkaardig profiel) aanstellen. Voor maximale impact wordt zo'n toezichthoudende functie op elk niveau aangeduid (bij data consumers, providers, prosumers[376] en de data space zelf).
> Een heldere ***code of conduct***[377], die bij toetreding ondertekend wordt, en waarin duidelijke verwachtingen geformuleerd staan.
> Strikte **veiligheidsmaatregelen** en -procedures voor **persoonsgebonden en/of gepseudonimiseerde data**. Deze zijn essentieel om de privacy te garanderen en lopen waar mogelijk via geijkte procedures,

[375] *Het bijhouden (loggen) van dit soort informatie over transacties wordt ook wel 'provenance' (vanuit het perspectief van de data consumer) of 'traceability' (vanuit het perspectief van de provider) genoemd. De exacte definitie van beide termen vindt men terug in het Lexicon (hoofdstuk 13 Lexicon).*

[376] *Een prosumer is zowel consumer als provider.*

[377] *De Code of Conduct capteert een aantal regels, richtlijnen en verwachtingen omtrent 'goed gedrag' van de data space deelnemers. Ze kan in meerdere of mindere mate geformaliseerd zijn, afhankelijk van de keuzes die men binnen het governance framework maakt. Meer details over de Code of Conduct en hoe deze eruit kan zien, vindt men onder 7.4.2.5 Code of conduct.*

zoals bijvoorbeeld die van het **IVC**[378]. Wanneer het gaat over geaggregeerde data, moet er wel meer speelruimte zijn voor **exploratie**.

> Het bewaken van de **neutraliteit** van een health data space, waarbij vooral wordt gesteld dat politieke inmenging en overheidscontrole tot een minimum beperkt moeten blijven. Men wil vooral vermijden dat zorgorganisaties gecontroleerd en beoordeeld worden op basis van data die daar niet voor bedoeld zijn, wat kan leiden tot onjuiste conclusies. Controle op het correct gebruik van data is uiteraard wel een vereiste.

Vervolgens is er nog het thema '**datasoevereiniteit',** dat regelmatig aan bod komt. Waar de datasoevereiniteit van de ***data owner***[379] binnen een data space algemeen gedragen wordt (en zelfs als een leidend principe wordt beschouwd), is het onderwerp **'***datasoevereiniteit van de burger'* voer voor een complexe discussie. Zo zijn alle stakeholders zich bewust van de rechten van de burger als (mogelijke data) owner, en toont het ecosysteem de (theoretische) bereidwilligheid om een soort opt-out voor het gebruik van hun data te voorzien. Anderzijds weerklinkt ook de bezorgdheid dat het maatschappelijk belang moet kunnen primeren op de individuele rechten. Hierbij wordt verwezen naar de nood aan volledige en representatieve datasets om degelijk beleid te kunnen voeren. Men zou daarom kunnen vertrekken vanuit een model volgens het *glass-breaking principe*: uitgaan van de rechten van het individu (opt-out), maar toestaan dit te doorbreken wanneer de maatschappelijke waarde primeert.

Tot slot benadrukt het ecosysteem het belang van **inclusiviteit** als een kernprincipe, waarbij gestreefd wordt naar het zoveel mogelijk vermijden van uitsluiting van bepaalde groepen of individuen; hoe dit in de praktijk gerealiseerd moet worden, blijft echter onduidelijk.

7.2.3 Bouwblok 2: Juridische en organisatorische vorm

Dit bouwblok definieert de **organisatorische en juridische vorm** (of entiteit) die de data space zal aannemen bij oprichting. Om deze vorm te bepalen, moet rekening worden gehouden met de uitgezette strategie (zie bouwblok 1), en met eventuele wettelijke en zakelijke doelstellingen en verplichtingen. Zaken zoals het gekozen **business model** en de beoogde **financiering** hebben bijvoorbeeld een impact op de keuze voor een *for-profit* of een *non-profit* entiteit.

Daarom wordt in dit bouwblok ook nagedacht over zakelijke thema's zoals de (kern)diensten die de data space in-house dan wel extern wil leveren, de financieringsbronnen en de compensatie die participanten al dan niet zullen betalen (of ontvangen) voor hun dataproducten of -diensten.

Andere factoren, zoals de al dan niet tijdelijke of permanente aard van de data space en haar plaats van incorporeren, zullen van invloed zijn op (onder andere) het wettelijk kader waarbinnen de data space zich zal begeven, en bepalen mee de **rapporteringsverplichting** en **vereisten op vlak van representatie**. Deze zullen op hun beurt belangrijk zijn voor het vormgeven van de (**minimale) governance structuur** en het type governance-organen dat de data space zullen besturen. Meer uitleg over de governance structuur en een voorstel tot hoe deze er finaal zou kunnen uitzien, vindt men terug onder hoofdstuk 7.3 Governance structuur van een health data space.

Het moge duidelijk zijn dat de vraagstukken en keuzeopties die in dit bouwblok aan bod komen, **grote implicaties hebben voor het verdere bestuur van de data space**, zowel op wettelijk, zakelijk als organisatorisch vlak. Dit bouwblok is cruciaal voor het verdere ontwerp van de data space en haar governance structuur en is erg afhankelijk van de beslissingen die de toekomstige stichtende partners zullen nemen. In die zin zullen veel van de voorgestelde suggesties vanuit het ecosysteem pas finaal in de weegschaal kunnen worden gelegd wanneer deze stichtende partners gekend zijn.

---

[378] *Informatieveiligheidscommittee. Aangifte bij (en evaluatie door) het IVC is verplicht voor toegang tot persoonsgebonden data in de gezondheidssector. Zie ook 6.2.4.9* IVC – Beraadslaging.

[379] *Zie ook 6.2.10.4 IE-rechten in de EHDS aangaande het begrip 'data owner'.*

7.2.3.1 Organisatorische vorm volgens het ecosysteem

DSSC definieert drie grote vraagstukken die mee vorm geven aan de finale opties voor de juridische en organisatorische vorm van een data space (DSSC, 2024). Deze kan men samenvatten als:

> Maakt de data space deel uit van een bestaande entiteit of een bestaand initiatief, of is het een op zichzelf staande entiteit?
> Is de data space een tijdelijke entiteit of wordt het een permanente entiteit?
> Is de visie en missie van de data space gericht op algemeen maatschappelijk nut of op winst?

Door deze vragen te beantwoorden en de bijhorende beslissingsboom te volgen, kan men de opties voor de 'ideale' structuur voor een data space bepalen[380]. Binnen het ecosysteem heerst eensgezindheid betreffende de tweede dimensie: de health data space moet vertrekken vanuit de ambitie een **permanent en duurzaam initiatief** te zijn. Op korte termijn kan men eventueel starten vanuit een tijdelijke en informele structuur, gebaseerd op onderlinge afspraken en goodwill, maar ook dan moet er al van in het begin een duidelijke **roadmap** op tafel liggen richting een permanent (en dus wettelijk verankerd) initiatief.

Het eerste vraagstuk is iets moeilijker te beantwoorden. Zo ziet men voor- en nadelen in zowel het aansluiten bij een bestaand initiatief als in het opzetten van een nieuw initiatief. Bij aansluiting bij een **bestaand initiatief** (zoals bijvoorbeeld de Vlaamse Smart Data Space, in sectie 7.3.5.1 Vlaamse Smart Data Space (VSDS) & Vlaamse Water Data Space (VWDS)) kan men terugvallen op de reeds bestaande governance structuur en framework, en hoeft men die enkel te verfijnen in functie van de noden van het gezondheidsdomein. Deze optie gaat er uiteraard vanuit dat er geen al te grote discrepanties bestaan tussen de heersende noden en verwachtingen. Het alternatief, dat door de meerderheid van de gesproken ecosysteempartners wordt gedragen, omhelst het opzetten van een **nieuwe entiteit**. Het voordeel is dat de nieuwe health data space dan maximaal onafhankelijk kan zijn (onder andere van politieke invloeden), en naar eigen goeddunken kan worden beheerd. Belangrijk voor het ecosysteem is wel dat het verder bouwt op reeds bestaande (sterke) netwerken. Op die manier kan het **reeds opgebouwde vertrouwen** optimaal benut worden. Het laatste vraagstuk (*not-for-profit* of *for-profit*) blijkt meteen ook het meest verdelend te zijn, onder andere door onzekerheden binnen de wetgeving[381] en het te verwachten financieringsmodel voor een (health) data space[382].

7.2.3.2 Financiering en businessmodel volgens het ecosysteem

De meeste bevraagde partijen verwachten dat de ontwikkeling en installatie van een health data space een **grote initiële investering** zal vragen, die de individuele (stichtende) leden niet zullen willen of kunnen dragen. Er wordt dus verwacht dat de **overheid** zo'n initiatief (alleszins in eerste instantie) **financiert**. Dit wordt verder beargumenteerd vanuit de visie dat de overheid ook grote winst kan halen uit het goed functioneren van een health data space, onder andere via betere beleidsbeslissingen (zie ook sectie 7.2.2.1 Missie, visie en scope volgens het ecosysteem).

Op termijn ziet men de health data space als een **zelf-bedruipend systeem** functioneren. De grootste kosten zullen voornamelijk liggen bij de operationalisering (inclusief governance), en het onderhoud van de infrastructuur en connectoren. Deze kosten kunnen voor de data space worden gecompenseerd door

[380] *DSSC stelt uiteraard enkel een abstractie van de opties op Europees niveau voor, en gaat niet dieper in op de verschillende mogelijke nationale juridische entiteiten. Binnen dit project werd wel dieper ingegaan op de verschillende nationale opties, die ook doorsproken werden met het ecosysteem. Op basis van deze legale en contextuele input, werd uiteindelijk een voorstel geformuleerd (zie 7.3.4* Voorstel: governance structuur*).*

[381] *In de huidige wetgeving lijken er momenteel geen regels te zijn die deelname van commerciële partners of het commercialiseren van gezondheidsdata verbieden, maar deze wetgeving is een werk van voortschrijdend inzicht. Zo valt niet uit te sluiten dat dit op termijn wijzigt.*

[382] *Een belangrijke vraag hierbij is of Europa de financiering van een nationale Health Data Space verplicht zal maken om in de noden van de EHDS te kunnen voorzien.*

middel van lidmaatschapsbijdragen, datatransactiekosten, servicekosten en projectfinanciering. Voor de prosumers kunnen de kosten deels worden gecompenseerd door, onder andere, de behaalde efficiëntie-winsten. Door het business model van de data space hierop te enten, kan men de continuïteit garanderen wanneer de eventuele overheidssubsidies op termijn opdrogen.

Bovenstaand model, waarbij men van een gesubsidieerde financiering naar een zelf-bedruipend model evolueert, is echter nog vaag. Het exacte **verdienmodel** dat hiervoor gerealiseerd moet worden, blijkt nog erg moeilijk vast te pinnen. Verschillende opties worden op tafel gelegd:

- ***Betalen per gebruik*** (bijvoorbeeld per datatransactie)
- ***Lidmaatschap of vaste kost***: dit kan al dan niet via een getrapt model, waarbij verschillende types prosumers een verschillend tarief betalen voor gebruik van de data space. De voorkeur gaat daarbij uit naar gratis gebruik voor onderzoeks- en beleidsinstellingen en betalend gebruik voor commerciële partijen.
- ***Betalen voor (value-added) diensten***: de prosumer kan tegen betaling gebruik maken van *bijkomende third-party* diensten en applicaties zoals bijvoorbeeld API's, transformaties, visualisaties ... Dit model kan ook getrapt aangeboden worden, met verschillende tarieven voor verschillende types users.
- ***Quid pro quo***: data space participanten kunnen gratis gebruik maken van de data space indien men zowel data provider als data user is. Uit de gesprekken met het ecosysteem blijkt echter dat een aantal partners slechts een beperkte bereidheid tonen om gratis data te delen. Men verwacht een eerlijke (financiële) compensatie voor de verstrekte data assets. Deze optie lijkt daarom moeilijk realiseerbaar of combineerbaar met de andere pistes.

Elk van de voorgaande opties heeft zijn eigen voor- en nadelen, maar het is duidelijk dat geen enkele piste op zich een eenduidig antwoord biedt op de vraag '*hoe moet een data space zichzelf financieren'*.
Finaal zal het antwoord waarschijnlijk in een combinatie van verschillende verdienmodellen te vinden zijn.

Er is wél eensgezindheid dat de kerndoelstelling van een health data space het **maatschappelijk belang** aangaat en niet het nastreven van een winstoogmerk. De voorkeur lijkt daarom naar een **not-for-profit** juridische vorm te gaan, met de focus op niet-financiële waardecreatie in de plaats van het uitkeren van winsten[383]. Het grootste vooredeel van (te starten met) een not-for-profit juridische vorm ligt in de creatie van **vertrouwen** naar de burger en partnerorganisaties toe. Bovendien staat een non-profit noch subsidiering van de overheid (belangrijk in de opstartfase), noch sponsoring uit de privésector in de weg[384]. De keuze voor een non-profit zou ook geen negatieve invloed hebben op het al dan niet mogen toetreden van commerciële partners en staat het financieel valoriseren van datatransfers (voorlopig) ook niet in de weg.

Voor welk verdienmodel of welk type legale entiteit men finaal ook opteert, het ecosysteem beklemtoont dat de informatie en details rond financiële transacties steeds **transparant** raadpleegbaar moeten zijn.

7.2.3.3 Rol van de overheid volgens het ecosysteem

De eventuele politieke betrokkenheid in een health data space wordt niet uniform geëvalueerd door het hele ecosysteem. Bepaalde overheidsinstanties zien voor zichzelf een kleine of grote rol weggelegd in (het oprichten van) een health data space. Voor een groot deel van het ecosysteem is het echter essentieel dat een health data space zo **apolitiek** mogelijk wordt beheerd, en dat een overheidsinstantie niet de enige of dominante drijvende kracht achter de organisatie is. Er wordt immers gesuggereerd dat instanties zoals het RIZIV, overheidsdepartementen en andere organisaties niet per se 'neutraal genoeg' zijn, wat gevoelens van weerstand oproept tegen hun mogelijke rol als exclusieve of primaire leider van een health data space.

---

[383] *Opmerking: zoals in 6.2.2 Vennootschapsrecht al aangehaald, staat de legale vorm for-profit of not-for profit van de data space los van die van haar participanten. Onafhankelijk van welk van legale vorm gekozen wordt, kunnen volgens de huidige wetgeving zowel for-profit als not-for-profit organisaties toetreden tot de data space.*

[384] *Een voorbeeld van een succesvol datadelingsinitiatief met sponsoring uit de privé-sector is het open dataplatform van de Port of Antwerp-Bruges (https://www.portofantwerpbruges.com/onze-haven/open-dataplatform)*

Tegelijkertijd is er wel behoefte aan **vertegenwoordiging** vanuit politieke instanties, zoals het Departement Zorg, om stroomlijning en efficiëntie te bevorderen. De overheid kan daarom optreden als één van de (stichtende) leden van de health data space, maar niet als enige dominante partij. Binnen die context gaat de voorkeur dan ook uit naar een eventuele politieke vertegenwoordiging in de **Algemene Vergadering** (het besturend orgaan), maar met een **raadgevend** (en geen stemgerechtigd) mandaat[385].

Naast deze sturende rol zou de overheid ook beperkte inspraak kunnen krijgen in het opstellen van het **operationeel kader**, en het financieel en zakelijk beheer van de data space (al wordt dit laatste niet unaniem gedragen). Tegelijkertijd is men zich er wel van bewust dat een overheid die instaat voor de **initiële financiering** (zie sectie 7.2.3.2 Financiering en businessmodel volgens het ecosysteem), ook een zekere rol zal willen hebben in het financiële beleid.

Over de rol van de overheid als **controleorgaan** voor het **correct gebruik** van data, zijn de meningen sterk verdeeld. Voor sommigen is de overheid de enige bespreekbare partner als controleorgaan. Andere partijen verkiezen dan weer dat controles gebeuren door een **onafhankelijke partij**, en net niet door de overheid. Een overheidsvertegenwoordiging in het superviserend orgaan zou namelijk tot een gebrek aan vertrouwen kunnen leiden. Er wordt immers meermaals aangehaald dat controle op data die daar niet toe bestemd is, mogelijk aanleiding kan geven tot verkeerde conclusies.

Een extra vereiste voor het ecosysteem is dat er **samenwerking is tussen de verschillende bestuurlijke niveaus** (Vlaams, Belgisch en Europees) om te allen tijde een verdere versnippering van de data en datadelingsinitiatieven tegen te gaan. Hierbij wordt een aantal keer verwezen naar een waterval, waarbij informatie en regelgeving vanop het ene bestuurlijke niveau naar het andere doorstroomt. Tegelijkertijd is er ook een wens om voldoende **regionale autonomie** te bewaren zodat men wendbaar kan blijven en kan inspelen op eventuele verschillen in de inhoudelijke regionale vraagstukken en de data die daarvoor nodig is.

Om die wendbaarheid verder te ondersteunen, acht men het ook nodig dat er ruimte is om **bottom-up** use case initiatieven op te zetten. De bezorgdheid leeft immers dat door de complexiteit van onze landstructuur het te lang zal duren voor er overheidsmatig een voldoende solide basis is voor een health data space en dat kostbare tijd zo verloren zal gaan. Daarom wordt gekeken naar een **hybride aanpak**, waarbij elk vanuit zijn eigen framework werkt en snelheid maakt, maar wel steeds rekening houdt met de beslissingen en initiatieven op de andere niveaus. Zo kan men gebruik maken van synergieën tussen de verschillende niveaus en dubbel werk vermijden.

Als conclusie kunnen we dus stellen dat het ecosysteem een health data space ziet als een initiatief dat vooral breed gedragen moet worden door het gezondheidsecosysteem, en waarin de overheid bij voorkeur slechts een beperkte, **ondersteunende rol** vervult.

7.2.3.4 Rol van andere instanties volgens het ecosysteem

Hoewel de **HDA** (zie ook 3.4.2.1 HDA) in zo goed als elk gevoerd gesprek naar boven komt als een niet-te-ontbreken speler in de health data space, geraakt men niet echt uit aan de concrete invulling van hun rol. Zo ziet men de HDA als een:

- (meta)data broker.
- partij die de brug vormt tussen de EHDS naar de lokale health data space. Wat dit specifiek inhoudt, is echter onduidelijk voor het ecosysteem.
- lid van het superviserend orgaan, waarbij het een soort van *data access committee*-rol zou opnemen (onder andere via het goedkeuren van data requests en data sharing agreements), en toegang tot de data space zou controleren en autoriseren op basis van legale en ethische regels.
- verantwoordelijke voor de training en onboarding tot de data space.

[385] In de statuten kan worden vastgesteld dat verschillende leden verschillende (stem)rechten hebben. Zo kan geëxpliciteerd worden welke partij stemrecht heeft, en welke niet.

Het moge duidelijk zijn, ook voor het ecosysteem, dat de HDA al deze verwachte rollen niet daadwerkelijk zal kunnen en willen opnemen.

Voor **Athumi** (zie ook 3.4.3.1 Athumi) ziet men vooral een rol weggelegd als **clearing house**. Op korte termijn verwacht men van een clearing house dat die *logging* en verificatie van de transacties opneemt, alsook het contractbeheer. Op lange termijn kan daar facturatie bijkomen, al kan deze rol ook door een andere service provider ingevuld worden. Voor sommige partners staat een clearing house er ook voor in dat ex-deelnemers (bijvoorbeeld na een gedwongen offboarding voor het overtreden van de regels) geen feitelijke datatransancties meer kunnen uitvoeren. Duidelijk is wel dat het ecosysteem onvoldoende kennis heeft van wat een clearing house is, welke functie het uitvoert, en hoe Athumi juist in dit plaatje past.

Omtrent **eHealth** (zie ook 7.3.5.4 eHealth) zijn de meningen verdeeld. Gezien de bekendheid van eHealth in het gezondheidsecosysteem, en het feit dat het opereert via een decentraal systeem, lijkt het de ideale voorloper van een health data space te zijn. In die hoedanigheid zou eHealth bijvoorbeeld een rol kunnen opnemen in het bepalen van de **architecturale** keuzes, **interoperabiliteit** of **datastandaarden**[386].
Anderzijds wekt de nauwe verweving tussen eHealth en het politiek landschap ook veel weerstand op.

Een belangrijke rol in de health data space is weggelegd voor **de (gezondheids)community**. Dit zijn de pioniers in het ecosysteem die nu al datadelingsinitiatieven opzetten en waar een gezonde vertrouwensbasis reeds aanwezig is. In deze community zitten (vertegenwoordigers van) zorgverstrekkers, commerciële partners, universiteiten, organisaties zoals Sciensano en vertegenwoordigers van patiëntenorganisaties. Het ecosysteem verwacht dat deze community **vertegenwoordigd** is op de **hoogste governanceniveaus** binnen de health data space en een actieve rol kan opnemen in het bepalen van haar **strategische** koers en **operationele** werking.

Tot slot werd duidelijk dat de rol van een aantal bijkomende partijen, zoals Digitaal Vlaanderen, de Datavindplaats, healthdata.be, het Informatieveiligheidscomité of SOLID nog niet duidelijk is.
Ze zijn *initieel* dan ook niet top-of-mind voor het gezondheidsecosysteem.

7.2.3.5 Rol van de burger volgens het ecosysteem

Het ecosysteem is het niet eens over het vraagstuk of individuele burgers moeten kunnen deelnemen aan de health data space. Enerzijds wil men toegang tot gezondheidsdata zo **laagdrempelig** mogelijk maken voor iedereen die iets wil doen met (geaggregeerde) data. Zo gaan er stemmen op om de toegang voor burgers gratis te maken. Anderzijds ziet men een grote **complexiteit** in het beheren en controleren van de toegang en het beheren van het gebruik van individuele burgers.

7.2.3.6 Governance structuur volgens het ecosysteem

Over de structuur en organisatie van de health data space bestaan verschillende visies, maar in essentie kunnen deze herleid worden tot minimaal onderstaande organen, die samen de **Governance Authority** moeten vormen. De uiteindelijke samenstelling en representatie van de organen hangt deels ook samen met het type vennootschap dat wordt gekozen voor de data space (zie 6.2.2 Vennootschapsrecht).

> Een ***beslissingsorgaan,*** dat strategische en beleidsbeslissingen neemt. Het bepaalt de strategie en visie, de principes, het business- en financieringsmodel, etc. Dit orgaan is multidisciplinair, **representatief** voor het gezondheidslandschap en tegelijk ook beperkt in zijn aantal leden om de **werkbaarheid** van het orgaan te optimaliseren. Zo kan dit bestaan uit de stichtende leden, een afvaardiging uit het ecosysteem en eventueel een afvaardiging uit de politiek (al moet men er volgens de meesten zeker over waken dat de health data space zo apolitiek mogelijk blijft, en dat het zwaartepunt vooral bij de

[386] *Het uitzetten van richtlijnen voor deze onderwerpen behoort overigens tot een van de kerntaken van eHealth.*

gezondheidsactoren zelf ligt). Bij voorkeur is de samenstelling van dit orgaan **interfederaal**, aangezien gezondheidsdata dat ook zijn. In het geval van **crisissituaties** mag het sturend orgaan kordaat de nodige beslissingen nemen, eventueel zonder langdurig voorafgaand overleg en consensus (zoals dit ook het geval was tijdens de coronacrisis).

> Een ***operationeel* orgaan,** dat de uitvoerende taken op zich neemt. Het operationeel orgaan moet een **mandaat** krijgen van het beslissingsorgaan om haar taken uit te voeren. Op korte termijn zal de health data space eerder klein zijn en kan een enkel orgaan (bestaande uit een of meerdere personen) alle uitvoerende taken opnemen. Naarmate de data space groter wordt, zal men de operationele taken meer moeten verdelen. Volgens het ecosysteem kan men - op langere termijn – dan ook **werkgroepen** voorzien, die elk een specifieke taak opnemen. Zij bestaan uit experts met domeinkennis die enerzijds de beslissingen van het sturend orgaan uitvoeren, en anderzijds advies kunnen formuleren (vanuit een gezamenlijke visie) naar het sturend orgaan toe. Eventueel kan men, in het scenario van meerdere, grote werkgroepen, nog een '**multidisciplinaire raad'** als tussenlaag introduceren, waarin een afgevaardigde of 'liaison' uit elke werkgroep zetelt.

> Een ***superviserend orgaan***, dat verantwoordelijk is voor de autorisatie en toetredingsvoorwaarden[387] en dat toeziet op het eigenlijk gebruik van de data. Dit orgaan buigt zich ook over ethische kwesties en heeft een adviserende rol inzake conflictresolutie, al zijn het in eerste instantie de betrokken partijen zelf die geschillen onderling dienen op te lossen. Het superviserend orgaan grijpt slechts in het slechtste geval in om bij te sturen. Het superviserend orgaan kan een intern orgaan zijn, maar opereert wel steeds **neutraal** (*in casu* mag er geen belangenvermenging zijn tussen haar zetelende leden en de use case of het dispuut in kwestie). Het orgaan is **multidisciplinair** (met leden die kennis hebben rond het wetenschappelijk domein, het legale en ethisch domein, etc.). Het kan zich voor bepaalde complexe vraagstukken steeds laten bijstaan door externe partijen met een meer diepgaande expertise, zoals bijvoorbeeld een ethisch comité voor vraagstukken rond ethische dilemma's. De taken van dit superviserend orgaan zullen op korte termijn eerder opgenomen worden door het operationeel orgaan, maar op middellange termijn lijkt een apart orgaan wenselijk om de neutraliteit verder te garanderen.

Waar er redelijk veel unanimiteit bestaat over de inhoudelijke governancefuncties en -organen, blijken de onderlinge relaties en verhoudingen iets minder duidelijk. Zo gaan er stemmen op die de voorkeur hebben voor een meer klassieke **hiërarchische structuur** (met als grote voordeel dat er meer duidelijkheid is) tot een **niet-hiërarchische** '*circulaire'* structuur, waarin alle organen eigenlijk op eenzelfde hiërarchisch niveau staan en samen tot consensus moeten komen (wat uiteraard tot nog grotere buy-in zou kunnen leiden). Een deel van het ecosysteem ziet in deze laatste optie een manier om meer gewicht te geven aan de prosumers en research community binnen het beslissingsproces.

7.2.4 Bouwblok 3: Use case definitie en selectie

De waarde van een data space wordt grotendeels bepaald door de waarde van de use cases die erin aan bod komen. DSSC omschrijft een use case als de plek waar "*two or more participants use a data space [...] to create value (business, societal or environmental) from data sharing*" (DSSC, 2024). Dit leidt tot een netwerkeffect waarbij een data space die goede use cases kan voorleggen, meer waarde kan bieden aan potentiële participanten, waardoor het meer participanten kan aantrekken die op hun beurt goede use cases op tafel kunnen leggen.

[387] *Het superviserend orgaan is verantwoordelijk voor controle op het naleven van de toetredingsvoorwaarden. De voorwaarden zelf zijn vastgelegd door het beslissingsorgaan. De beslissing of er dan feitelijke toegang wordt verleend tot een data asset, ligt bij de data space participant zelf (soevereniteitsprincipe).*

Om dit zelfversterkend netwerkeffect te realiseren, moet een data space dus *a priori* over twee aspecten nadenken: de **voorwaarden, vereisten en beperkingen** waaraan de use cases moeten voldoen enerzijds, en de **meerwaarde** die het als data space kan bieden **aan participanten** anderzijds.

Om deze twee aspecten te kunnen definiëren, haakt dit bouwblok in op de twee voorgaande bouwblokken. Zo geven de gekozen scope en principes uit bouwblok 1 mee vorm aan de criteria voor use case selectie en de definitie van de niet-financiële meerwaarde voor participanten, en bepaalt het high-level business model uit bouwblok 2 mee hoe eventuele monetaire of financiële waarde vertaald kan worden naar de participanten. Door deze zaken reeds vóór de oprichting van de data space holistisch te benaderen, kan men meer controle behouden over waar en hoe waardecreatie zal gebeuren.

7.2.4.1 Voordelen van een health data space voor use case participanten volgens het ecosysteem

De **datasoevereiniteit** van de data provider en het beschermen van de **privacy** zijn twee vaak terugkomende voordelen die een data space aan haar use case participanten kan bieden. Verder zou een data space ook tot meer **administratieve efficiëntie** moeten kunnen leiden, onder andere omdat data-aanvragen gecentraliseerd worden. Daardoor zullen meer databronnen **beschikbaar** zijn voor organisaties en ontstaat meer ruimte voor **innovatie**. Verder kan een data space ook **standaardisatie en interoperabiliteitsvereisten** opleggen aan haar gebruikers, waardoor use cases op een hogere **datakwaliteit** kunnen vertrouwen, wat dan weer tot meer potentieel **hergebruik** leidt.

Opvallend is dat de meeste van deze voordelen eerder data-technisch of operationeel van aard zijn. Financiële **winst** is niet top of mind wanneer men het over de mogelijke voordelen voor use cases heeft. Zoals eerder aangehaald, heeft dit ook te maken met de overtuiging dat winst slechts op langere termijn realistisch is: deelname aan een data space vereist immers een zekere datamaturiteit van participanten en het opbouwen hiervan binnen een organisatie *kost* in eerste instantie geld, eerder dan dat het financieel iets oplevert. Bovendien zal data space technologie initieel een extra technische component vormen, boven op de reeds bestaande data exchange platformen, waardoor het initieel eerder *meer* dan minder zal kosten. Het is pas op lange termijn, wanneer de technologie en data meer *matuur* zijn, dat men significante kost- en efficiëntiewinsten voor participanten mag verwachten.

7.2.4.2 Use case criteria volgens het ecosysteem

In lijn met de maatschappelijke focus die ook uit het strategisch luik naar voren kwam, schuift het ecosysteem opnieuw een **maatschappelijke focus** (*the greater good*) en **ethische correctheid** naar voren als use case criteria voor het **gezondheids**- en **welzijnsdomein**. Een use case wordt daarbij alleen maar sterker indien er reeds van in het begin nagedacht werd over het eventueel **hergebruik** van de data of dataproducten in extra use cases.

In eerste instantie wil het ecosysteem de focus leggen op use cases die **geaggregeerde data** gebruiken. Men is er echter van overtuigd dat dit op termijn moet evolueren richting use cases die ook **gepseudonimiseerde data** inzetten, omdat men zo onder andere ook longitudinale analyses mogelijk kan maken.

Het ecosysteem spreekt ook de voorkeur uit om **zo min mogelijk beperkende factoren** op te leggen aan de use cases, zodat zo veel mogelijk initiatieven rond secundair gebruik (zie 2.1.1 European Health Data Space regulering) van gezondheidsdata mogelijk worden (dit uiteraard steeds binnen de context van het heersend wettelijk kader). Zo moet men steeds een open geest bewaren voor use cases die data uit **andere domeinen** wensen te gebruiken, zolang de use case zelf maar ten dienste staat van het maatschappelijk belang van de gezondheidszorg.

Wel vindt het ecosysteem dat er bepaalde criteria rond **datakwaliteit** en **datamanagement** aan de use case verbonden mogen worden. De data space mag namelijk geen “one time data dump” worden en aangeleverde data worden idealiter onderhouden en geüpdatet[388]. Men is er zich echter wel van bewust dat de financiële en organisatorische mogelijkheden van potentiële data space gebruikers dit vandaag (nog) niet (altijd) toelaten. Dit soort criteria leent zich er dan ook toe om geleidelijk aan geïntroduceerd en afgedwongen te worden.

Op korte termijn wil men vooral starten met ***not-for-profit*** use cases om het vertrouwen op te bouwen. Op langere termijn mogen use cases ook een *for-profit* finaliteit hebben. Deze mening wordt gedragen door de meerderheid van de stakeholders.

7.2.5 Bouwblok 4: Data space overeenkomsten en regels

In dit bouwblok wordt het regelgevend kader waarbinnen de data space participanten zullen opereren bepaald. In tegenstelling tot bouwblok 2, waar vooral onderzocht wordt welke externe regulaties van tel zullen zijn voor de data space (zoals bijvoorbeeld de juridische vorm), ligt de nadruk hier op de **intern afgesproken regels, voorwaarden en afspraken** waaraan de data space en haar participanten onderhevig zullen zijn. Dit bevindt zich op twee niveaus: (1) regels met betrekking tot het **toetreden** tot de data space en (2) regels met betrekking tot het uitvoeren van de **use cases**, inclusief datatransfers of het aanbieden van data services.

De keuzes die uit dit bouwblok voortvloeien, vormen de basis van het **governance framework**, of het geheel aan interne regels, processen, vereisten, procedures en principes die de dagelijkse werking van de data space ondersteunen. Dit governance framework geeft op haar beurt richting aan een aantal cruciale oprichtingsdocumenten, zoals bijvoorbeeld de **toetredingsvoorwaarden** zoals geformuleerd in de **accession agreement**. Meer uitleg over het governance framework, de types regels en policies en de accession agreement vindt men terug in hoofdstuk 7.4 Governance framework van een health data space.

Uiteraard zijn de vele types regels, contracten en voorwaarden onderhevig aan de huidige nationale en supranationale wetgeving. Aangezien data spaces nog een relatief nieuwe technologie zijn, en het wettelijk-ethisch kader hierrond nog in volle ontwikkeling is, spreekt het voor zich dat ook dit bouwblok **onderhevig is aan gespecialiseerde en veranderende kennis**. Voor de meest recente en gespecialiseerde kennis verwijzen we daarom naar het relevante hoofdstuk 6 Juridische en ethische principes.

Gezien de specificiteit van het onderwerp en de afhankelijkheid van de keuzes van zowel het heersend wetgevend kader als de uiteindelijke stichtende leden, moet men dit bouwblok vooral intern behandelen. De input vanuit het ecosysteem kan per definitie slechts gelimiteerd en indicatief zijn.

7.2.5.1 Algemeen wetgevend kader volgens het ecosysteem

Het gezondheidsecosysteem heeft weinig helderheid over welke externe wetgeving er van toepassing is. Men kent de term ‘European Health Data Space’ of ‘EHDS’, maar weet niet wat dit concreet betekent voor de praktische implementatie van een health data space op lokaal niveau. Andere wetgevende kaders zoals de Data Governance Act of de AI Act zijn amper bekend. Het scheppen van **duidelijkheid en educatie** hieromtrent kan dus één van de diensten zijn die een data space aanbiedt aan haar deelnemers.
Het ecosysteem benadrukt wel dat **ethische principes** een sleutelrol moeten spelen binnen het governance framework, ook wanneer deze niet expliciet vervat zijn in de wetgeving. Wat ethisch en onethisch gedrag is, dient dan ook verwoord te worden in de toetredingsvoorwaarden voor een data space. Bij voorkeur worden deze opgesteld door een werkgroep bestaande uit experten en eindgebruikers.

[388] *De data provider zou verantwoordelijk moeten zijn voor de volledigheid van de data en dus ook voor o.a. toestemming (consent) van data owners. Dit gaat echter buiten de grenzen van een data space zoals nu (Q4 2024) gedefinieerd.*

Op korte termijn ziet men het (technisch) afdwingen van de interne regels niet haalbaar en vreest men dat dit remmend kan werken op het aantrekken van participanten. Als alternatief kan men partners wel stimuleren een engagement aan te gaan om bepaalde regels (gradueel) toe te gaan passen.

7.2.5.2 Selectieprocedure voor use cases volgens het ecosysteem

Zoals in bouwblok 3 besproken, hanteert men best een aantal op voorhand afgesproken criteria om use cases al dan niet te onboarden tot de data space. De procedure voor hoe die **use case onboarding** kan gebeuren, kan verschillen op korte dan wel lange termijn. Zo kan men er bij opstart voor kiezen de use case onboarding **manueel** te laten verlopen. Een **intern comité** valideert dan of een use case aan de criteria tot onboarding voldoet. Zo'n procedure is uiteraard tijds- en arbeidsintensief, maar staat **controle** toe op de opgestelde principes van de health data space en op de datakwaliteit. Bovendien creëert het in de eerste fase van oprichting van een data space de ruimte om te ontdekken welke additionele principes en use case criteria nog belangrijk zijn voor het ecosysteem.

De meerderheid van het ecosysteem is het er echter over eens dat er zo snel mogelijk moet worden overgegaan naar een **geautomatiseerd** aanvraagproces met zo weinig mogelijk overhead. Deze aanpak zorgt voor meer efficiëntie en snelheid in de aanvraagprocedure.

7.2.5.3 Toetredingsprocedure tot de data space volgens het ecosysteem

Voor de initiële onboarding van een data space participant vertrekt men volgens het ecosysteem idealiter vanuit een **use case**. Men kan via de use case immers achterhalen waarom iemand toegang wenst tot de data space. Dit kan opnieuw via een manueel proces, al gaat de voorkeur ook hier uit naar een zo snel mogelijke overschakeling naar een geautomatiseerd proces (zie 7.2.5.2 Selectieprocedure voor use cases volgens het ecosysteem).

Participanten kunnen echter ook op andere manieren dan een use case deelnemen aan een data space. Zo kunnen zij toegang vragen om bepaalde **(data)services** aan te bieden. Het gaat dan over diensten als cross-platform integraties, integraties met AI-applicaties, datatransformaties, anonimisering en pseudinomisering, data visualisatie, enzovoort. Deze services staan in principe los van een use case. Het aanbieden van data services is echter nog onbekend terrein voor het ecosysteem.

Vooraleer partijen toegang krijgen tot de health data space, moeten zij zich akkoord verklaren met de ***accession agreement* of toetredingsvoorwaarden**. Indien de data space de aanvraag tot toetreding **goedkeurt**, ontvangt de data space participant middels een identificatie- en authenticatieprocedure de benodigde **credentials of access tokens**. Een deelnemer die de **connector** geïnstalleerd heeft, kan zijn token of credential dan gebruiken om **in te loggen** tot de data space.

7.2.5.4 Uittredingsprocedure uit de data space volgens het ecosysteem

Volgens het ecosysteem zijn er (voorlopig) twee scenario's die aanleiding kunnen geven tot beëindiging van deelname aan de data space. Het eerste scenario vindt plaats wanneer een data space deelnemer zich (herhaaldelijk) **niet houdt aan de gemaakte afspraken** uit de accession aggreement of eventuele data sharing agreements. In dit geval kunnen zij, na een of meerdere aanmaningen, gedwongen uit de data space worden gezet op initiatief van de Governance Authority[389]. Deze procedure kan eventueel gekoppeld worden aan een bijkomende boete. Uiteraard kunnen deelnemers aan een data space deze ook steeds **vrijwillig** verlaten. Voor dit scenario zijn er geen duidelijke criteria, en de procedure moet standaard in gang gezet kunnen worden.

[389] *Bij vaststelling van een inbreuk gaat de Governance Authority of haar vertegenwoordiger in eerste instantie in gesprek met de overtredende partij, die de tijd en mogelijkheid krijgt om mitigerende maatregelen te nemen. Enkel indien hier geen gehoor aan wordt gegeven, gaat men over tot een gedwongen exit.*

Het ecosysteem vindt het in dit geval wel cruciaal dat men voldoende rekening houdt met eventuele lopende contractuele verplichtingen naar data consumers of data service providers toe, zodat deze de tijd hebben om een alternatieve (data)leverancier te vinden.

7.2.5.5 Contracten tussen participanten volgens het ecosysteem

De procedure voor het opstellen van contracten tussen deelnemers blijft nog onduidelijk voor het ecosysteem. Wel is het wenselijk dat prosumers **maximaal agency** bewaren over de **inhoud** van de contracten, die eventueel in een door de data space aangeboden **template** gegoten kan worden. Deze templates kunnen evolueren doorheen de tijd. Op korte termijn kan men zich beperken tot een enkele standaard template, maar op langere termijn zou men verschillende templates en/of technologische componenten kunnen bouwen die meer opties aanbieden.

Een van de voordelen die het ecosysteem ziet aan een data space, is de mogelijkheid om de **publicatie** van contracten te beheren via een clearing house. Dit maakt de langdurige consultatie van contracten namelijk mogelijk, waardoor er meer **transparantie** gecreëerd kan worden. Niet alle prosumers willen echter alle contractvoorwaarden publiekelijk maken. Tot op welk niveau van detail deze contracten transparant moeten zijn en voor welke type data space participanten, is dus nog niet uitgeklaard.

7.2.6 Bouwblok 5: Data governance

Een aantal gemaakte keuzes uit de eerdere bouwblokken (zoals bijvoorbeeld de contracten, policies, toetredingsvoorwaarden, on- en offboardingsprocedures, veiligheidsmaatregelen, etc.) zullen ook technisch uitgewerkt moeten worden in de data space. Vooraleer men kan overgaan tot de specifieke implementatie van die technologische oplossingen, moet men eerst nadenken over de **organisatorische implicaties** van de gemaakte keuzes. Daarom wordt in dit laatste bouwblok het data-technisch ontwerp van de data space verkend. Het is een **exploratie** waarin nog niet te diep wordt ingegaan op de technische details. Dat is immers deel van een latere functionele analyse. De focus in dit bouwblok ligt enkel op de data-technische aspecten die **invloed hebben op (andere) governance-gerelateerde keuzes**. Zo wordt er gedefinieerd wie de verantwoordelijkheid neemt op vlak van de **infrastructuur en de value-added services** die de data space wil aanbieden; welke keuzes men moet maken rond het bijhouden van de provenance en de traceability van de data[390]; wordt er geëxpliciteerd hoe men identiteitsverificatie- en management wil organiseren; en worden beslissingen gemaakt met betrekking tot de interoperabiliteit, standaardisatie en het beheer van (meta)data. Dit is namelijk cruciaal om de waarde van de health data space te maximaliseren via het (her)gebruik van data.

Deze inzetbaarheid van data wordt vandaag al ondersteund door heel wat internationale initiatieven, zoals de internationaal gehanteerde **FAIR-data principes**[391]. FAIR is een acroniem voor de vier richtlijnen (findable (vindbaar), accessible (toegankelijk), interoperable (interoperabel) en reusable (herbruikbaar)) die in 2016 opgesteld werden om data providers te begeleiden in het genereren van kwalitatieve data en metadata. Deze ondersteunen de data-technische weg naar meer standaardisatie en interoperabiliteit. Aangezien deze principes in lijn liggen met de ambities en doelstellingen van data space technologie, is het maar logisch dat de FAIR-principes mee de basis zouden vormen voor kwaliteitsvolle (meta)data in een health data space[392].

---

[390] *Provenance en traceability verwijzen naar het opslaan en consulteerbaar maken van 'bewijsmateriaal' rond het gebruik, de origine, de verwerking … van een datatransactie. De exacte definitie van de termen en het onderscheid tussen beide kan men terugvinden in het lexicon (zie hoofdstuk 13).*

[391] *Meer info kan men terugvinden op www.go-fair.org of in 6.2.8.*

[392] *Alhoewel de FAIR-principes waardevolle richtlijnen kunnen bieden voor (meta)datakwaliteit, heeft het geen zin om te streven naar 100% FAIR data, enerzijds omdat dit onrealistisch is, en anderzijds omdat er geen eensgezindheid heerst over wat 'voldoende FAIR' is. We raden daarom aan om FAIR op te nemen in de toetredingsvoorwaarden tot een health data space via een intentieverklaring, waarin een partij zich engageert om zo goed mogelijk de FAIR data principes te hanteren, zonder duidelijke resultaatsverbintenis.*

Naast het gebruik van de FAIR data principes en een goed metadatabeheer, zijn er verschillende andere methoden en technieken die kunnen worden ingezet om de kwaliteit van data te verbeteren. Zo kan een **geautomatiseerde data validatie en/of monitoring** worden geïnstalleerd om de continue gegevensinvoer en -verwerking te controleren op fouten, inconsistenties, ontbrekende waarden of duplicaten.
Ook **AI en machine learning** kunnen worden ingezet voor patroon- en foutendetectie in data. Tot slot kunnen ook **training en bewustwording** een belangrijke rol spelen in het herbruikbaar maken van data. Deze items werden echter niet onderzocht in dit onderzoeksproject en zijn materiaal voor een vervolgproject. Het is echter duidelijk dat al deze aspecten impact kunnen hebben op de governance van een health data space. Door reeds vóór de oprichting van de data space na te denken over deze data-technische aspecten, kan men tijdig anticiperen op toekomstige technische vraagstukken en de eventuele oplossingen ervan ook afstemmen op en integreren in de andere governanceprocessen en -keuzes die men in de overige thematische bouwblokken maakt.

7.2.6.1 Data-technische vereisten volgens het ecosysteem

Er heerst momenteel nog veel onduidelijkheid binnen het ecosysteem wat de data-technische vereisten betreft, aangezien het voor de bevraagde partijen vaak nog onduidelijk is welke technische bouwblokken relevant zullen zijn, en hoe en door wie deze dan beheerd moeten worden. Wel is duidelijk dat de onderwerpen 'identiteits-en autorisatiemanagement' en 'datakwaliteit' twee prangende bezorgdheden zijn die een goed beheer vereisen om vertrouwen te verkrijgen.

Autorisatie en identificatie zijn essentiële onderdelen die voor het ecosysteem aan een strikte governance onderworpen moeten worden. Volgens het ecosysteem moet deze autorisatie **op het niveau van de use case** verlopen, zodat men per use case verifieert of een partij, in die specifieke context, recht heeft op toegang tot een dataset. De finaliteit of de doelstelling van het gebruik van de data is daarbij de belangrijkste drijfveer voor het al dan niet toestaan van toegang. Om vertrouwen te induceren, zou de evaluatie aan de hand van strikt gecommuniceerde richtlijnen en door een **onafhankelijk orgaan** (*data access committee*) moeten gebeuren. Technisch zijn er verschillende leveranciers van oplossingen mogelijk, die al dan niet in combinatie gebruikt kunnen worden (denk bijvoorbeeld aan itsme voor burgers of KUBE (Isabel Group) voor ondernemingen).

Identificatie en autorisatie kan toegewezen worden op een aantal niveaus, gaande van het individu tot een rol of organisatie. Door de authenticatie op organisatieniveau te brengen, kan men de **complexiteit** voor het beheer ervan voor de health data space aanzienlijk verlagen. Het nadeel is echter dat sommige data **privacy/AVG-gevoelig** zijn, en niet zomaar met elk individu binnen een organisatie gedeeld kunnen worden. Dit kan opgelost worden door identificatie en autorisatie op individu-niveau te laten gebeuren (zie hieronder). Dit gaat uiteraard gepaard met een complexer beheer, aangezien elk individu apart een token zal moeten krijgen. Volgens het ecosysteem zijn er alvast twee pistes:

> *Optie 1 - toegang per individu.* Hierin neemt de **health data space** zelf **de verantwoordelijkheid** voor de verificatie van de rechten van elk individu binnen elke organisatie. De feitelijke uitvoering kan via een derde partij gebeuren, maar de data space is eindverantwoordelijke. In dit geval kan de data space vereisen dat de aanvrager per use case beschrijft welk individu de data zal gebruiken en voor welk doeleinde. Dit wordt dan vastgelegd in de data sharing agreements of digitale contracten en kan geconsulteerd worden via het clearing house.
> *Optie 2 - toegang per organisatie.* Hier legt men de **verantwoordelijkheid bij de aanvragende organisatie**. De organisatie vraagt (en krijgt) toegang tot de data space en beheert dan intern welke personen toegang hebben, bv. via een eigen toegangsportaal. Een uitwerking hiervan is te vinden in de *Circle of Trust* van Vitalink/eHealth[393]. Deze omvatten 13 criteria voor zorginstellingen die garanderen dat zij voldoende rekening houden met privacy en veiligheid wanneer meerdere zorgverleners toegang krijgen

[393] https://www.vitalink.be/gebruikers/ik-ben-een-individuele-zorgverlener/circle-of-trust

tot data. Op deze manier is het niet de health data space die instaat voor de toegang van alle individuele werknemers binnen een organisatie. Deze optie draagt volgens het ecosysteem duidelijk de voorkeur.

Achteraf moet het **feitelijke gebruik** van de data ook geverifieerd kunnen worden. Dit refereert naar de ***tracebility*** van het data (asset) gebruik, en draagt bij aan het opbouwen van transparantie in de data space. Hoe dit feitelijk beheerd moet worden, is echter nog een vraagteken voor het ecosysteem.

Over het **belang van datakwaliteit** voor het goed functioneren van een health data space bestaat geen discussie. Meer nog, het verbeteren en garanderen van de datakwaliteit wordt gezien als één van de grootste meerwaarden van een data space. Een grootste probleem daarbij is echter dat de datamaturiteit **-** en dus datakwaliteit - erg kan verschillen tussen de stakeholders. Een tweede struikelblok is de **onduidelijke definitie van de term 'datakwaliteit'**. Verschillende partijen hechten immers belang aan de verschillende dimensies van datakwaliteit, waardoor de ene dataset voldoende kwalitatief is voor de ene use case, maar onvoldoende voor de andere. De definitie van 'datakwaliteit' moet daarom mogelijk **op use case niveau** gebeuren.

Eén van de belangrijkste indicatoren voor datakwaliteit voor het ecosysteem, is de **transparantie** omtrent de **volledigheid, correctheid, origine en beschikbaarheid (in de tijd) van de data**. Zo willen data consumers duidelijkheid over de timing van datacaptatie, de dekkingsgraad van de populatie waarbinnen de datacaptatie gebeurde, de regelmaat van updates van de data, de exacte onderzoeksprotocollen enz. Dit betekent dat er voor kwalitatief hergebruik van data voldoende **metadata** voorhanden moeten zijn die al deze details expliciteert. Helaas hinkt de **kwaliteit van metadata** vaak achterop. De meeste stakeholders geven aan hier weinig of niet mee bezig te zijn. Ook de publicatie van metadata in datacatalogi staat niet op punt. De verantwoordelijkheid voor deze aspecten ligt volgens het ecosysteem eerder bij de **data providers** dan bij de data space, al kan die wel bepaalde diensten aanbieden om data providers hierin te ondersteunen en hen verder aan te moedigen er werk van te maken via de toetredingsvoorwaarden van de data space.

Voor het beheer van de metadata lijkt de voorkeur van het ecosysteem uit te gaan naar een **gefedereerd of decentraal beheer van metadata**, al moeten de metadata wel **centraal geconsulteerd** kunnen worden[394]. Hiermee wordt bedoeld dat de metadata op verschillende locaties bij de data providers staan, maar via een centraal systeem uitgewisseld en opgevraagd kunnen worden. Dit heeft als voordelen dat de **autonomie** bij de data provider blijft; de privacy optimaal gewaarborgd wordt; een beveiligingslek in een systeem niet direct het geheel in gevaar brengt; het systeem **flexibel** is; en men gemakkelijk kan **opschalen**. Echter, hoe de centrale consultatie er concreet moet uitzien, is nog onduidelijk. Voor sommigen is er bij voorkeur slechts één metadatabroker die als *single-point-of-truth* fungeert. Dit schept helderheid en duidelijkheid en gaat een wildgroei aan systemen tegen. Volgens anderen kunnen er meerdere metadatabrokers naast elkaar bestaan, zolang deze maar conform de Europees gedefinieerde regels werken. Elke metadatabroker moet in dat geval wel over dezelfde (volledige) informatie beschikken, maar kan deze aanbieden op een andere manier.

Naast de volledigheid van de data, speelt ook data **standaardisatie** een rol in datakwaliteit. Het ecosysteem is van mening dat er prioritair ingezet moet worden op **semantische** standaarden, en pas op langere termijn op standaarden voor dataopslag. Standaarden voor dataoverdracht vindt men ondergeschikt in de discussie, aangezien dit een eerder beperkte impact heeft op de data kwaliteit *an sich*. Men benadrukt wel dat de data space zich niet mag vastbijten op een enkele standaard en een **combinatie van internationaal erkende standaarden** moet ondersteunen. Dit wordt beargumenteerd door het feit dat de gezondheidssector er, in tegenstelling tot een aantal andere sectoren, nog steeds niet in geslaagd is tot een enkele standaard te komen. Over de vraag of standaarden **afgedwongen** moeten worden, is het ecosysteem verdeeld.

[394] *Hiermee wordt bedoeld dat de metadata in het beheer van de data providers zit en blijft. Een centrale catalogus kan de gegevens raadplegen en via een zoekmachine aanbieden. Op deze manier is de aangeboden metadata steeds up-to-date en niet afhankelijk van updates van het centrale platform.*

Sommigen denken dat data space participanten in veel gevallen niet over voldoende datamaturiteit beschikken om zich aan strikt afdwingbare criteria te houden. Zij verkiezen dan ook om eerder via een type **intentieverklaring** te werken, waarbij partijen "zo goed mogelijk" conformeren aan bepaalde standaarden, zonder resultaatsverbintenis. Andere partijen uit het ecosysteem zien het afdwingen van standaarden als de enige optie, aangezien het niet-naleven ervan een erg nefaste impact kan hebben op de interoperabiliteit van de data.

Het ecosysteem is het er verder over eens dat de richtlijnen omtrent de governance van zowel datakwaliteit als metadatakwaliteit centraal vanuit de data space moeten komen. De verantwoordelijkheid voor de opvolging van die richtlijnen is echter een **gedeelde verantwoordelijkheid** tussen de verschillende partijen in de data space: data providers zijn verantwoordelijk voor het aanbieden van kwaliteitsvolle data en metadata; data consumers zijn verantwoordelijk voor het gebruik van de data en moeten afwijkingen melden; en de broker is verantwoordelijk voor de kwaliteitsvereisten en collectie en publicatie van de metadata. Wil men dit alles nog verder stroomlijnen, dan kan men een **interne cel** voorzien binnen de data space die zich toelegt op het garanderen, stimuleren en controleren van de datakwaliteit.

Deze interne cel zou dan kunnen rapporteren aan een **governanceorgaan** dat zich toelegt op de **technologische roadmap en referentiearchitectuur.** Deze "Architectural Lead" kan een duurzaam kenniscentrum worden voor data-technische requirements en kennis, wat ook toelaat snel te schakelen wanneer omstandigheden hierom vragen. In de governance structuur zou deze entiteit onder het sturend orgaan moeten staan. Het sturend orgaan bepaalt dan de strategisch-technische principes voor de data space (en legt bijvoorbeeld vast dat de health data space IDSA-*compliant*[395] moet zijn), en de architecturale entiteit maakt op basis daarvan de bijhorende **technische keuzes**. Belangrijk voor het ecosysteem is dat deze keuzes steeds **transparant** en consulteerbaar zijn voor data space participanten. Verder draagt dit orgaan de **verantwoordelijkheid voor het onderhoud** van de data space infrastructuur en de *value-added services* in de data space. Het eigenlijke onderhoud van de infrastructuur kan ofwel intern binnen de data space gebeuren, ofwel geoutsourcet worden. De verantwoordelijkheid voor het onderhoud van de **connectoren** ligt volgens het ecosysteem bij de **participanten** zelf.

Wat betreft de (types) **value-added services** die op korte of lange termijn in een health data space aangeboden zouden moeten worden, heerst veel onduidelijkheid, veelal omdat men niet goed weet wat mogelijk is in een health data space. Enkele voorbeelden die ter sprake kwamen zijn:

- **data services**, zoals datastandaardisatie of semantische mapping.
- **facturatieservice** (zoals Athumi reeds aanbiedt), al is dit op korte termijn niet prioritair.
- **marktplaats** die toelaat om extra diensten aan te bieden zoals het bouwen van dashboards of de creatie van geaggregeerde datasets.
- **veiligheidsdiensten.**

Men is ervan overtuigd dat deze diensten een belangrijke bron van **inkomsten** kunnen worden, hetzij voor de data space zelf, hetzij voor data space participanten. Een goed doordacht beheer van deze diensten is daarom een essentieel onderdeel van de governanceoefening.

Tot slot kan men nog opmerken dat er voor heel wat andere beheersvraagstukken (zoals data provenance, data space registers ...) nog veel onduidelijkheid heerst, en men vaak naar **Europa en lokale wetgevers of autoriteiten** (zoals de HDA) kijkt voor richting.

[395] *IDSA staat voor 'international data space association' en voorziet een technisch kader voor data spaces. Zie 3.4.1.1 voor meer informatie.*

7.3 GOVERNANCE STRUCTUUR VAN EEN HEALTH DATA SPACE

7.3.1 Introductie: Opbouw governance structuur en framework

De vorige sectie nam de inhoudelijke bouwblokken van governance onder de loep. Vanuit deze bouwblokken worden twee essentiële conceptuele dimensies onderscheiden voor 'good governance' in een health data space: de **governance structuur** – die focust op het verduidelijken van de organisatie, rollen en verantwoordelijkheden – en het eerder reeds gedefinieerde **governance framework**, dat de nadruk legt op het bepalen van de processen, regels en procedures die nodig zijn voor het goed beheer van de data space.

Om deze twee concepten in te vullen, zullen de oprichters van de data space keuzes moeten maken. Deze keuzes zijn onderbouwd door de specifieke noden van de data space en haar ecosysteem. Ze staan steeds in functie van de bredere context en worden ingegeven door de stand van zaken op elk van de domeinen die de thematische bouwblokken vormen. Onduidelijkheden in de maatschappelijke, legale, ethische, zakelijke of strategische context beperken dan ook het vermogen om eenduidige keuzes te maken, waardoor men **vaak meerdere opties of keuzemogelijkheden** voor ogen zal moeten houden.

Een concrete invulling van een governance structuur en framework voor een health data space zal dus steeds onderhevig zijn aan de finaal gemaakte keuzes. Het **voorstel tot de governance structuur** dat hieronder volgt, legt de nadruk daarom op het **aanbieden van een aantal opties of keuzemogelijkheden, zowel op korte termijn** (voor een kleinschalige data space) **als op langere termijn** (voor een grotere, maar ook meer op hypotheses steunende data space).[396] Uiteraard worden de suggesties onderbouwd door degelijke argumenten, ontleend aan de desk research of gesprekken met het ecosysteem, maar we behouden het voorrecht het niet als een definitief antwoord voorop te stellen. Wel geloven we dat onderstaand voorstel een **onderbouwde eerste aanzet kan zijn waarop men, op basis van voortschrijdend inzicht, verder kan bouwen**.

Finaal wordt dit voorstel tot een governance structuur nog aangevuld met een aantal **alternatieve governance-scenario's**, geïnspireerd op de reeds gemaakte keuzes van bestaande spelers in het ecosysteem (zoals bijvoorbeeld e-Health, Faqir, Athumi, en SOLID).

7.3.2 Definities: Governance structuur en relevante terminologie

Binnen het kader van dit onderzoeksproject werd al snel duidelijk dat de huidige definities rond governance niet alleen vaak door elkaar gebruikt worden, maar in vele gevallen ook ontoereikend zijn. Het is daarom belangrijk een aantal concepten helder te definiëren, vooraleer over te gaan tot een suggestie voor de invulling ervan.

Zoals in de introductie (7.1.1 Wat is data space governance?) al werd aangehaald, kan *governance* volgens de eigen definitie samengevat worden als "het ondersteunen van beslissingen ten voordele van goed bestuur, en dit door middel van zowel heldere regels als duidelijke rollen en verantwoordelijkheden." Ter vergelijking: DSSC definieert [data space] governance als "the processes to develop, maintain and enforce the governance framework of a particular data space" (DSSC, 2023), waarbij het governance framework gericht is op de regels, procedures en overeenkomsten betreffende het (operationeel) beheer van de data space.

Deze definitie, waarbij governance wordt gelijkgesteld aan het governance framework, bleek voor dit onderzoeksproject echter ontoereikend. Een van de grote vraagstukken die uit de gesprekken met het ecosysteem naar voren kwamen, had namelijk betrekking op het aspect 'verantwoordelijkheden en mandaten'.

[396] *Aangezien de PoC erg beperkt is, behoeft deze geen volwaardige governance structuur en kan ze voornamelijk verder bouwen op (al dan niet formele) afspraken en samenwerkingsverbanden tussen de consortiumpartners. Eventuele suggesties voor de PoC worden dan ook niet hier behandeld, maar staan direct in het relevante hoofdstuk (zie hoofdstuk 9.5).*

Er moet duidelijk bepaald worden w*ie* de regels en processen ontwikkelt, onderhoudt en afdwingt, welke organisaties erbij betrokken zijn, welk mandaat ze hebben, en hoe ze zich tot elkaar verhouden. Daarom werd het noodzakelijk geacht de **dimensie 'rollen en verantwoordelijkheden' explicieter naar voren te schuiven binnen governance**, en als een vraagstuk an sich te behandelen. Naar analogie met de meer bekende term *organisatiestructuur* (waar het heel wat eigenschappen mee deelt), werd ervoor gekozen dit geheel aan rollen en verantwoordelijkheden af te dekken met de term ***governance structuur***.

De beslissing om governance structuur als een aparte pijler te behandelen, naast het governance framework, wordt ondersteund door twee argumenten. Ten eerste voldoen we hiermee aan de hierboven aangehaalde **verwachtingen vanuit het gezondheidsecosysteem**; en ten tweede sluit het aan bij de observatie dat er een **natuurlijke match is tussen bepaalde thematische bouwblokken en de twee governance dimensies**. Vragen rond het thema *legale en organisatorische vorm* bleken automatisch mee vorm te geven aan de governance structuur, terwijl vragen rond de thema's *data-technische requirements* en (vooral) *regelgevend kader* sterke overlap vertoonden met te maken keuzes op vlak van het governance framework.

Daarom willen we, op basis van het gevoerde onderzoek, de term *governance structuur* introduceren als een apart te beschouwen pijler die kortweg omschreven kan worden als "het web aan relaties tussen de verschillende governance-organen, rekening houdende met zowel de specifieke rollen en verantwoordelijkheden binnen de data space, als met externe actoren buiten de data space."

7.3.2.1 Governance Authority

Aansluitend op deze definitie van de governance structuur, moeten ook twee andere veelgebruikte termen toegelicht worden: *governance authority* en *governance bodies* (we zullen deze term afwisselend met de Nederlandse term *governance-organen* gebruiken).

DSSC gebruikt de term ***governance authority*** voor een data space participant die verantwoordelijk is voor "creating, developing, operating, maintaining and enforcing the governance framework for a particular data space, without replacing the role of public enforcement authorities." (DSSC, 2023) De governance authority **omvat dus zowel de bestuurlijke functie** (bepalen, controleren en afdwingen van het governance framework) **als de uitvoerende functie** (onderhouden en operationaliseren van het governance framework) *binnen* de data space.

Deze rol en verantwoordelijkheden passen duidelijk binnen de omschrijving van een governance structuur, maar zijn er een ietwat engere interpretatie van. De governance structuur zoals hierboven gedefinieerd beschrijft namelijk ook de rollen en verantwoordelijkheden van organen of entiteiten die *geen* deel uitmaken van de data space, maar die wel een directe bijdrage leveren tot haar onderhoud, ondersteuning of operationalisering. Zo valt, volgens deze interpretatie, een externe adviserende entiteit (bv. het informatie-veiligheidscomité, IVC) *wel* binnen de governance structuur van de data space, maar *niet* binnen de governance authority. Voor de rest van dit hoofdstuk zal de term governance authority dan ook in die hoedanigheid worden gebruikt: het geheel aan *interne* entiteiten die het governance framework vormgeven, ontwikkelen, onderhouden en operationaliseren.

7.3.2.2 Governance Bodies

Tot slot moet nog het onderscheid worden gemaakt tussen de governance authority en een *governance body*. De governance authority kan namelijk uit één of meerdere *governance bodies* bestaan (afhankelijk van o.a. de wettelijke verplichtingen, omvang en noden van de data space), waarbij een ***governance body*** **elke entiteit is binnen de data space die een gedifferentieerde en gespecialiseerde governance-functie uitvoert**. Typisch worden de bestuurlijke en de uitvoerende governance-functies gescheiden, maar grotere data spaces kunnen hier verder in gaan en bijkomende governance-verantwoordelijkheden en rollen aflijnen. Zo kan bijvoorbeeld een superviserende of controlerende functie worden toegevoegd, of kunnen domeinspecifieke adviserende rollen in het leven worden geroepen.

Samenvattend kan men stellen dat elke data space een governance authority omvat, die kan bestaan uit één of meerdere governance-organen. Elk governance-orgaan heeft zijn eigen (duidelijk omlijnde) governance-functies en verantwoordelijkheden. Deze governance-organen staan bovendien niet los van elkaar, maar hebben samenwerkings- en rapporteringslijnen die zich zowel intern (binnen de data space) als extern (als deel van het ecosysteem) tot elkaar verhouden. Dit geheel aan rollen, verantwoordelijkheden en onderlinge relaties wordt weergegeven en omschreven in de governance structuur.

7.3.3 Voorstel: juridische vorm

Zoals eerder aangegeven in de methodologische aanpak, zijn er een aantal essentiële vraagstukken die men als data space moet beantwoorden vooraleer men vorm kan geven aan de governance structuur.
De antwoorden op deze vragen geven namelijk richting aan de specifieke legale en organisatorische vorm voor de data space, en op die manier ook aan een aantal vereisten op het vlak van governance en representatie. Daarom werd in de onderzoeksfase veel tijd en aandacht besteed aan het evalueren en formuleren van de verschillende mogelijke antwoordopties voor deze vraagstukken, zowel wat betreft de (feitelijke) voor- en nadelen als de (subjectieve) voorkeuren vanuit het ecosysteem. Op basis hiervan konden een aantal assumpties worden gemaakt die samen het uitgangspunt vormen voor de voorgestelde juridische vorm en governance structuur.

1. *Maakt de data space deel uit van een bestaande entiteit of een bestaand initiatief, of is het een op zichzelf staande entiteit?*

De Health Data Space is een op zichzelf staande entiteit. Om meer wendbaarheid en (politieke en financiële) onafhankelijk te garanderen, gaat de voorkeur van het ecosysteem sterk uit naar een Health Data Space die als aparte entiteit opereert (zie hoofdstuk 7.2.3.3 Rol van de overheid volgens het ecosysteem). Dit wil zeggen dat ook de governance structuur van de health data space onafhankelijk zal opereren en zich niet binnen een reeds bestaande organisatie (zoals bijvoorbeeld het Departement Zorg) bevindt. Dit laat bovendien toe om vertegenwoordiging uit verschillende relevante organisaties of entiteiten te voorzien binnen de Health Data Space (onder andere ook politieke vertegenwoordiging waar en indien gewenst).

2. *Is de data space een tijdelijke entiteit, of wordt het een permanente entiteit?*

De Health Data Space is een permanent initiatief, aangezien de missie en visie vertrekken vanuit de maatschappelijke meerwaarde voor de volksgezondheid op lange termijn. Een succesvolle Health Data Space steunt bovendien op vertrouwen, zowel tussen de participanten onderling als tussen participanten en de data space. Een permanente entiteit die collaboratie op lange termijn voorstaat (onder andere via een meer geformaliseerde samenwerking en een centraal afsprakenkader) is daartoe meer geschikt dan een *ad hoc* samenwerkingsverband dat vertrekt vanuit onderlinge one-to-one afspraken en goodwill. (zie hoofdstuk 7.2.3.3 Rol van de overheid volgens het ecosysteem).

3. *Is de visie en missie van de data space gericht op algemeen maatschappelijk nut, of op winst?*

De Health Data Space is een organisatie zonder winstoogmerk. Dit vraagstuk is het meest complex om te beantwoorden, maar de keuze voor een non-profit organisatiestructuur kan voornamelijk beargumenteerd worden vanuit de breed gedragen veronderstelling dat een non-profit structuur tot meer vertrouwen zal leiden binnen het ecosysteem (en dus de adoptie en het gebruik van de data space zal stimuleren).
Door een expliciete maatschappelijke missie naar voren te schuiven, kan de te verwachten weerstand tegen het delen van gezondheidsdata gedeeltelijk opgevangen worden (zie hoofdstuk 7.2.3 *stukken over vertrouwen/non-profit in interviews met ecosysteem*).

Bovendien sluit een non-profit model financiële compensatie niet uit: een non-profit organisatie mag winst genereren (bijvoorbeeld via ledengelden of donaties en sponsoring), zolang de winsten die hieruit voortkomen geherinvesteerd worden in het maatschappelijk doel (zie hoofdstuk 6.2.2 Vennootschapsrecht).

Daarbij staat het de data space ook vrij om commercieel ingestelde partijen als participant toe te laten tot de data space.[397] Een non-profitorganisatie staat dus niet per definitie haaks op de vraag naar een entiteit die zowel politiek als (op termijn) financieel zelfstandig kan opereren.

Met deze assumpties als uitgangspunt, en steunend op de legale scan, is actueel de *non-profit vereniging*[398] dus het meest logische bedrijfstype voor een Health Data Space. Binnen dit type zijn er nog twee relevante mogelijke juridische vormen: de *vzw* (vereniging zonder winstoogmerk) en de *stichting*. Beide types verenigingen streven uiteraard een belangeloos doel na, maar verschillen van elkaar op een aantal praktische dimensies[399] die men kan samenvatten als:

- het te verwachten aantal stichtende leden
- de mogelijkheden op vlak van beslissings- en stemrecht
- de mogelijkheden voor internationale expansie
- de graad van formalisering van de vereniging.

	VZW	***STICHTING***
Minimaal # stichtende leden	Meerdere leden vereist	Mogelijk met slechts één lid
Beslissings-/stemrecht	Toegekend aan (working) members in AV	Geen leden met stemrecht
Graad van formalisatie	Medium *(Minder vereisten dan vennootschappen, maar wel vereisten op vlak van representatie, zie onder (AV & RvB))*	Laag *(Vrij in te vullen)*
Internationalisering	Eenvoudig	Complex

Een meer volledige omschrijving van de eigenschappen van beide types verenigingen kan men terugvinden in 6.2.2 Vennootschapsrecht, maar gezien de verwachting dat de Health Data Space meerdere stichtende leden zal hebben die een zekere mate van beslissingsrecht zullen verwachten, is de vzw vandaag de dag de meest waarschijnlijke juridische vorm voor een Health Data Space. Het volgende stuk rond de **governance structuur zal dan ook vertrekken vanuit de legale vereisten tot representatie voor een vzw**.

7.3.4 Voorstel: governance structuur

Ter herhaling, op basis van het gevoerde onderzoek en uitgeschreven hierboven, wordt de term *governance structuur* omschreven als “het geheel aan governance-organen, inclusief de bijhorende rollen, verantwoordelijkheden, en verhoudingen, zowel tot elkaar (binnen de data space) als tot relevante externe actoren (buiten de data space).”

[397] *De vraag of een non-profit data space al dan niet commerciële diensten (met winstoogmerk) mag faciliteren wanneer zij hier zelf geen winst uithaalt, valt niet met 100% zekerheid te beantwoorden. De legale scan identificeerde, op het moment van dit schrijven, echter geen duidelijke barrières of verboden. Bovendien mogen commerciële actoren gebruik maken van de diensten die een Health Data Space zou aanbieden, daar het uiteindelijke gebruik van de gegevens door de data users geen invloed heeft op de belangeloze doelstelling van de data space zelf.*

[398] *Afhankelijk van de ambities op lange termijn is het belangrijk te vermelden dat de overgang van een non-profit naar een for-profit organisatie quasi-onmogelijk is, onder andere omdat het vermogen vervalt daar de finaliteit van de entiteit wijzigt (van belangeloos naar winstoogmerk). Indien men op termijn dus for-profit ambities heeft, dan is het beter (1) bij de oprichting al vanuit een for-profit structuur te vertrekken of (2) een nieuwe entiteit (vennootschap) in het leven te roepen. Alternatief kan men beide structuren in parallel beheren, met alle complexiteit van dien (zie bijvoorbeeld Faqir, dat gelijktijdig een Foundation (vzw) en een Institute (NV) beheert). Omgekeerd is ook de omzetting van een for-profit naar een non-profit overigens erg complex en bij voorkeur te vermijden.*

[399] *Zowel bij de vzw als bij de stichting kan afgeweken worden van bovenstaande principes indien anders opgenomen in de statuten.*

7.3.4.1 Minimale governance structuur

Gezien de specifieke vereisten tot representatie binnen een vzw, zal de governance structuur van de Health Data Space op zijn minst uit een ***Algemene Vergadering*** (sturend) en een ***Bestuursorgaan*** (uitvoerend) moeten bestaan. Voor beide organen zijn de (minimale) verantwoordelijkheden wettelijk verankerd (al kan men hier te allen tijde van afwijken door de deviaties duidelijk op te nemen in de statuten).

Algemene Vergadering (AV)

Samenstelling: bestaat uit de stichtende leden (*founding members*) en eventuele werkende leden (*working members*), die al dan niet (gelijkwaardig) stemrecht[400] hebben.

Verantwoordelijkheden: de Algemene Vergadering stelt bij oprichting de statuten van de vzw op en heeft verder een sturende functie. Ze staat in voor grote strategische beslissingen, stelt de leden van het Bestuursorgaan aan (of ontzet deze uit hun functie) en keurt de jaarrekening van de vzw goed (indien van toepassing). Tot slot kan de Algemene Vergadering beslissen over het wijzigen van de statuten of het wijzigen van de juridische vorm van de entiteit[401].

Bestuursorgaan (Raad van bestuur, RvB)

Samenstelling: bestaat verplicht uit minimaal drie leden, die *statutair* aangesteld zijn door de Algemene Vergadering.

Verantwoordelijkheden: het Bestuursorgaan voert alle overige bevoegdheden uit en heeft een voornamelijk executieve functie. Zo stelt het de jaarrekening op, dat ze ter goedkeuring voorlegt aan de Algemene Vergadering. Het Bestuursorgaan kan contractueel personeel in dienst nemen en dagelijkse bestuurders aanduiden.

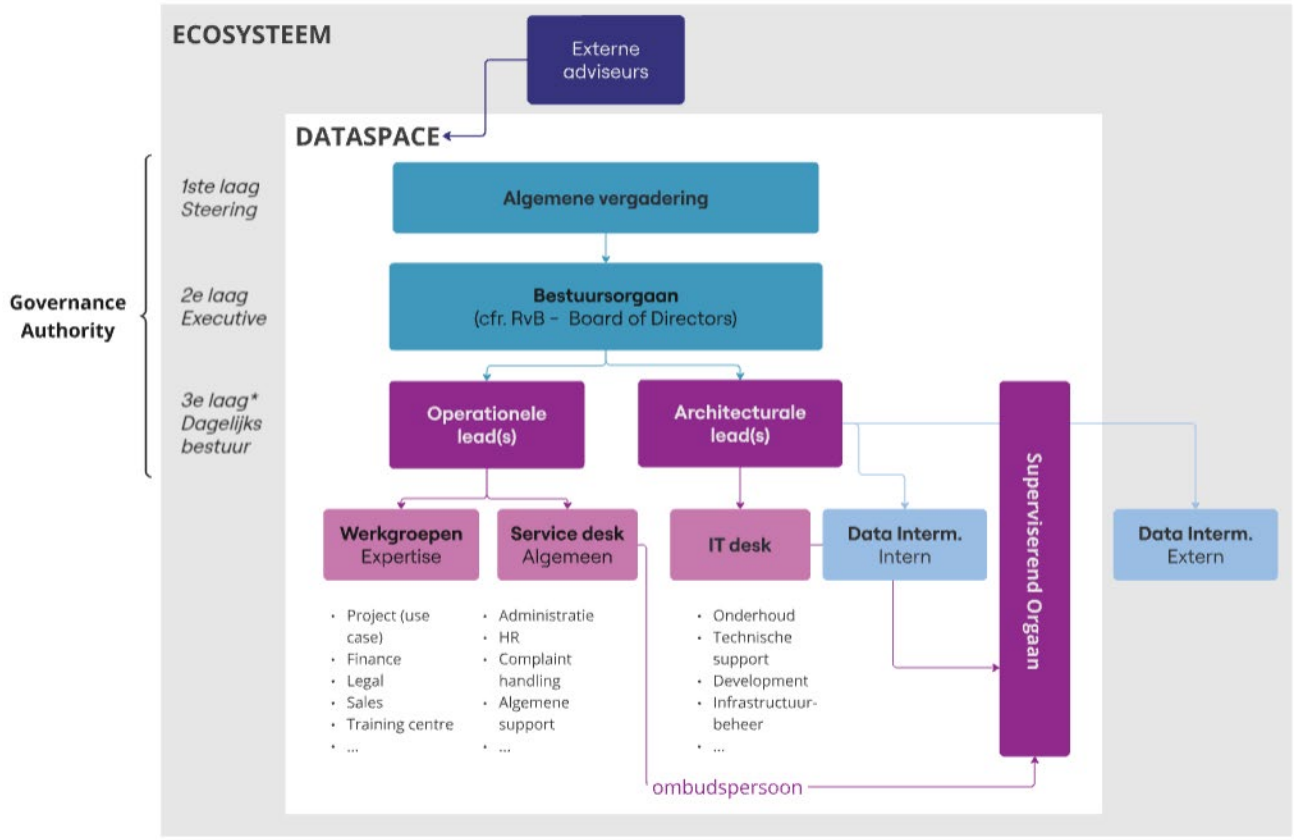
7.3.4.2 Uitgebreide governance structuur

Zoals aangegeven vormen de Algemene Vergadering en het Bestuursorgaan de *minimale* governance structuur. Op korte termijn zal deze structuur - die ook de Governance authority vertegenwoordigt - volstaan om de belangrijkste taken van een net opgestarte Health Data Space op te nemen. Naarmate de data space opschaalt en meer use cases en participanten onboardt, zal ook de nood ontstaan om bepaalde bevoegdheden (governancefuncties) uit te besteden aan gespecialiseerde entiteiten (governance bodies).

Onderstaand organigram stelt zo'n **governance structuur op langere termijn** voor, waarbij de data space haar kerntaken en -verantwoordelijkheden naar **verschillende gespecialiseerde entiteiten gedelegeerd heeft**. Deze bijkomende governanceorganen representeren een uitdieping van de bestuurlijke en uitvoerende verantwoordelijkheden van het Bestuursorgaan, en onderhouden de dagelijkse werking van de data space op operationeel en architecturaal vlak. De hieronder voorgestelde structuur is in geen geval een monolithische structuur die als dusdanig overgenomen moet worden: elk van de verantwoordelijkheden die aan bod komen, kan in eerste instantie door een ander (reeds bestaand) orgaan vertegenwoordigd worden. Enkel wanneer de data space groter en complexer wordt, zal het noodzakelijk worden deze gespecialiseerde organen gradueel en in functie van de heersende noden in het leven te roepen.

[400] *In principe hebben alle leden van de AV gelijk stemrecht, maar hiervan kan afgeweken worden in de statuten. Zo gaat de voorkeur van het ecosysteem uit naar vertegenwoordiging in de AV van de stichtende leden (met stemrecht), eerstelijnsgezondheidsactoren (met stemrecht – vertegenwoordiging via beroepsverenigingen voor artsen, apothekers ...), het middenveld (met stemrecht) en – eventueel – Europese of federale politieke vertegenwoordiging (zonder stemrecht, om wantrouwen vanuit burgers en het middenveld tegen te gaan).*

[401] *Gezien de complexiteit die gepaard gaan met het omvormen van de legale entiteit, houdt dit in de praktijk in dat de AV ertoe kan beslissen dat de vzw overgaat in een ivzw (internationale vzw); een cv erkend als sociale onderneming; of een erkend cvso (coöperatieve vennootschap met sociaal oogmerk).*



Figuur 12: Uitgebreide governance structuur

Operationele lead(s)

Samenstelling: De Operationele Lead is een niet-verplichte, dagelijkse bestuursfunctie. Ze wordt contractueel aangesteld door (en rapporteert aan) het Bestuursorgaan. Deze rol kan zowel door een enkele persoon als door meerdere personen (bijvoorbeeld een afvaardiging van de werkgroepen) uitgevoerd worden.

Verantwoordelijkheden: Dit bestuursorgaan is verantwoordelijk voor de niet-technische operationele werking van de data space. In die hoedanigheid:

> Concretiseert het de richtlijnen van het Bestuursorgaan naar specifieke operationele processen, regels en procedures, en kan het advies geven omtrent het opstellen van nieuwe regels of procedures;

> Indien de data space gebruik maakt van werkgroepen en/of een Service Desk, dan staat de Operationele Lead ook in voor het dagelijks bestuur (opvolgen, aansturen, evaluatie,...) van deze functies.

> Indien de data space gebruik maakt van Data Intermediaries (zie lager in dit hoofdstuk), dan werkt de Operationele Lead samen met de Architecturale Lead om deze samenwerking vorm te geven en te coördineren.

> Tot slot werkt de Operationele Lead samen met het Superviserend Orgaan om de navolging van de (interne) regels en procedures op te volgen, en om eventuele conflicten of klachten adequaat op te lossen.

Architecturale lead(s)

Samenstelling: De 'Architecturale Lead' loopt parallel aan de Operationele Lead. Het is een niet-verplichte, dagelijkse bestuursfunctie die wordt uitgevoerd door één of meerdere personen, en die contractueel wordt aangesteld door (en rapporteert aan) het Bestuursorgaan.

Verantwoordelijkheden: Waar de Operationele Lead de algemene visie en richtlijnen in operationele taken en processen omzet, is de Architecturale Lead verantwoordelijk voor het uitzetten en realiseren van de referentiearchitectuur. Het doel is om de technologische ontwikkeling van de data space goed af te stemmen op de strategische en zakelijke visie van de Algemene Vergadering en het Bestuursorgaan.
De Architecturale Lead is verantwoordelijk voor:

> De afstemming en realisatie van de architecturale roadmap. Dit gebeurt in nauw overleg met het Bestuursorgaan, aan wie het ook adviseert omtrent architecturale en (data-)technische beslissingen (bv. de selectie van de te gebruiken standaarden). De Architecturale Lead ontwikkelt ook de nodige architecturale processen en procedures.
> De aansturing van de data space infrastructuur, ook indien de operationalisering ervan uitbesteed is aan een derde partij. In dit geval zorgt de Architecturale Lead ervoor dat de infrastructuur in lijn ligt met de uitgezette referentiearchitectuur.
> Indien de data space een IT-desk heeft voor (onder andere) dagelijkse (technische) ondersteuning, dan stuurt de Architectural Lead deze aan.
> Het coördineren van eventuele Data Intermediaries , zodat hun activiteiten en services aansluiting vinden bij de roadmap van de data space. Dit gebeurt in samenspraak met de Operationele Lead.
> Tot slot werkt de Architecturale Lead samen met het Superviserend Orgaan om de navolging van de data-technische regels en procedures op te volgen, en eventuele conflicten of klachten op te lossen (bv. het niet-opvolgen van regels rond te gebruiken (meta)datastandaarden).

Superviserend orgaan

Samenstelling: Het Superviserend Orgaan heeft als voornaamste taak om vertrouwen te creëren in de goede en neutrale werking van de data space. Om dit te kunnen realiseren, opereert deze (niet-verplichte) rol ietwat anders dan de tot nog toe beschreven organen:

> In een ideaal scenario wordt deze functie (semi-)onafhankelijk beheerd, en wordt het niet direct aangestuurd of bezoldigd door het Bestuursorgaan.
> Het bestaat uit meerdere leden, idealiter geselecteerd uit zowel interne en externe partners, die een zekere kennis hebben van de belangrijkste juridische en ethische vraagstukken in het gezondheidsdomein.[402] Bovendien hebben deze leden zich ook het Health Data Space governance framework eigen gemaakt, aangezien zij hiernaar zullen verwijzen bij het uitvoeren van hun taken.
> Het is wenselijk dat elk aangesteld lid van het Superviserend Orgaan ook een back-up (of reservelid) heeft. In het geval van belangenvermenging kan dit reservelid dan de taken overnemen (denk bijvoorbeeld bij een dispuut rond een entiteit waar een zetelend lid een (commerciële) relatie mee heeft).

Verantwoordelijkheden: Algemeen genomen controleert het Superviserend Orgaan de goede werking van de data space en haar (uitvoerende) governanceorganen. Het hoofddoel van dit bestuursorgaan is niet om bestraffend te werken (hoewel het hier een mandaat toe heeft), maar om een eerlijke, transparante en faire werking te garanderen via advies en sturing.

> Het Superviserend Orgaan voert haar controlerende en sanctionerende taken uit op basis van de afspraken, rollen en verantwoordelijkheden zoals gedefinieerd in het governance framework en de Accession Agreement.
> Het adviseert het Bestuursorgaan in het geval van conflictsituaties of bij complexe inbreuken tegen de regels. Het Superviserend Orgaan doet dan een suggestie rond de te volgen procedure en stappen (gaande van een open gesprek tot een aanmaning, beboeting of zelfs een verplichte offboarding). Op basis van haar juridische expertise, kan het ook inschatten of eventuele verdere juridische stappen moeten gezet worden.

[402] *Gezien de functie van het Superviserend Orgaan binnen de data space, lijkt het logisch dat de DPO een van de intern zetelende leden is.*

> Een mature data space schakelt idealiter een **ombudsman of -vrouw** voor de dagelijkse afhandeling van klachten. Op die manier wordt het Superviserend Orgaan enkel ingeschakeld bij complexe situaties, en kunnen minder urgente of complexe issues naar andere organen of bestuursniveaus doorverwezen worden.

Werkgroepen

Samenstelling: De werkgroepen zijn een niet-verplichte operationele entiteit. Ze bestaan uit één of meerdere personen met een specifieke domeinexpertise. Werkgroepen zijn erg flexibel en kunnen tijdelijk in het leven worden geroepen. Zo kan men een tijdelijke werkgroep oprichten om een complexe use case die specifieke kennis vereist te onboarden – en deze weer opdoeken na afronding van de onboarding.

Verantwoordelijkheden: De werkgroepen vormen een aanvulling op de taken van de Operationele Lead, en voeren gespecialiseerde operationele processen binnen een specifiek domein uit. Vanuit hun domeinexpertise geven ze ook advies aan de Operationele Lead. In een meer complexe data space zou men een afvaardiging per werkgroep binnen het orgaan van de Operationele Lead kunnen laten zetelen.

Service desk & IT desk

Samenstelling: De Service Desk en de IT Desk lopen parallel aan elkaar. Ze bestaan uit één of meerdere personen met een beleidsondersteunende functie.

Verantwoordelijkheden: De support desks zijn verantwoordelijk voor de uitvoering van respectievelijk de algemene operationele processen (Service Desk) en de (data-)technische processen (IT Desk).
De Service Desk voert bijvoorbeeld de algemene administratie en HR-taken uit, terwijl de IT Desk de infrastructuur onderhoudt of systeemupdates beheert. Beide functies zijn eerstelijnsverantwoordelijke voor de afhandeling van (algemene of technische) klachten of vragen, en staan hiervoor in nauw contact met de ombudsman/-vrouw.

Externe adviseurs

Voor bepaalde taken of expertises zal de data space best op reeds bestaande externe kennis vertrouwen. Binnen het gezondheidslandschap bestaan er reeds een aantal goed ingeburgerde procedures of adviesorganen die op *ad hoc* basis bepaalde (governance)vraagstukken die buiten de reguliere expertise van de data space vallen kunnen beantwoorden. Zo kan men voor complexe ethische vraagstukken aankloppen bij bestaande *ethische comités*, of moet men zich voor aanvragen rond privacygevoelige data tot het IVC[403] wenden.

Data intermediaries

De Data Intermediary is een entiteit die één of meerdere *core services* van een data space aanbiedt (denk bijvoorbeeld aan een clearing house, een (metadata) broker ...).[404] Deze core services kunnen ingekapseld zijn in de werking van de data space, of kunnen door (externe) partners aangeleverd worden. In dit geval moeten de contacten en afspraken met de Data Intermediaries goed afgestemd worden op de strategie van de data space, hetzij door het Bestuursorgaan zelf (minimale governance structuur), hetzij door de Operationele en/of Architecturale Lead (zie ook het hoofdstuk 6.2.4 Algemene Verordening Gegevensbescherming (AVG)).

Uit verschillende gesprekken met het ecosysteem kwamen een aantal partijen naar voren als (logische) Data Intermediaries binnen een Health Data Space: Athumi (clearing house), Departement Zorg (metadatabroker), e-health (pseudonimisatie), HDA (data access) ...[405]

---

[403] *Voor meer informatie over het IVC (informatieveiligheidscomité) en de geijkte procedure, zie 6.2.4.9.*

[404] *Deze definitie van de term Data Intermediary volgt de meer generieke interpretatie van DSSC, en is veel breder dan de strikte definitie opgelegd door de DGA om een officieel door de EU erkende Data Intermediary Service Provider (DISP) te worden. Zie 6.2.4 voor meer informatie over de specifieke vereisten voor erkenning tot een DISP door de DGA.*

[405] *De vermelde partijen kunnen deze Data Intermediary-rollen probleemloos opnemen volgens de DSSC-definitie. Indien zij ook erkend willen zijn als DISP, dan moeten deze actoren volledig neutraal opereren, en mogen ze de aangeboden data zelf niet gebruiken.*

Governance Authority

Voor de uiteindelijke werking van de data space zullen sommige van de hierboven beschreven organen meer essentieel zijn dan anderen. Deze organen hebben logischerwijze meer zeggenschap over het opstellen, valideren, controleren en aanpassen van het governance framework, en vormen samen de **Governance Authority**. In een minimale governance structuur valt deze samen met de Algemene Vergadering en het Bestuursorgaan. Binnen een grotere en complexere data space moet niet elk orgaan een even verregaand mandaat hebben, en zullen sommige wél deel uitmaken van de Governance Authority (Algemene Vergadering, Bestuursorgaan, Operationele en Architecturale Lead, Superviserend Orgaan), en andere niet (werkgroepen, support desks, data intermediaries, externe adviseurs). Het zijn deze governance-organen die *niet* in de Governance authority zetelen, maar die *wél* belangrijk zijn voor de goede werking van de data space, die onder de eerder gedefinieerde term *governance structuur* vallen.

Governanceorgaan	Functie	Governance Authority
Algemene Vergadering	Sturend (strategisch)	Ja
Bestuursorgaan	Executief	Ja
Operationele Lead	Dagelijks bestuur	Ja
Architecturale Lead	Dagelijks bestuur	Ja
Superviserend Orgaan	Controlerend en sactionerend	Ja
Werkgroepen	Uitvoerend (expertise)	Nee
Service Desk	Ondersteunend (algemeen)	Nee
IT Desk	Ondersteunend (technisch)	Nee
Externe adviseurs	Advies (expertise)	Nee
Data Intermediaries	Uitvoerend (core service)	Nee

Figuur 13: Overzicht governance structuur van een health data space (voorstel)

7.3.5 Alternatieve governance structuur en keuzes

Voorgaande organigram voor een governance structuur is een gefundeerd voorstel dat steunt op inzichten uit interviews en desk research. In de praktijk zijn er reeds geïmplementeerde governance structuren bij bestaande organisaties. Een aantal daarvan hebben ter inspiratie gediend voor bovenstaand model, hetzij rechtstreeks, hetzij omwille van de contrasterende keuzes die gemaakt zijn.

Het loont daarom de moeite deze alternatieve governance structuren bij organisaties als de Vlaamse Water Data Space, Athumi, Solid, FAQIR, en eHealth even kort onder de loep te nemen, en de meest interessante, inspirerende of afwijkende keuzes te duiden, rekening houdend met de respectievelijke voor- en nadelen van deze keuzes voor het opzetten van een health data space. De info in het hierop volgende deel werd verzameld via desk research.

7.3.5.1 Vlaamse Smart Data Space (VSDS) & Vlaamse Water Data Space (VWDS)

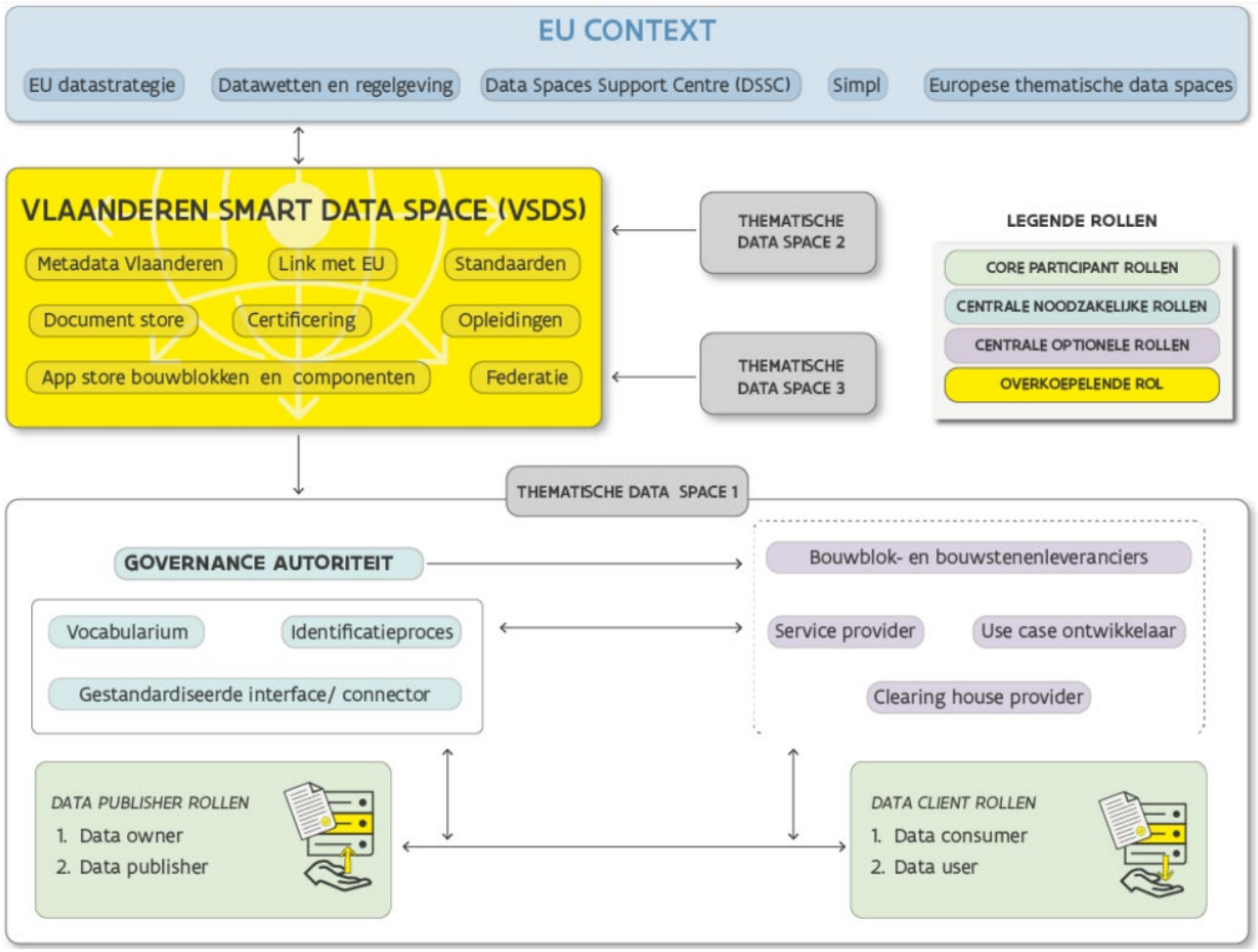
Om te voorzien in de vraag naar (regionale) data spaces, is Vlaanderen sinds een aantal jaar bezig met het opzetten van een **centraal platform dat** hierin **technisch en organisatorisch kan ondersteunen**: de **Vlaamse Smart Data Space** of VSDS . Deze ondersteuning wordt geboden onder andere via technische standaarden, componenten (of bouwblokken)[406], en een governance framework (of afsprakenkader). Bovenop deze centraal aangeboden deeloplossing, kan dan een domeinspecifieke data space gebouwd worden (Digitaal Vlaanderen, 2024).

Vandaag zijn er al een aantal lopende thematische use cases, waaronder die voor mobiliteit en water. Die laatste, de **Vlaamse Water Data Space (VWDS)**, is een interessante case voor governance, enerzijds omdat zij de generieke **governance structuur** van de VSDS aangevuld heeft met keuzes die inspelen op de eigen noden; en anderzijds omdat de VWDS - als eerste Vlaamse data space - een **accession agreement** heeft opgesteld, die bovendien ruimer gaat dan een overzicht van de zuivere regels en procedures.

7.3.5.1.1 Governance structuur (VSDS)

Net zoals het een aantal technische bouwblokken centraal aanbiedt, stelt de VSDS voor om ook de belangrijkste governance beslissingen **centraal** aan te bieden, vanuit een door de VSDS aangestuurde **governance authority**. Deze heeft het mandaat om de richtlijnen voor veilige datadeling en goed databeheer uit te zetten, en kan ingrijpen bij inbreuken. Ze legt de **algemene afspraken** vast, die van toepassing zijn voor alle thematische data spaces. Hieronder vallen ook een aantal **data-technische keuzes**, zoals de semantische standaarden en vocabularies, de keuze voor een bepaald identificatie- en/of autorisatiemechanisme, en de keuze voor een specifieke uitwisselingsstandaard.

[406] *Voor meer details over de technische keuzes die gemaakt zijn door VSDS (componenten, standaarden ...), zie 3.4.3.2.*

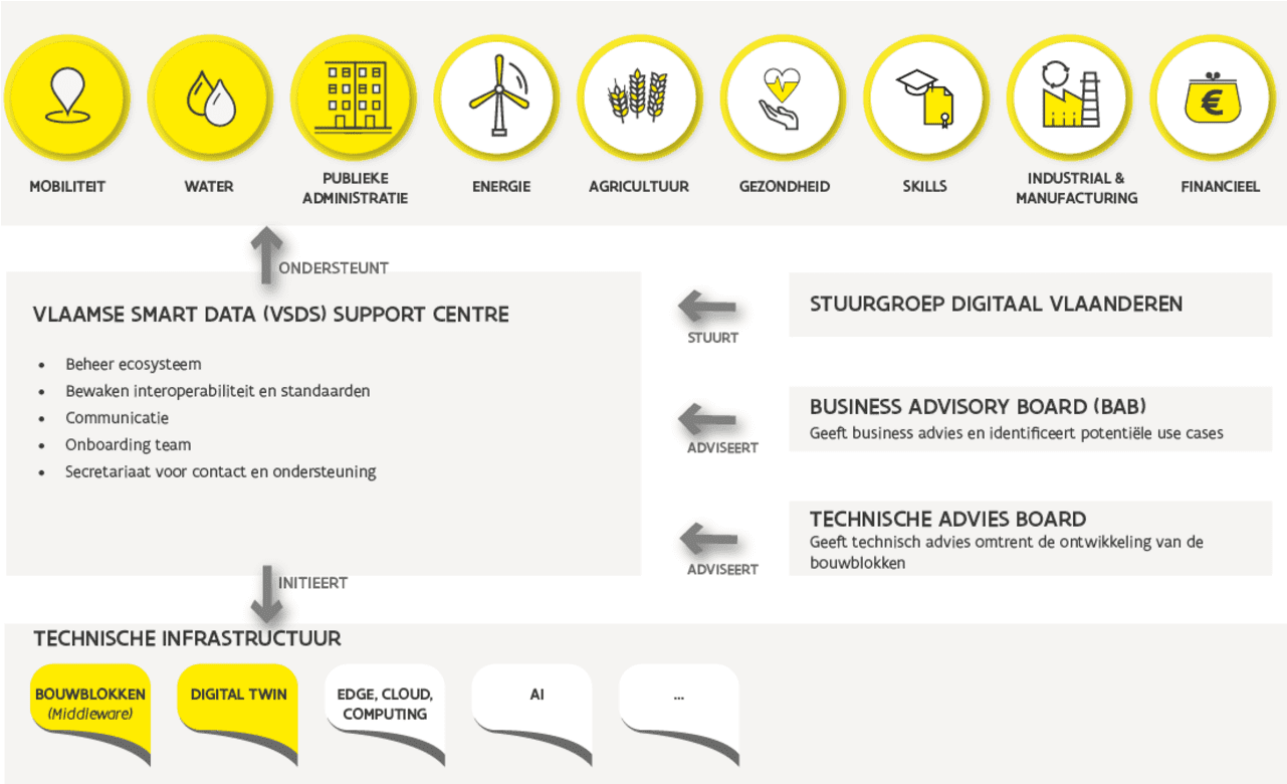


Figuur 14: VSDS: Governance authority & rollen

Ter aanvulling van deze centrale keuzes, laat de VSDS de thematische data spaces ook vrij om een aantal eigen keuzes te maken. Zo wordt van de thematische data spaces verwacht dat ze het **algemene governance framework aanvullen met eigen regels en afspraken**, zowel op het niveau van de participant (via smart contracts, zie ook 7.4.1.3 Types policies) als middels een eigen aanvullend afsprakenkader. Ook op strategisch en technisch niveau wordt de ruimte gelaten een aantal functies en rollen vrij in te vullen, onder andere met de keuze voor data intermediaries zoals het clearing house (Digitaal Vlaanderen, 2024).

Tot slot voorziet de VSDS – naast een governance authority - ook nog in een **operationeel** gericht *VSDS Support Centre*, dat de individuele thematische data spaces ondersteunt en begeleidt in hun werking. Dit Support Centre wordt, net als de governance authority, aangestuurd door het **sturend** niveau (Stuurgroep Digitaal Vlaanderen), en geadviseerd door twee **adviserende** instanties (**business** en **technisch**). De Stuurgroep is ook de instantie die de certificering en goedkeuring voorziet van eventuele nieuwe thematische data spaces.

Over het algemeen kan men stellen dat de VSDS met een redelijk klassieke governance structuur werkt, die breed inzetbaar binnen de verschillende domeinen. De keuze voor een **centrale governance authority** die de algemene spelregels uitschrijft en beheert, is in die optiek ook logisch. Gezien de nood aan een aangepast afsprakenkader (of governance framework) per thema, lijkt het echter ook aangewezen een **governance authority op (thematisch) data space niveau** te hebben, die de afspraken, regels en overeenkomsten die domeinexpertise vereisen kan aansturen.



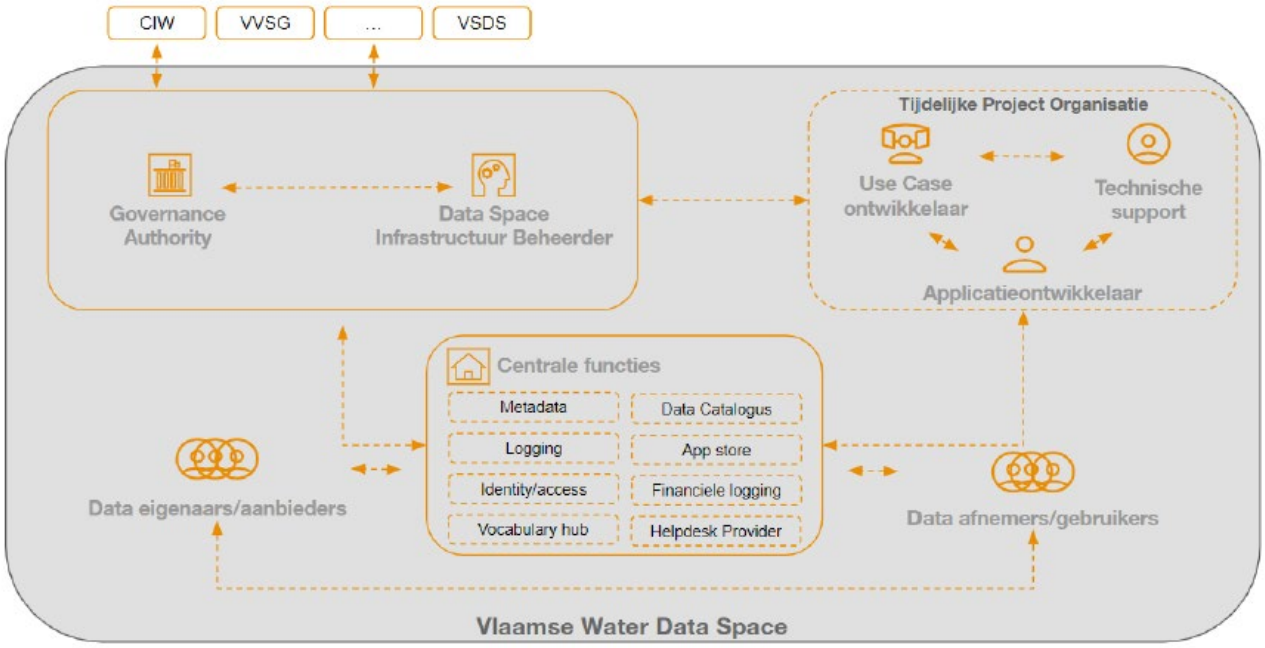
Figuur 15: VSDS: Governance structuur

7.3.5.1.2 Governance structuur (VWDS)

Als een van deze thematische data spaces, bouwt de Vlaamse Water Data Space (VWDS) verder op de richtlijnen en principes van de VSDS. Bovendien heeft het een eigen **governance authority**, die naast de strategie vooral het mandaat heeft om **toezicht** te houden op de goede naleving van de procedures en afspraken, en eventueel aan **handhaving** te doen. Haar rol valt dus sterk samen met die van een superviserend orgaan. De governance authority bestaat uit key stakeholders uit het domein met sterke domeinexpertise en kennis van de data. Verder vallen ook stakeholdermanagement, change management en - vooral - het goedkeuren en implementeren van de use cases onder haar bevoegdheid.

De VWDS plaatst naast de governance authority ook een **Data Space Infrastructuur Beheerder**, die de data space **technisch** uitwerkt, onder andere door het aanleveren en operationaliseren van de componenten. Deze rol komt dus overeen met die van de *Architectural Lead.*

Het is interessant te observeren hoe sterk de governance structuur van de VWDS vooral gericht is op de **operationele dimensie**. Zo voorziet ze, naast een operationeel gerichte governance authority en een (technisch uitvoerende) Data Space Infrastructuur Beheerder, ook in een interne **geformaliseerde structuur voor projectmanagement voor use cases**, met duidelijk gedefinieerde taken en rollen voor *use case ontwikkelaar*, *technische support*, en *applicatieontwikkelaar*. Dit valt uiteraard te verklaren door de sterke verweving met de VSDS, die reeds een groot deel van de algemene en data-technische governance op zich neemt, waardoor het beheer van de VWDS zelf meer operationeel en uitvoerend gericht is. Deze keuze houdt steek voor een data space die integreert met de principes en richtlijnen van VSDS, maar is minder geschikt voor een health data space, waar er een veel grotere complexiteit heerst op vlak van data- en privacygevoeligheid. Het goed en correct omgaan met die gevoeligheden (wettelijk, ethisch, data-technisch ...) vereist een governance authority met een ruimer mandaat en meer slagkracht.



Figuur 16: VWDS: Governance structuur

7.3.5.1.3 Accession agreement (VWDS)

Tot slot is de VSDS ook interessant in haar benadering tot de toetredingsvereisten voor deelname. Zo heeft zij, conform de verwachting van de VSDS naar een eigen afsprakenkader per thematische data space, een aantal basisdocumenten opgesteld, die samen een soort van **accession agreement** vormen. Aangezien deze nog in de ontwerpfase zitten en (nog) niet publiek beschikbaar zijn, behouden we ons het recht deze enkel high-level te bespreken, met de nadruk op die elementen die inspirerend werden bevonden, of die parallel lopen aan de keuzes die gemaakt zijn in het voorstel voor een accession agreement van een health data space.

- ***Oprichtingsverklaring***: dit document wordt vereist door de VSDS en zet de **visie** en **missie** uit. Het omvat ook een intentieverklaring die onder andere vastlegt dat de VWDS de basisprincipes van de VSDS zal aanhangen.
- ***Governance charter***: dit document omvat een definitie van de verschillende (**operationele) rollen en verantwoordelijkheden**[407] binnen de VWDS, en legt een aantal bijkomende **werkafspraken** vast die aan het datatechnische raken (bijvoorbeeld rond datakwaliteit of change management). In het governance charter wordt sterk de nadruk gelegd op het beschrijven van een aantal **processen** die cruciaal zijn voor de goede operationele werking van de data space, zoals bijvoorbeeld de on- en offboardingsprocedure of data-uitwisselingsprocedure. Deze aanpak lijkt een interessante aanvulling op een klassieke toetredings-overeenkomst die meer op regels en afspraken berust, omdat het een duidelijk referentiekader biedt hoe de data space beheerd zal worden. Om die reden werd de on- en offboardingprocedure ook opgenomen in de template voor een accession agreement van een health data space.

[407] *De VWDS heeft een erg diepgaand overzicht opgesteld van de verschillende mogelijk rollen, met een duidelijke omschrijving van het type (beleid en richtlijnen; strategisch en operationeel; technisch), de noodzakelijkheid, en de specifieke taken en verantwoordelijkheden. Het is een sterk geformaliseerde aanpak, die enerzijds veel duidelijkheid schept, maar anderzijds ook restrictief kan werken.*

> ***Deelnemersverklaring***: de deelnemersverklaring omschrijft de **algemene voorwaarden**[408] tot deelname, en raakt aan meer *legal* onderwerpen zoals IP, gegevensbescherming, aansprakelijkheid, etc. Het legt ook vast welke **specifieke rol** de kandidaat-participant zal opnemen, en wat de dienovereenkomstige taken en verantwoordelijkheden zullen zijn.

De verschillende basisdocumenten bieden samen een relatief volledig overzicht van verschillende onderwerpen die in de accession agreement aan bod moeten komen om een duidelijk kader voor deelname te scheppen, en kan daarom, na publicatie, als voorbeeld dienen om richting te geven aan de accession agreement van een health data space.

7.3.5.2 Athumi

Athumi (zie ook 3.4.3.1 Athumi) werd eind 2022 opgericht als het Vlaamse datanutsbedrijf, en heeft als doelstelling de "veilige gegevensdeling en datasamenwerking in datagedreven ecosystemen te stimuleren, met aandacht voor de bescherming van de gegevens van de burgers en met minimale administratieve lasten" (Athumi, 2023). Als deel van haar aanbod naar de markt, bouwt en beheert het onder andere een aantal dataplatformen[409] - waaronder de op Solid-technologie[410] steunende *Pods* (Personal Online Datastore; zie ook de volgende sectie voor meer informatie over governance voor Solid) – en aanvullende diensten, waaronder facturatie.

Athumi kwam binnen dit onderzoekstraject vaak aan bod als potentiële partner, onder andere om de rol van clearing house op te nemen. In de gesprekken met hen, kwam ook hun *huidige* (en eventueel toekomstige) *governance structuur* aan bod.

7.3.5.2.1 Governance structuur

De governance structuur van Athumi volgt die van een **klassieke onderneming**, met een Raad van Bestuur (RvB, Bestuursorgaan) en een operationeel (management)team. Daarbovenop steunt Athumi ook op een Adviescomité, en is er afvaardiging van twee regeringscommissarissen[411] (eenzelfde structuur vindt men in grote lijnen trouwens terug bij eHealth). De verschillende organen voeren volgende taken uit:

> **Raad van bestuur**: strategische visie en beslissingen, toetredingsvoorwaarden (op aanbeveling van het Adviescomité).
  - De voorzitter van de RvB wordt aangesteld door de Vlaamse Regering.

> **Operationeel (management)team**: in de praktijk brengen van strategische beslissingen.

> **Adviescomité**: formuleert aanbevelingen rond het gebruik van en toegang tot persoonsgegevens, en het algemeen veiligheidsbeleid.
  - Het Adviescomité wordt aangesteld door de Vlaamse Regering.
  - Bestaat uit experts op vlak van datatechnologie en data- en informatieveiligheid.
  - Vaste benoemingen en plaatsvervangende leden, om belangenvermenging te vermijden.

> **Regeringscommissarissen**: controleren of de werking en begroting overeenstemmen met de statuten en de samenwerkingsovereenkomst met Vlaanderen.
  - De regeringscommissarissen zijn afgevaardigd door de Vlaamse Regering.

---

[408] *De Algemene Voorwaarden dekken onderwerpen af als lidmaatschap, datagebruik, funding, enforcement ...*

[409] *Alhoewel Athumi vandaag een aantal technologische oplossingen heeft ontwikkeld, geeft het ook aan dat het deze rol in de toekomst zo weinig mogelijk wil opnemen, en het bouwen van componenten liever aan de markt laat.*

[410] *Voor meer informatie over de Solid-technologie, zie ook 3.4.3.3* **Fout! Verwijzingsbron niet gevonden.**. *Voor meer informatie over governance voor Solid, zie 7.3.5.5* **Fout! Verwijzingsbron niet gevonden.**.

[411] *Athumi is een verzelfstandigde onderneming, maar Vlaanderen is nog steeds meerderheidsaandeelhouder, en vaardigt twee regeringscommissarissen af om controletaken uit te voeren.*

Achterliggend wordt de RvB, conform de normale gang van zaken, aangesteld door de **Algemene Vergadering**.

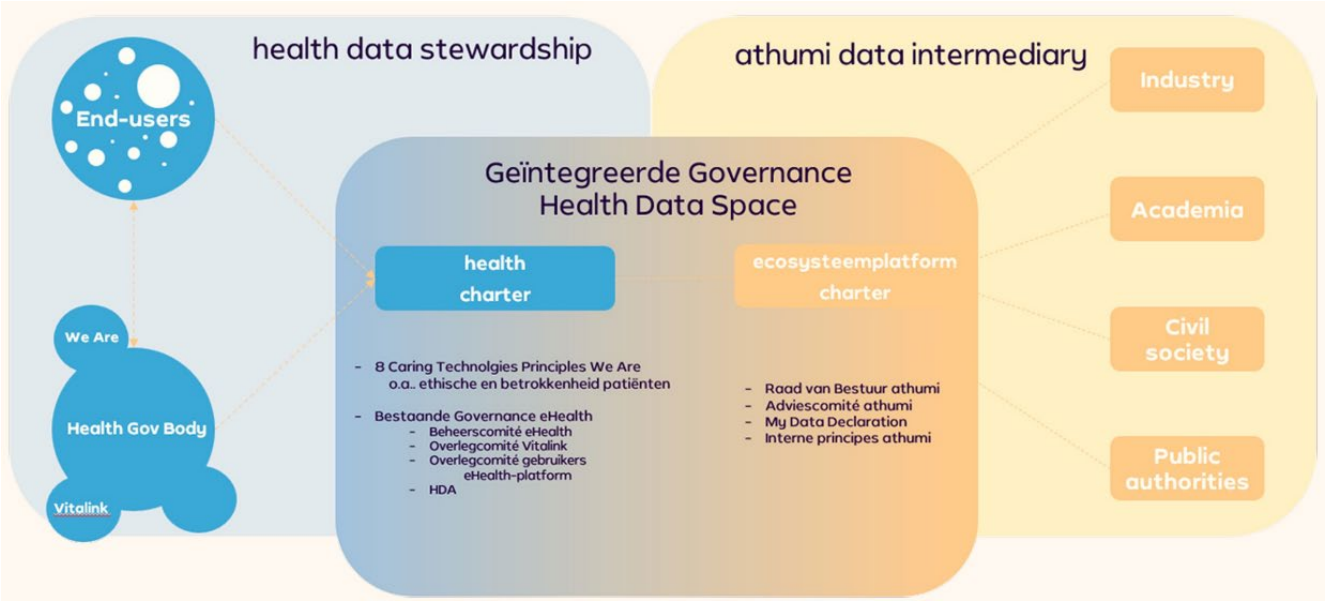
In grote lijnen vindt men hier dezelfde structuur terug die ook in het voorstel voor de health data space naar voren werd geschoven, met een 'drievuldigheid' bestaande uit een **strategisch** orgaan, een **operationeel** of uitvoerend orgaan, en een **controlerend** orgaan. In tegenstelling tot de health data space, die ambieert politiek onafhankelijk te zijn, is Athumi wel sterk **verweven met de Vlaamse overheid**, die haar meerderheidsaandeelhouder is, en die bijgevolg een stevige vinger in de pap te brokken heeft wat betreft de aanstelling van individuen binnen de governance organen.

Een tweede verschil situeert zich op het niveau van de operationele werking, en het belang van dataveiligheid. Aangezien Athumi ook individuele persoonsgegevens beheert (via onder andere de pods), heeft men ervoor gekozen een vierde governance-orgaan te installeren: het Adviescomité, dat zich specifiek buigt over **gegevenstoegang en -veiligheid**. Voor de health data space, die in eerste instantie enkel met geaggregeerde gegevens werkt, werd dit niet nodig geacht, en wordt aangeraden voornamelijk op externe expert-adviseurs (zoals het IVC) te vertrouwen.

7.3.5.2.2 Andere relevante learnings

In haar werking focust Athumi sterk op het verhelderen van de **dataflows en de bijhorende rollen en taken** voor de **use case participant**. Daarbij spreken zij niet enkel over de klassieke data-uitwisselingsrollen (data user, data provider ...), maar hebben ze deze aangevuld met onder andere GDPR-rollen (zoals verwerkingsverantwoordelijke), en met specifieke terminologie die zijzelf hanteren als datanutsbedrijf (bijvoorbeeld aanleveringsentiteit, ontvangende entiteit). Voor *elke* verwerking of dataflow worden deze rollen gemapt en uitgetekend. Het voordeel van deze aanpak is uiteraard dat men een erg duidelijk en helder beeld krijgt van de datanoden binnen de use case, maar anderzijds is dit proces ook erg arbeidsintensief, en, naar eigen zeggen, **niet schaalbaar**. Op termijn wil Athumi deze taken dus outsourcen, bijvoorbeeld door op zoek te gaan naar partners en connectoren (Doccle, Itsme ...) die deze (educatieve) taak kunnen en willen opnemen.

Gezien de nadruk die Athumi legt op dataveiligheid, mag het niet verbazen dat elke use case gepaard gaat met het indienen van een *request* via een **aanvraagformulier**. Dit aanvraagformulier peilt naar de rechtsgrond, data flows en classificaties (zie bovenstaande), toestemmingsprocedure, etc. en wordt al dan niet goedgekeurd door het Adviescomité, dat op haar beurt doorverwijst naar externe partijen (zoals het IVC) indien nodig. In functie daarvan wordt, aan de hand van een **beslissingstabel**, bepaald welke documenten en overeenkomsten opgesteld moeten worden (bijvoorbeeld joint controller, data sharing agreement ...). Het moge duidelijk zijn dat waar dit proces erg grondig wordt gevoerd en sterk inzet op het correct toepassen van de wetgeving en regulering, het ook een erg **manueel en bureaucratisch** proces is, dat enkel op kleine schaal toepasbaar is.



Figuur 17: Athumi: geïntegreerde governance

Tot slot heeft Athumi een interessante aanpak wat betreft haar governance framework, en de regels en procedures dat het hanteert. Athumi bouwt namelijk verder op het principe van **geïntegreerde governance** (Vanhooreweder, 2024), waarbij zij vertrekken vanuit de **eigen expertise** voor governancethema's waar ze zelf sterk in staan (bijvoorbeeld dataveiligheid), maar vertrouwen op de **domeinexpertise van de use case partners** voor het bepalen van de voorwaarden, vereisten en regels die eigen zijn aan dat domein. Toegepast op het domein gezondheid, wil dit bijvoorbeeld zeggen dat regels met betrekking tot gezondheidsdata of de biomedische principes *niet* onder het beleid van Athumi vallen, maar opgesteld worden op advies van en in samenspraak met de klant, waarbij bestaande modellen zoals die van HDA of eHealth als leidraad worden gebruikt. Gezien de domeinoverschrijdende missie van Athumi, is dit een pragmatische aanpak die toelaat te bouwen **op zowel de eigen sterktes als die van haar partners**. Voor de health data space, die zich duidelijk binnen één domein situeert, is dit minder aan de orde, maar de aanpak kan wel inspirerend werken voor eventuele toekomstige use cases die aan andere thema's raken.

7.3.5.3 FAQIR

De FAQIR Foundation werd opgericht met als ambitie gezondheidsdatastromen te optimaliseren en gezondheidsdata te ontsluiten via (een ecosysteem rond) veilige *personal health data vaults.* De nadruk ligt hierbij op het **primair gebruik** van gezondheidsdata. Vanuit hun diepgaande expertise in zowel data als de gezondheidszorgsector, hebben de twee oprichters erg veel aandacht besteed aan (de werking van) het governance model binnen de FAQIR Foundation. De nadruk ligt hierbij steeds op continue verbetering en *versioning*, waardoor onderstaande governance structuur en framework eerder een momentopname zijn van wat Faqir als een permanente evolutie beschouwt.

7.3.5.3.1 Governance structuur

Gezien haar juridische vorm (een non-profit vzw)[412], bestaat FAQIR uit een **bestuursorgaan** (*Board of Directors)* dat de visie en missie uitzet en de strategische beslissingen neemt. Dit orgaan wordt hierin geadviseerd door een **Ethisch Comité**. Daarboven staat, conform de richtlijnen voor een vzw, nog een **Algemene Vergadering**. Deze organen vormen samen de "Denkers".
Daarnaast bestaat FAQIR nog uit een aantal **operationele (management)organen** (comités en werkgroepen) of "Doeners", zoals bijvoorbeeld:

[412] *Zie hoofdstuk 6.2.2.3 voor meer uitleg over de implicaties van de keuze voor een vzw als legale vorm.*

- ***Patiëntenraad*** (*Patient Advisory Council*), die de belangen van individuele burgers en patiënten vertegenwoordigt.
- ***Datatoegangscomité*** (*Data Access Committee)*, die data-aanvragen onderzoeken en goedkeuren. Zij worden hierin verder ondersteund door de privacy & security teams.
- ***Technologisch adviesorgaan***, dat de technologische infrastructuur beheert en bestuurt.
- ...

Tot slot zijn er ook de "Dromers", een groep **stakeholders** die op vrijwillige basis meedenken over de toekomst en de strategische krijtlijnen op lange termijn mee bepalen.

Ondanks haar (vooralsnog) beperkte schaal, heeft FAQIR dus wel al een **complexe governance structuur**, waarbij de verschillende governancetaken al van in het begin toegewezen zijn aan verschillende organen of werkgroepen. Ze vertrekt bij het aflijnen van die functionele pakketten **vanuit de eigen principes en waarden**: om het principe "community & engagement" te realiseren, betrekt FAQIR de patiënt direct bij het governance proces via een eigen *Patient Advisory Council*; om "privacy & security" te garanderen, zet het een toegewijd *Data Access Committee* op, met ondersteuning van privacy en security teams, etc.
Op die manier wil de stichting zo goed mogelijk anticiperen op de vele vraagstukken die er rond governance binnen het gezondheidsdomein heersen.

7.3.5.3.2 Governance framework

Interessant aan de manier van werken van FAQIR, is dat ze haar govenance framework[413] - net als haar governance structuur - als een *work in progress* ziet. Deelnemers ondertekenen de op het moment geldende voorwaarden, wetende dat deze **gradueel strenger** zullen worden. Zo werkt FAQIR momenteel vaak met **intentieverklaringen** (bijvoorbeeld op vlak van het behalen van bepaalde accreditaties), maar neemt ze in haar voorwaarden ook op dat deze op termijn zullen overgaan in strengere regels.
Bij iedere **update** van de voorwaarden, moeten de kandidaat-deelnemers deze opnieuw expliciet goedkeuren en ondertekenen. Om transparantie te garanderen, maakt FAQIR de huidige en vorige versies van het afsprakenkader[414] steeds publiek beschikbaar via GitHub (***versioning***). Deze manier van werken, waarbij het governance framework voortdurend en transparant in ontwikkeling is, zou ook zinvol kunnen zijn voor de health data space, zeker gezien de nadruk die het ecosysteem legt op transparantie als voorwaarde tot vertrouwen.

Om de verantwoordelijkheden rond correct gebruik te stroomlijnen, hanteert FAQIR doorgaans het beleid dat de samenwerkingsovereenkomst vanuit een organisatie ondertekend wordt, en dat de organisatie dan ook de verantwoordelijkheid neemt voor (het correct gebruik door) haar werknemers[415]. FAQIR vertrekt hier, net als voor veel andere regels, vanuit een **trust-based aanpak**, waarbij de afspraken niet per se (technologisch) afgedwongen worden, maar nageleefd worden op basis van vertrouwen. Deze manier van werken kan, in combinatie met intentieverklaringen en *versioning* van het governance framework, een goede manier zijn om bepaalde afspraken (initieel) vrijer te beheren, en pas op termijn, naarmate men leert uit de praktijk, strikter te handhaven.

Als deel van haar governance framework, heeft FAQIR ook een procedure voor **conflictresolutie** uitgewerkt. Deze procedure vertrekt vanuit een melding die gemaakt wordt binnen een user comité. Het user comité buigt zich dan over de klacht of vraag, en laat zich hier eventueel bij adviseren door de "Denkers" (bestuursorgaan en/of ethisch comité). Uiteindelijk deelt het bestuursorgaan het "finale" (niet-dwingende)

---

[413] FAQIR zelf gebruikt de term 'Code of Conduct' om haar geheel aan interne regels, toetredingsvereisten en algemene voorwaarden te omschrijven. Voor de analyse van hun governance model, hebben we er echter voor gekozen de term 'governance framework' te gebruiken, om verwarring met de eigen definitie van de Code of Conduct (zie 7.4.2.5) te vermijden.

[414] FAQIR werkt steeds met verschillende overeenkomsten voor het afsprakenkader, afhankelijk van het niveau van datadeling. Zo sluit een data owner een andere overeenkomst af met zijn eerstelijnszorgverstrekker (bv. arts), dan met een partij die de data voor secundair gebruik wil raadplegen.

[415] Artsen vormen hierop de uitzondering: zij ondertekenen steeds persoonlijk, niet vanuit een praktijk of vakorganisatie.

advies mee. Indien een bepaald onderwerp meermaals aan bod komt, wordt een evaluatie gemaakt van hoe men dit probleem of die klacht naar de toekomst toe kan vermijden. Elke klacht wordt ook steeds gelogd, zodat issues niet onder mat geveegd kunnen worden.

7.3.5.3.3 Andere relevante learnings

Zoals eerder aangehaald in dit rapport, is het belangrijk om zich ervan te verzekeren dat men hetzelfde conceptueel framework en dezelfde terminologie gebruikt wanneer men het over (onder andere) governance heeft. Daarom ontwikkelt FAQIR (in samenwerking met anderen) een uitgebreide **ontologie** rond data en data governance. Deze zal als template beschikbaar gemaakt worden, en kan dan opgepikt worden door de health data space indien gewenst.

Om zich ervan te verzekeren dat een use case relevant is, hanteert FAQIR een aantal criteria en richtlijnen[416]. Het Data Access Comité valideert of de aanvraag conform deze richtlijnen is, en giet de richtlijnen ook in een soort van **template of checklist** voor een goede **use case**. Ook voor de health data space lijkt zo'n use case checklist een interessant instrument te zijn dat, dixit FAQIR, bij kan dragen tot een verhoogde kwaliteit van de ingediende use cases, en dus meer (her)gebruik van de data op langere termijn.

7.3.5.4 eHealth

eHealth is een federale instantie die de onderlinge elektronische dienstverlening en informatie-uitwisseling tussen alle actoren in de gezondheidszorg wil bevorderen en ondersteunen, met respect voor zowel de persoonlijke levenssfeer van patiënten als voor het medisch beroepsgeheim. eHealth bestaat uit het **eHealth-platform voor data-uitwisseling**, maar biedt verder ook verschillende **andere oplossingen en diensten** aan, waaronder een dienst voor het anonimiseren en pseudonimiseren van gegevens, gebruikers- en toegangsbeheer, een dienst voor end-to-end versleuteling, eHealth-certificaten, etc. Bovenop deze basisdiensten, die het (gratis) aanbiedt, is de eHealth-organisatie ook verantwoordelijk voor het opnemen van een aantal **bijkomende taken** binnen het gezondheidslandschap. Het gaat dan over zaken als het ontwikkelen van relevante ICT-standaarden.
Gezien haar federaal mandaat en scope, mag het niet verbazen dat zowat alle belangrijke actoren binnen het Belgische gezondheidszorglandschap (RIZIV, FOD's, Sciensano, NIC, KCE, FAGG, ziekenhuisnetwerken ...) betrokken zijn bij haar werking. Dit impliceert ook dat de eHealth-organisatie een zware, complexe governance structuur kent.

7.3.5.4.1 Governance structuur

eHealth wordt aangestuurd door een beheerscomité, dat de klassieke taken van een **Algemene Vergadering** uitvoert (goedkeuring van de strategie en visie, en jaarlijkse kwijting van de begroting).
Dit comité bestaat uit 31 leden:

- Voorzitter, met stemrecht.
- 21 stemgerechtigde leden, uit verschillende gezondheids- en overheidsinstellingen zoals het Riziv en FOD Volksgezondheid.
- 4 raadgevende leden met stemrecht voor strategische beslissingen (missie, visie ...). Deze leden zijn ministerieel benoemd vanuit 4 verschillende ministeries, op verschillende beleidsniveaus.
- 6 raadgevende leden zonder stemrecht, met vertegenwoordiging uit onder andere de Kruispuntbank en eerstelijnsactoren.

Alle leden worden voor zes jaar benoemd, met mogelijkheid tot hernieuwing, en ieder lid heeft een aangewezen plaatsvervanger.

---

[416] *Een van de belangrijke criteria bij FAQIR is hergebruik. Zo wordt voor elke ingediende use case gevraagd op voorhand na te denken over mogelijke andere use cases of onderzoeksvragen in de toekomst.*

Het **dagelijks bestuur** wordt uitgevoerd door een **manager**, die wordt benoemd door het beheerscomité en toezicht houdt op de uitvoering van de beslissingen. Hij of zij wordt hierin ondersteund door (minimaal) een *deputy*.[417]

Bovenop deze minimale structuur, met een Algemene Vergadering en een Bestuursorgaan, heeft eHealth ook een **overlegcomité van gebruikers**, dat uit 32 leden bestaat. Zij behartigen de **belangen van de sector**, en moeten voor bepaalde beslissingen verplicht geconsulteerd worden door het beheerscomité.
Het overlegcomité bestaat uit:

- 22 stemgerechtigde leden, met vertegenwoordiging uit de eerstelijnszorg, verzekeringsinstellingen en patiëntenverenigingen.
- 10 raadgevende leden, die de deelstaten en federale overheid vertegenwoordigen.

Dit geheel aan governance-organen wordt **gecontroleerd door twee ministerieel aangestelde regeringscommissarissen**.

Bovenstaande beschrijving van de eHealth governance-structuur illustreert een erg klassiek model, met een sterk hiërarchische structuur. Op het bestuurlijk niveau kent eHealth erg brede vertegenwoordiging, waarbij zowat alle actoren en politieke betrokken instanties een (stemgerechtigd) zitje krijgen. De politieke verstrengeling, die men op elk governance-niveau terugvindt, betekent uiteraard dat men een directe lijn heeft met de politiek, maar ook dat er weinig of geen onafhankelijke koers gevaren kan worden, en dat men gevoelig is aan de richting waaruit de politieke wind waait. Aangezien men de health data space als een apolitieke entiteit wil positioneren, lijkt dit governance-model dus niet geschikt.

7.3.5.4.2 Andere relevante learnings

Waar de algemene governance-structuur niet ideaal lijkt voor een health data space, zijn er wel een aantal andere learnings die inspirerend kunnen werken. Zo heeft eHealth een duidelijk omschreven **klokkenluidersprocedure**, dat bedoeld is voor zowel medewerkers als externe partijen die integriteitsschendingen willen melden.

Men kan er melding maken van **inbreuken** door mensen met een professionele relatie tot de organisatie (gaande van medewerkers tot aandeelhouders en bestuurders of zelfs aannemers of leveranciers) op basis van volgende types overtredingen:

> *Schendingen van wet- en regelgeving*: dit betreft overtredingen van Europese en nationale wetten, besluiten, omzendbrieven, en interne regels die van toepassing zijn op federale overheidsinstanties en hun medewerkers.
> *Risico voor gezondheid, veiligheid of milieu:* overtredingen die een bedreiging vormen voor het leven, de gezondheid, de veiligheid van personen of het milieu.
> *Ernstige tekortkomingen in professionele verplichtingen*: overtredingen die wijzen op ernstige gebreken in het goede beheer of in de professionele verplichtingen binnen een federale overheidsinstantie.
> *Bewust bevelen of adviseren tot een integriteitsschending:* het geven van orders of adviezen die leiden tot integriteitsschendingen.
> *Schendingen in het kader van overheidsopdrachten:* dit omvat overtredingen die plaatsvinden tijdens overheidsopdrachten.

[417] *Deze manager (algemeen directeur) is ook steeds de administrateur-generaal van de Kruispuntbank van de Sociale Zekerheid. De deputy is een van de directeurs-generaal.*

Meldingen kunnen, al dan niet **anoniem**, worden ingediend via een **intern platform**, en moeten gedetailleerde informatie bevatten, zoals de relatie van de melder met het eHealth-platform, een beschrijving van de inbreuk, en mogelijke bewijsstukken. Na ontvangst van de melding onderzoekt een aangewezen persoon (DPO) binnen eHealth of de melding binnen het beleid valt. Indien de melding ontvankelijk wordt verklaard, kan de **DPO** een **onderzoek opstarten**. De melder wordt doorheen het proces op de hoogte gehouden van de voortgang van het onderzoek volgens duidelijke richtlijnen. Bij afronding van het onderzoek wordt de klokkenluider op de hoogte gesteld van de resultaten.

Het opstellen van een gelijkaardige procedure voor het melden van inbreuken of conflictresolutie, lijkt aangewezen voor de health data space, zeker in de context van de accession agreement (zie 7.4.2.4 Governance framework). De hierboven beschreven procedure, met duidelijke voorwaarden, criteria en procesflow, kan daarbij ter inspiratie dienen.

7.3.5.5 Solid

In tegenstelling tot de andere hier besproken entiteiten, is Solid geen organisatie maar een technologie, die het mogelijk maakt **persoonlijke datakluizen (of *pods*) decentraal te beheren en te delen**. Dit maakt dat **data ownership** en privacy **management** volledig in handen van de **individuele burger** blijven. In die zin kan Solid gezien worden als een (gedeeltelijk) antwoord op ethisch-maatschappelijke vraagstukken rond privacy en het onevenwicht in het beheer en de valorisatie van data (zie ook 7.1.3 Governance binnen de context van het domein gezondheid).

Als technologie wordt Solid vandaag reeds ingezet door een aantal relevante actoren in het gezondheids-landschap: zowel Athumi als FAQIR kijken naar Solid om hun doelstellingen op vlak van veilige datadeling te realiseren. Elk van die actoren zet de technologie daarbij in binnen de eigen werking en het eigen governance model. Deze werden hierboven reeds beknopt besproken.

Daartegenover staat echter ook dat een nieuwe technologie ook gelegenheid biedt tot het **introduceren van nieuwe governance modellen**. Zo werden in 2024 een aantal research papers gepubliceerd die een voorstel doen tot ‘governance voor Solid’. Het is dit model dat we hier even kort - als potentieel inspirerend alternatief - willen omschrijven.

In de white paper *Governance Models for Solid Platform Ecosystems* (Vlaamse Overheid, 2024) beschrijven de auteurs een aantal bestaande governance modellen voor datadelingsplatformen aan de hand van 18 parameters. Het traditionele model voor **governance voor data spaces** wordt daarbij omschreven als “**data capitalism**”, waarbij data een *asset* vormen die (financiële) waarde creëren. In tegenstelling tot dit meer klassieke, economisch gedreven model, stelt de paper ook een aantal andere datadelingsmodellen voor, waaronder **datacoöperatieven**. Op deze datadelingsplatformen kunnen **individuele leden hun data gezamenlijk aanbieden** (wat de waarde ervan verhoogt), zonder dat ze hierbij de **controle** over hun data afstaan. Vaak zijn deze datacoöperatieven gericht op het verdedigen van de belangen van hun leden.

Omdat de klassieke datadelingsmodellen - zeker voor persoonsdata - heel wat weerstand oproepen bij individuele burgers (onder andere door een gebrek aan vertrouwen in het fair gebruik van hun data) en gekenmerkt worden door een machtsonevenwicht (waarbij grote organisaties de overhand hebben ten aanzien van het individu), ontstond er steeds meer **nood aan een nieuw technologisch én governance model** dat dit machtsonevenwicht kon adresseren. Daarbij wordt Solid naar voren geschoven als technologisch antwoord, op voorwaarde dat het ook een meer **participatief governance model,** naar voorbeeld van een datacoöperatieve, kan hanteren (Van Damme, Mechant, de Mildt, Dewaele, & Vandercruysse, 2024).

Zo'n governance model, dat gebaseerd is op dat van datacoöperatieven, brengt een aantal **voordelen** met zich mee. Ten eerste kunnen de hoge eisen die anders gesteld worden aan individuele burgers op vlak van **digitale geletterdheid en kennis van de wetgeving** opgevangen worden door het collectief[418]. Bovendien onderschrijven individuen bij toetreding tot de coöperatieve ook de **gemeenschappelijke regels en doelstellingen**, wat de kans op eventuele discussies (bijvoorbeeld over data management en data privacy) verkleint. Door als collectief te handelen, en individuele **data gemeenschappelijk te beheren**, kan een datacoöperatieve ook een **sterkere onderhandelingspositie** innemen dan een individu, en betere voorwaarden (financieel of anders) afdwingen. Dit gemeenschappelijk beheer van de data heeft ook als voordeel dat een datacoöperatieve in zaken als **datakwaliteit, standaardisatie en interoperabiliteit** kan voorzien, bijvoorbeeld door haar leden de nodige tools en ondersteuning aan te bieden (Van Damme, Mechant, de Mildt, Dewaele, & Vandercruysse, 2024).

Samenvattend kan men stellen dat bovenstaand governance model voor Solid grotendeels dezelfde voordelen met zich meebrengt als het klassieke governance model van data spaces: efficiënter beheer via de centrale coördinatie van een aantal richtlijnen, gekoppeld aan meer data autonomie en zeggenschap voor de data owner. Het grote verschil zit uiteraard in de aard van de data owner (institutioneel vs. individueel), en het type data dat hiermee gepaard gaat (geaggregeerd vs. persoonsgebonden). Voor een health data space, die in eerste instantie met geaggregeerde data werkt, is het nieuwe, nog niet beproefde Solid-governance model, niet direct aan de orde. Wil men **op termijn ook Solid-technologie integreren in de health data space** (bijvoorbeeld om persoonsdata aan te kunnen bieden), dan loont het om **dieper in te gaan om de best practices en learnings die men uit het governancemodel van een datacoöperatieve kan halen**.

7.4 GOVERNANCE FRAMEWORK VAN EEN HEALTH DATA SPACE

In tegenstelling tot de governance structuur, leent het governance framework zich er niet toe om het theoretisch kader om te zetten in een (weliswaar op assumpties en hypotheses gebaseerde) concrete suggestie voor de toekomstige health data space. Het governance framework kan **in de huidige conceptuele fase** van de Health Data Space namelijk **onmogelijk in specifieke regels, processen en procedures vertaald worden**, aangezien deze te nauw verweven zijn met - onder andere - de voorkeuren van de uiteindelijke *founding partners* en participanten, de gekozen technologische oplossing(en), of de finale legale en organisatorische vorm.

In plaats van een premature oplijsting van hypothetische regels en processen, werd daarom geopteerd voor een **template** van een ***accession agreement*** (of toetredingsovereenkomst), waarin de basisstructuur voor zo een overeenkomst wordt voorgesteld. Elk van de kernonderwerpen die inhoudelijk aan bod moeten komen, worden besproken, en - met dank aan CiTiP[419] – wordt een suggestie gedaan rond **mogelijke invullingen of toekomstige keuzeopties**. De uiteindelijke stichtende leden kunnen hier op een later moment dan op terugvallen om de finale versie gerichter vorm te geven.

7.4.1 Definities: Governance framework en relevante terminologie

Een governance framework is "**het geheel aan interne regels, processen, vereisten, procedures en principes die de dagelijkse werking van de data space ondersteunen.**" Het framework wordt opgesteld door de Governance Authority van de data space die daarvoor steunt op interne en externe kennis en expertise, zodat het een **effectief en verantwoord beleid** kan voeren.

---

[418] *Een van de uitdagingen bij het beheer van Personal Data Stores is dat het een hoge digitale geletterdheid en expertise vraagt van de gebruiker. Om autonoom zijn of haar datarechten uit te oefenen, wordt impliciet ook verwacht dat de gebruiker kennis heeft van datadeling en wetgeving daarrond. Bovendien is deze hierbij zelf aansprakelijk voor de correcte uitvoering ervan. In een coöperatief model wordt deze kennis door experten binnen de community aangebracht, waardoor de vereisten voor het individu minder strikt zijn (Van Damme, Mechant, de Mildt, Dewaele, & Vandercruysse, 2024).*

[419] *KU Leuven Centre for IT & IP Law - imec*

Zoals de definitie impliceert, omvat het governance framework verschillende en complexe aspecten, die verdere toelichting vereisen. De nodige definities en theoretische omkadering worden in de volgende sectie behandeld. Zo gaan we dieper in op het onderscheid tussen externe regels (opgelegd door externe entiteiten zoals (supra)nationale overheden), en interne regels (opgesteld door de data space zelf). Het zijn de laatste die onder de definitie van een governance framework vallen. De intern opgestelde regels zijn uiteraard onderhevig aan de externe regels. [420]

7.4.1.1 Regels vs. policies

Vooraleer dieper in te gaan op de nuances van een governance framework en de verschillende soorten regels die daarin aan bod komen, is het zinvol even stil te staan bij het onderscheid tussen twee (Engelstalige) termen die vaak door elkaar worden gebruikt: *rules* (regels) en *policies* (overeenkomst).

DSSC definieert ***policies*** als een meer algemene overeenkomst tussen twee (of meer) partijen. Het zet de lijnen uit wat betreft de rechten en plichten van de betrokken partijen. Een *policy* of overeenkomst kan in een set van regels vertaald worden. ***Rules*** zijn dus meer specifiek en bijgevolg directief, en bepalen de specifieke rechten en plichten op microniveau.

In de realiteit wordt het onderscheid echter zelden gemaakt, en wordt vooral de term *rules* of *regels* gebruikt om de verschillende soorten (al dan niet specifieke en directieve) richtlijnen te capteren. De term *policies*, daarentegen, wordt vooral voorbehouden aan de specifieke context van *access*, *usage* of *consent policies* (zie 7.4.1.1 Regels vs. policies voor meer details). Voor de rest van dit hoofdstuk zal deze conventie verder gevolgd worden, en wordt de term *rules* (regels) als overkoepelende term gebruikt.

7.4.1.2 Types regels

7.4.1.2.1 Interne vs. externe regels

Een data space is onderworpen aan twee types regels: interne regels, en externe regels. De **externe regels** verwijzen naar de legislatieve richtlijnen die opgelegd worden **door externe entiteiten**, niet de data space zelf. Vaak gaat het om regionale, nationale of supranationale politieke entiteiten, zoals bijvoorbeeld de EU. De regels en wetten in kwestie zijn ook per definitie **niet-onderhandelbaar en verplicht te volgen**. Relevante voorbeelden binnen de context van de health data space zijn bijvoorbeeld de Data Governance Act, de Data Act, de relevante Belgische of Vlaamse wetten ...

Daarnaast kan de data space, middels de Governance Authority, ook regels **opleggen aan zichzelf en haar participanten**. Deze interne principes en regulaties zijn niet wettelijk bindend, maar scheppen een **bijkomend kader** waarbinnen de data space participanten met elkaar in interactie kunnen treden. De interne regels worden **geconsolideerd in het governance framework** en kunnen in (onder andere) de accession agreement en haar toetredingsvereisten terugkeren[421]. Omdat ze niet wettelijk verplicht zijn, kunnen deze bijkomende regels steeds (her)onderhandeld worden tussen de data space, haar stichtende leden, en haar participanten. Het gebrek aan wettelijke verplichting, wil echter niet zeggen dat de interne regels per definitie vrijblijvend zijn: de data space kan, bij monde van de Governance Authority, steeds **zelf bepalen hoe strikt en afdwingbaar** de interne regels zullen zijn.

[420] *De relevante extern opgelegde regulaties en bepalingen werden bovendien reeds in Hoofdstuk **Fout! Verwijzingsbron niet gevonden.** behandeld.*

[421] *De accession agreement is niet per se gelimiteerd tot enkel een overzicht van de interne regels. In veel gevallen is het aangewezen ook een aantal relevante en courante externe regels en wetten aan te halen in de toetredingsvereisten, om eventuele onduidelijkheid tegen te gaan. De voorbeeldtemplate van de accession agreement in dit document (zie bijlage 6D) omvat dan ook een mix van interne en externe regels.*

7.4.1.2.2 Harde vs. zachte regels

De mate waarin regels strikt en afdwingbaar zijn, wordt bepaald door **twee criteria**:

- ***Formalisatie***: Regels kunnen slechts afgedwongen worden wanneer de eraan onderworpen partij er enerzijds van op de hoogte is, en anderzijds zijn of haar akkoord heeft gegeven. Ondertekende contracten zijn een duidelijk voorbeeld van sterk geformaliseerde afspraken.
- ***Meetbaarheid***: Daarnaast moet men kunnen meten of de regels ook uitgevoerd zijn conform de gemaakte afspraak. Zo kan men bepaalde overeenkomsten over 'goed gedrag' wel formeel op papier zetten en laten ondertekenen (bijvoorbeeld in een code of conduct), maar aangezien 'goed gedrag' moeilijk definieerbaar noch meetbaar is, zal de uiteindelijke uitvoering ervan steeds meer op goodwill berusten.

Regels die aan deze twee criteria voldoen, kan men als ***harde* regels** beschouwen: ze zijn duidelijk afgesproken, en de uitvoering ervan is afdwingbaar via hetzij de wet, hetzij intern opgestelde mechanismes of procedures (bijvoorbeeld via het trust framework). Daartegenover staan de meer ***zachte* regels**: afspraken die men onderling maakt, maar die ofwel niet op papier staan (bijvoorbeeld een mondelinge afspraak), ofwel niet meetbaar en afdwingbaar zijn (en dus op goodwill vertrouwen).

Mate van…	**Afdwingbaar - LAAG**	**Afdwingbaar - HOOG**
Formalisatie - LAAG	bv. mondelinge overeenkomst	
Formalisatie - HOOG	bv. intentieverklaring, code of conduct, …	bv. (ondertekende) bindende overeenkomst, contract, …

● **Hard**
● **Zacht**

Figuur 18: Overzicht harde vs. zachte regels

Het voordeel van **harde regels** is uiteraard dat er **meer duidelijk** bestaat rond de verwachtingen, en dat ze ook toelaten **meer controle** uit te oefenen over de **implementatie** ervan. In het geval van een health data space zou men zo bijvoorbeeld zaken als interoperabiliteit, datakwaliteit of standaarden kunnen afdwingen. Te veel harde regels kunnen echter **beperkend werken** en de aantrekkelijkheid en flexibiliteit van de data space in het gedrang brengen. Door te streng op te treden, kunnen data space participanten zich mogelijk beknot voelen in hun vrijheid, wat kan leiden tot minder participanten en datatransacties. Een solide governance framework probeert dus steeds het evenwicht te bewaren tussen voldoende harde regels om de implementatie te ondersteunen, en voldoende flexibiliteit om ook trust-based te kunnen werken.

7.4.1.3 Types policies

Zoals eerder aangegeven, wordt de term *policies* binnen dit governance framework vooral gebruikt om te verwijzen naar een van volgende drie types: access-, usage- of consent policies (DSSC, 2024).

- ***Access policies*** (of toegangsovereenkomsten) zijn die regels die opgesteld worden rond het **verkrijgen van toegang**. Dit kan zowel op het niveau van de data space zelf, als op het niveau van een specifieke data asset (zoals een data set).
- ***Usage policies*** (of gebruikersovereenkomsten) hebben dan weer betrekking op de regels voor het **correct gebruik** van de data space en haar data assets.[422]
- ***Consent policies*** (of toestemmingsbeleid) zijn specifieke regels die van toepassing zijn wanneer er bijkomende toestemming van derden (vaak data owners) nodig is voor het **(her)gebruik van persoonlijke gegevens**.

[422] *Voor de klassieke usage policies werd een rudimentaire template voorzien ondere Terms of Use, zie Bijlage 7D.*

7.4.1.4 Policies op data asset niveau: digitale contracten

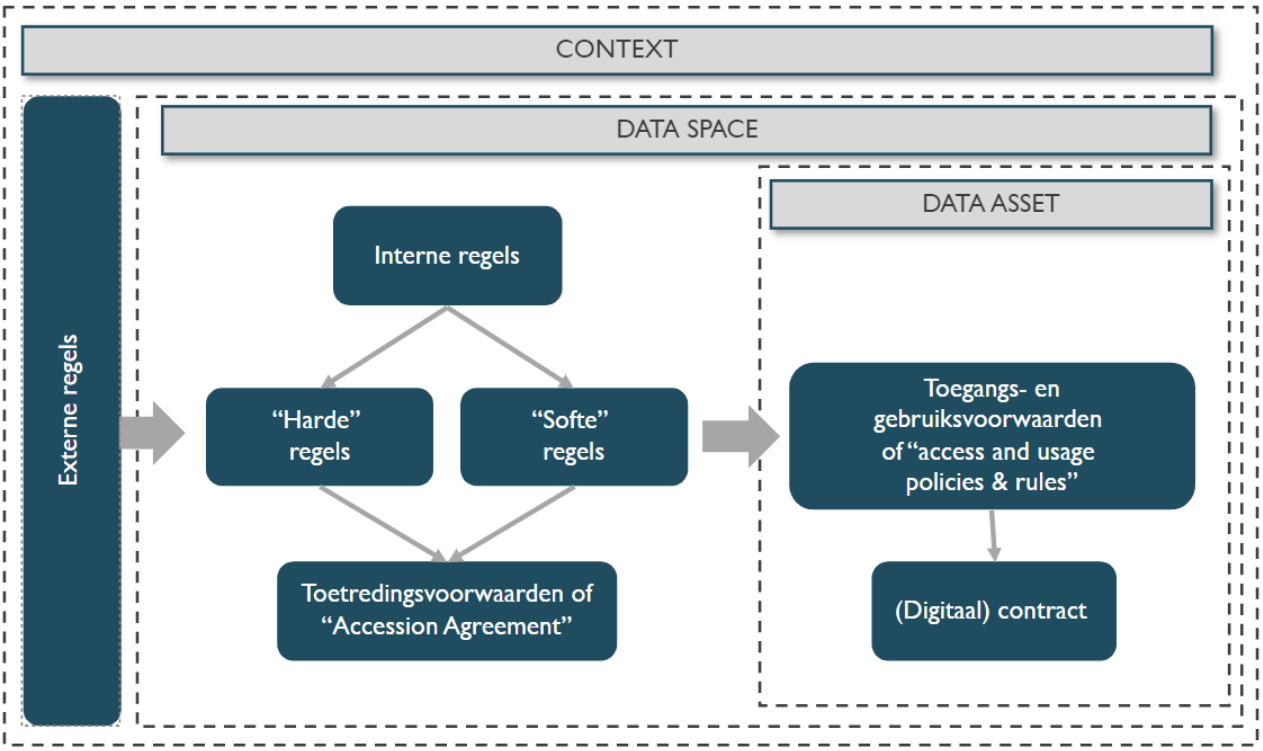
De keuze voor wie de controle heeft over deze policies is erg bepalend voor de richting die men als health data space uit wil. Een data space die **datasoevereiniteit** wil ondersteunen, moet het data providers en data owners namelijk mogelijk maken om soeverein te kunnen beslissen over het gebruik van de eigen data via policies op data asset niveau. De data space zal hiervoor richtlijnen moeten voorzien in haar governance framework, en ervoor moeten zorgen dat de policies implementeerbaar en valideerbaar zijn via het trust framework.

Deze specifieke afspraken, gemaakt op data asset niveau, komen bovenop de generieke toetredings-voorwaarden van de data space, en zijn van tel vanaf het moment dat een data asset aangeboden of gebruikt wordt. Ze worden finaal opgenomen in een **(digitaal) contract** tussen een data (asset) provider en een data (asset) consumer.

7.4.1.5 Policies op data space niveau: toetredingsvoorwaarden en accession agreement

Naast de verschillende overeenkomsten op niveau van de data asset, zijn er ook specifieke toetredingsovereenkomsten die men kan opstellen **op het niveau van de data space zelf**. Deze zetten de voorwaarden uit waar participanten zich akkoord mee zullen verklaren wanneer ze toetreden tot de data space. De toetredingsvoorwaarden kunnen zowel interne als externe regels omvatten, en kunnen zowel hard als zacht zijn. Ze omschrijven zaken zoals de afgesproken **rollen en verantwoordelijkheden** (*governance structuur*); de **gedragscode** (*code of conduct*) en de specifieke regels en policies rond het **gebruik, de interpretatie, en de uitwisseling van data** (*terms & conditions*). Ook andere voorwaarden zoals IE-rechten, gegevensbeschermingsvoorwaarden, (cyber)security, risk management, datakwaliteit, etc. kunnen mee opgenomen worden in de toetredingsvoorwaarden.

Het geheel aan toetredingsvoorwaarden kan, voorafgaand aan de onboarding, opgenomen worden in een (gestandaardiseerd) document, dat men ook wel de **accession agreement** noemt. Dit stichtend document wordt bij toetreding ondertekend door de kandidaat-deelnemer, en is bindend. De voorwaarden zoals omschreven in de accession agreement kunnen steeds verder aangevuld worden met digitale contracten, die de specifieke bepalingen op data asset niveau vastleggen.



Figuur 19: Overzicht: types regels en voorwaarden in een data space

7.4.2 Voorstel: accession agreement

7.4.2.1 Wat is een accession agreement?

Zoals hierboven omschreven, is de accession agreement een **officieel en bindend document** dat bij toetreding ondertekend wordt door de kandidaat-deelnemer. Het omvat een aantal **toetredingsvereisten, regels en overeenkomsten** die de voorwaarden tot deelname aan en gebruik van de data space vastleggen. Deze kunnen **zowel externe regels** (denk hierbij aan bijvoorbeeld wettelijk opgelegde bepalingen met betrekking tot informatieveiligheid, gegevensbescherming etc.) **als interne regels** (zoals de usage policies op data space niveau) omvatten.

Naast deze meer strikte of harde regels en bepalingen, die grotendeels overeenkomen met het **governance framework**, kan de accession agreement ook een aantal andere onderwerpen omschrijven. Een goed onderbouwde accession agreement illustreert bijvoorbeeld ook de **strategische missie, visie en leidende principes** van de data space (zie ook 7.2.2Bouwblok 1: Scope en principes), en omschrijft welke rollen en verantwoordelijkheden er gedefinieerd zijn om deze strategie te kunnen realiseren. Het omvat dus ook een sectie die de **governance structuur**, governance authority en governance-organen beschrijft (stap 2). Bepaalde **interne regels** (usage policies) en **interne procedures**, zoals die voor on- en offboarding, een datalek, of conflictresolutie, kunnen hier al (high-level) in worden beschreven. Tot slot is de accession agreement ook een uitgelezen moment om ook de meer **zachte regels**, zoals ethische richtlijnen voor goed gedrag (of ***code of conduct***) op papier te zetten.

In de volgende secties worden de verschillende mogelijke **onderdelen van een accession agreement** kort besproken. De nadruk wordt hierbij gelegd op welke inhoudelijke items erin aan bod moeten komen. Deze theoretische omschrijving wordt ook aangevuld met een meer concrete toepassing in de vorm van een **template** (zie Bijlage 6.D Accession Agreement), waarin een voorbeeldstructuur met (high-level) invulling wordt gepresenteerd. De specifieke invulling van de hierin voorgestelde items zal, zoals steeds, afhangen van de finale keuzes die de stichtende leden maken. De template is dus geen finaal document, maar biedt vooral een praktisch vooronderzoek waarop de founding partners later kunnen terugvallen om efficiënt en gericht een accession agreement op te stellen.

7.4.2.2 Strategische context

Dit eerste mogelijke onderdeel van de accession agreement schept het **strategisch en situationeel kader** waarbinnen men de toetredingsvoorwaarden van de data space, en de data space zelf, moet situeren. Het beschrijft hierbij niet alleen de verschillende onderwerpen die ook in governance bouwblok 1 aan bod komen (missie, visie, scope, principes van de data space), maar ook de (domeinspecifieke) context waarbinnen het ecosysteem opereert, en de problemen of uitdagingen die aanleiding hebben gegeven tot het oprichten van een data space. Meer specifiek beschrijft het:

- **Context**: in welk domein situeert de data space zich, en wat zijn daar de grote trends of uitdagingen?
- **Visie**: waarom bestaat de data space? Welk probleem lost het op?
- **Missie**: wat wil de data space bereiken? Welke impact wil ze hebben?
- **Scope**: wat wil de data space wel en niet doen? Wat is haar ambitie?
- **Principes**: welke waarden en principes wil de data space uitdragen?

Alhoewel al deze onderwerpen hier idealiter in aan bod komen, is het niet de bedoeling een erg diepgaande analyse te maken van de strategische context. Een **beknopte omschrijving** (in maximaal enkele paragrafen) volstaat.

7.4.2.3 Governance structuur en rollen

In de introductie werd al beschreven hoe de accession agreement het afsprakenkader schept waarbinnen de toegang tot de data space beheerd wordt. Vooraleer men deze afspraken en regels in meer detail toelicht, is het zinvol ook even stil te staan bij de governance structuur: het geheel aan organisatorische rollen en functies die deze regels vormgeven, onderhouden, en reguleren.

In eerste instantie is het aangewezen de bestaande **data space rollen** kort toe te lichten en te definiëren. Verwijzend naar de nomenclatuur die men kiest te hanteren (zie *governance bouwblok 0: conceptueel ontwerp*), kan men hier meer toelichting geven bij wat men verwacht van een partij die (bijvoorbeeld) de rol 'data user' of 'data provider' opneemt. Deze definitie van de rollen kan aangevuld worden met een overzicht van de **functies of taken** die bij die verschillende rollen horen, en eventueel met een specificering van welke rol of taak deze specifieke kandidaat-participant zal opnemen.

Tot slot is de accession agreement ook het uitgelezen moment om de **governance structuur** van de data space meer geformaliseerd toe te lichten aan kandidaat-participanten. Bovenop de functionele rollen van een data space, kan men namelijk ook dieper ingaan op de specifieke ***governancefuncties*** die men nodig acht voor de goede werking van de data space; welke organen er bestaan om deze functies uit te oefenen; en hoe deze organen zich onderling tot elkaar (en/of tot eventuele relevante externe partijen) verhouden.

7.4.2.4 Governance framework

Het hoofddoel van de accession agreement is een meer formeel kader te bieden waarbinnen de **toetredingsvereisten, regels en overeenkomsten** voor deelname aan en gebruik van de data space worden gecodificeerd. Het expliciteren van (een deel van) het governance framework is dus een cruciaal onderdeel van de accession agreement.

De accession agreement kan echter zowel strikter als breder te interpreteren zijn dan het governance framework in het algemeen. Zo kan de accession agreement *breder* zijn omdat het ook een platform biedt waarop een **(selectie van) relevante *externe* regelgevende wetten, verplichtingen of richtlijnen** (denk bijvoorbeeld aan de richtlijnen van de Data Act) geconsolideerd kan worden. Tegelijkertijd is de accession agreement ook *enger* dan het goverance framework, dat *alle* interne regels, procedures en processen beheerst. Zoals reeds gezegd in 7.4.2.1 Wat is een accession agreement?, reguleert de accession agreement namelijk enkel de **algemene regels en afspraken die van toepassing zijn op het niveau van de data space zelf**, en die dus identiek zijn voor alle kandidaat-participanten. Vanuit het principe van datasoevereiniteit zijn er echter ook heel wat (al dan niet gestandaardiseerde) regels en policies die op data asset niveau worden bepaald, en die geformaliseerd worden in digitale contracten of data sharing agreements. Deze afspraken vallen niet alleen buiten de accession agreement, maar overstijgen deze ook: de specifieke overeenkomsten op data asset niveau primeren op de meer algemene afspraken op data space niveau van de accession agreement.

Deze **usage policies** (of gebruiksvoorwaarden) op data space niveau vormen in alle waarschijnlijkheid het meest omvangrijke onderdeel van de accession agreement, en zijn cruciaal aangezien deelname aan de health data space uitsluitend mogelijk is wanneer participanten akkoord gaan met de regels die hierin zijn vastgelegd.

Om het overzicht enigszins te bewaren, hebben we ervoor geopteerd hieronder enkel een **high-level overzicht** te bieden van de mogelijke afspraken die opgenomen kunnen worden in de usage policies. Voor een meer volledig overzicht verwijzen we graag naar de eigenlijke template in Bijlage 6.D Accession Agreement.

7.4.2.4.1 Interne regels (usage policies)

- ***Databronnen:*** Omschrijft afspraken rond welk type data men toelaat (bijvoorbeeld primaire vs. secundaire data).
- ***Dataverwerking en aansprakelijkheid*****:** Omvat afspraken die reguleren of de initiële verwerking van persoonsgegevens in overeenstemming is met de toepasselijke wet- en regelgeving inzake gegevensbescherming. Deze bepalen onder andere wie welke verantwoordelijkheid heeft met betrekking tot bijvoorbeeld het bepalen van een geldige rechtsgrondslag voor verwerking; de voorwaarden en waarborgen met betrekking tot anonimisering of pseudonimisering; of de implementatie van maatregelen om de integriteit van gegevens te garanderen.
- ***Datastandaarden en datakwaliteit***: Deze regels en policies hebben tot doel te waarborgen dat de gegevens bruikbaar, accuraat en betrouwbaar zijn voor de doeleinden waarvoor ze worden gedeeld. Ze beschrijven aan welke standaarden de (meta)data moeten voldoen; en hoe datakwaliteit wordt gedefinieerd en opgevolgd (bijvoorbeeld regels rond het uitvoeren van controles, validatie en correcties, of het documenteren van processen). Indien men voorwaarden wil opleggen in verband met het naleven van de FAIR-dataprincipes, dan kan men deze hier ook opnemen.
- ***Interoperabiliteitsvereisten*****:** Omschrijving van de technische standaarden en protocollen waaraan een data space deelnemer zich moet houden opdat de gegevens direct bruikbaar zouden zijn door de verschillende systemen, platformen en applicaties die door de health data space worden gebruikt. Het omschrijft ook wie de verantwoordelijkheid heeft voor interoperabiliteitstesting en het nemen van corrigerende maatregelen. Eventuele sancties bij het niet voldoen aan de interoperabiliteitsvereisten kunnen hier ook omschreven worden.
- ***Datagebruik*****:** Dit onderdeel beschrijft de voorwaarden voor het gebruik van de aangeleverde data, en wat de toegestane doeleinden en termijnen voor gebruik zijn. Deze bepalingen kunnen verschillen voor data providers en data consumers. Onderwerpen die bij beide types deelnemers aan bod komen zijn bijvoorbeeld de beperkingen op de verdere verwerking en deling van de gegevens, en de aansprakelijkheid bij misbruik. Voor data consumers kan men hier ook een dataretentieperiode vastleggen, met een omschrijving van de geijkte procedure bij voortijdig stopzetten van gebruik (zie ook: *offboarding*). Tot slot kan men hier ook relevante (technische) procedures (bijvoorbeeld ter identificatiemanagement, validatie en controle) beschrijven. Afwijkende voorwaarden kunnen steeds in de data sharing agreements omschreven worden.
- ***Risicobeheer*****:** Omschrijft de verantwoordelijkheid en aansprakelijkheid voor het identificeren, evalueren en mitigeren van risico's die verband houden met de levering en het gebruik van datasets binnen de health data space, inclusief de samenwerking hiertoe met de governance authority en eventuele meldingsplicht bij risico-incidenten. Voor data consumers wordt hier ook melding gemaakt van de verplichte beraadslaging door het Informatieveiligheidscomité bij verzoek tot toegang tot sociale persoonsgegevens.
- ***Beveiligingsmaatregelen*****:** Dit omschrijft het geheel aan maatregelen rond gegevensbescherming, onder andere op vlak van cybersecurity en het need-to-know principe[423].
- ***Renumeratiemodel*****:** Indien de data space betaling vraagt voor een of meerdere diensten, of lidgelden vraagt, dan omschrijft deze sectie de modaliteiten tot betaling.
- ***Intellectuele eigendom (IE) en confidentialiteit:*** Beschrijft wat er gebeurt met nieuwe IE-rechten die door een partij gecreëerd worden.
- ***Andere bepalingen en voorwaarden:*** Bijvoorbeeld bepalingen specifiek voor data intermediaries, vereisten in verband met neutraliteit, of het al dan niet exclusief gebruik van de health data space.

[423] *Het need-to-know principe is een security-concept dat toegang tot gevoelige gegevens wil beperken, onder andere door enkel toegang te geven tot gegevens aan die individuen of entiteiten die er daadwerkelijk nood aan hebben om hun functie te kunnen uitvoeren. Door dit principe aan te hangen, kan men het risico op onrechtmatige toegang of datamisbruik beperken.*

7.4.2.4.2 Externe regels

> ***Toepasselijkheid van bestaande wetgeving***: Onder dit hoofdstuk kan men een overzicht geven van het juridisch kader waarbinnen de health data space opereert. Participanten blijven daarbij steeds zelf verantwoordelijk voor de naleving van alle relevante nationale en internationale wetten, regelgeving, en richtlijnen op vlak van gegevensbescherming, gezondheidszorg, cybersecurity, etc.:
  - *Wetgeving rond privacy en persoonsgegevens*: omvat de geldende regels wat betreft consentmanagement; anonimisering; het verbod op de combinatie van datasets in de context van re-identificatie; meldingsplicht bij re-identificatie; en afspraken ter risicomitigatie.
  - *Geografische afbakening* (in het bijzonder voor verwerkingen buiten de Europese Economische Ruimte)
  - *Rechten van de betrokkenen*, inclusief het recht op inzage, gegevenswissing, beperking van verwerking, etc. (GDPR-regelgeving).
  - *Verwerkingsverantwoordelijkheid*, inclusief het recht van datagebruikers om een of meerdere verwerkers in te schakelen.

7.4.2.4.3 Procedures

Ter aanvulling van deze regels en afspraken (usage policies) kan het governance framework ook een aantal belangrijke procedures uitschrijven en toelichten:

> ***Data-uitwisselingsprocedure***: Omschrijft de (technische) procedure tot data-uitwisseling, met de verschillende fases die daarmee gepaard gaan.

> ***Meldingsplicht bij regelgevend conflict****:* Indien een (of meerdere) van de interne regels van de accession agreement niet overeenstemt met de wetgevende verplichtingen of een bevel van een toezichthoudende autoriteit, dan is een deelnemer verplicht hier zo spoedig mogelijk melding van te maken. De melding moet dan aan een afgelijnde procedure voldoen, en heeft als consequentie dat de meldende partij niet gesanctioneerd kan worden voor het niet-naleven van de regels die voortvloeien uit desbetreffend conflict.

> ***Onboardingsprocedure***: Deze sectie legt de standaardprocedure tot toetreding uit aan de hand van een aantal te doorlopen stappen. Deze procedure kan verschillen naargelang de rol van de deelnemer.

> ***Offboardingsprocedure***: Hier legt men de procedure uit tot uittreding uit de data space. Minimaal zal men hier twee mogelijke pistes moeten omschrijven: vrijwillige uittreding (bijvoorbeeld omdat deelname aan de data space niet langer in de strategische missie van de deelnemer past), en gedwongen uittreding (wanneer de governance authority een deelnemer uit de data space zet volgens duidelijk gedefinieerde criteria en voorwaarden).

> ***Handhaving en Sanctionering***: De health data space zal, als deel van haar werking, op verschillende niveaus aan handhaving (en eventueel sanctionering) doen. De procedures die daarbij horen kan men hier verder toelichten:
  - ***Auditrechten***: Omschrijft onder welke voorwaarden en met welk doel het bevoegd (superviserend) orgaan een audit van een data space participant kan aanvragen. Verder licht het de eigenlijke audit-procedure toe, met een duidelijke omschrijving van de scope en welke partij(en) als auditor mogen optreden. Tot slot worden de eventuele sancties verbonden aan vaststellingen tot niet-naleving omschreven.
  - ***Geschillen en Conflictresolutie***: In het geval van een conflict tussen twee of meerdere partijen, kan men een aantal mogelijke routes volgen (zoals onder andere 1. minnelijke schikking, 2. ethisch comité, 3. rechtbank (Nederlandstalige Rechtbank van Eerste Aanleg Brussel of Ondernemings-rechtbank)), met een beknopte omschrijving van welk type dispuut via welke weg benaderd moet worden. Elke data space zal binnen die context ook moeten nadenken over de **aansprakelijkheid**s-vorderingen die participanten aan elkaar kunnen richten, voornamelijk binnen de context van eventueel geleden schade ten gevolge van (bijvoorbeeld) nalatigheid door een andere partij.

De accession agreement moet hier omschrijven welk type schade eventueel in aanmerking komt voor compensatie en wat de (maximale) bedragen zijn die men op elkaar kan verhalen.

- ***Klokkenluidersprocedure***: Indien gewenst kan men een geijkte procedure opstellen voor het melden van overtredingen begaan door personen die een professionele relatie hebben tot de health data space (bv. medewerkers, onderaannemers ...). Die procedure, alsook de voorwaarden waaraan voldaan moet worden, kan men hier omschrijven. Dezelfde procedure kan ook publiekelijk gedeeld worden (bijvoorbeeld via een website), zodat ook externen die geen deelnemer zijn aan de data space melding kunnen maken.

> ***Wijzigingen aan de accession agreement of usage policies***: Beschrijft onder welke voorwaarden en omstandigheden de accession agreement of de usage policies gewijzigd kunnen worden, en welke procedure ter (weder)goedkeuring hiermee gepaard gaat. Indien er aan versioning wordt gedaan, kan men hier omschrijven hoe en waar de oudere versies geconsulteerd kunnen worden.

> ***Duur van de overeenkomst***: Op het einde van de accession agreement kan men ook nog een sectie invoegen rond de modaliteiten van de accession agreement zelf. Deze omschrijft vanaf wanneer ze in gaat, en vanaf wanneer haar voorwaarden niet langer van toepassing zijn op de ondertekende partij.

Tot slot merken we graag nog even op dat niet alle regels en afspraken die in de accession agreement staan, even bindend hoeven te zijn. Sommige overeenkomsten kunnen eerder op goodwill of intentie berusten. In zo'n scenario kan het helpend zijn met een **intentieverklaring** te werken. De kandidaat-participant verbindt zich dan tot een 'best effort' om de intentie te halen, maar heeft geen harde verplichting naar resultaat toe. Dit kan al dan niet gecombineerd werden met een afgesproken termijn, bijvoorbeeld om een transitieperiode af te spreken waarbinnen men van een commitment op intentie of effort naar een resultaatsverbintenis evolueert[424]. De enige voorwaarde hierbij is dat de aard van het engagement duidelijk omschreven staat.

7.4.2.5 Code of conduct

Als laatste onderdeel van de accession agreement kan men ook een apart stuk voorzien voor alle interne regels en richtlijnen die moeilijk hard te maken zijn, bijvoorbeeld omdat ze zich niet goed laten definiëren of meten. Het gaat dan in het bijzonder om weinig tastbare aspecten zoals ethiek en goed gedrag. Door deze helder te maken, kan men als data space een **bijkomend kader** scheppen dat richting geeft aan hoe data space participanten met elkaar (of anderen) in interactie treden.

Dit geheel aan **gedragsregels** (of *code of conduct*) kan (onder andere) onderwerpen als discriminatie, onpartijdigheid, of (seksuele) intimidatie en grensoverschrijdend gedrag beschrijven. Men kan hierbij gedragsregels vastleggen voor 'goed gedrag' binnen de context van de werking van de data space zelf, maar ook voor gedrag dat plaatsvindt in interacties met het ecosysteem in bredere zin. Indien men beperkingen wil opleggen naar het gebruik van andere data spaces toe, dan kan men die hier eventueel toevoegen. De *code of conduct* is ook het uitgelezen moment om relevante (algemeen geldende) **ethische principes** uit te leggen. Voor het domein gezondheidszorg zou men hier de vier biomedische ethische principes naar voren kunnen schuiven (zie ook hoofdstuk 6.1 Contractueel kader).

Net zoals voor alle andere regels en richtlijnen die opgenomen zijn in de accession agreement, is het belangrijk dat de code of conduct van in het begin duidelijk maakt wat de **consequenties** (en bijhorende procedures) zijn voor het overtreden ervan. Dit schept duidelijkheid, en vermijdt eventuele latere discussies.

[424] *Een mogelijke toepassing van een intentieverklaring (al dan niet met termijn) zou het afdwingen van een harmonisatiestandaard als OMOP kunnen zijn. Zo zou men kunnen vragen dat alle datasets OMOP-compliant zijn, maar in eerste instantie enkel een best effort vragen. Op termijn, bijvoorbeeld na 5 jaar, kan de 'overgangsperiode' aflopen, en kan men de vereiste strikter gaan afdwingen.*

7.4.2.6 Accession agreement: template

Finaal is de accession agreement een stichtend document, dat het speelveld voor deelname aan de data space gelijktrekt voor alle participanten middels duidelijke regels, afspraken, voorwaarden en verwachtingen. De hierboven beschreven basisstructuur en -onderdelen zijn slechts indicatief, in die zin dat er geen vast formaat bestaat of gehanteerd wordt door reeds bestaande data spaces. Anderzijds omvat een accession agreement volgens bovengenoemde structuur wel voldoende informatie om een duidelijk en helder beeld te scheppen van wat er van participanten verwacht wordt, en welke procedures de data space hanteert om die verwachtingen te realiseren.

Om de eventuele toekomstige leden van een health data space wat meer richting te geven bij het opstellen van hun accession agreement, werd ook een **template** opgesteld die bovenstaande theorie meer concreet uitwerkt en **toepast op het regulerend kader dat geldt binnen het gezondheidsdomein**. Dit document kan men terugvinden in bijlage 6.D.

8 ARCHITECTUUR

In dit hoofdstuk vertrekken we vanuit de technische bouwblokken en microservices die momenteel beschikbaar zijn en al gebruikt kunnen worden voor de technische uitbouw van een data space.
We verdiepen ons in de technische uitwerking naar programmeerbare componenten en hoe deze gebruikt werden binnen de PoC van dit project. Dit hoofdstuk is vooral bedoeld voor wie zich wil verdiepen in hoe een data space technisch werkt.

8.1 ANALYSE ACTUELE DATA SPACE COMPONENTEN

Dit hoofdstuk geeft een functionele beschrijving van de data space componenten en bespreekt wat er momenteel al beschikbaar is op de markt. Voor het lezen van dit hoofdstuk is het aangeraden om paragraaf 3.4.1.2 Technische bouwstenen volgens IDSA **Fout! Verwijzingsbron niet gevonden.** gelezen te hebben.

8.1.1 Connector

De connector is de “sleutel” tot de data space en biedt alle deelnemers aan de data space, zowel data providers als data consumers, toegang tot de data space.

Een connector moet voldoen aan volgende architectuurprincipes:

- **Eenvoudig** te gebruiken en te onderhouden met een kleine en efficiënte kern en zo min mogelijk externe afhankelijkheden.
- **Interoperabel** en **onafhankelijk** van platformen en ecosystemen.
- **Gedecentraliseerd**, waardoor softwarecomponenten met de benodigde capaciteiten om deel te nemen aan verschillende gegevensuitwisselingen aan de kant van de partners kunnen worden gekoppeld. Bovendien moet worden gewaarborgd dat gegevens alleen worden uitgewisseld tussen de overeengekomen punten.
- Alleen toestaan dat gegevens worden overgedragen die fundamenteel aan usage policies zijn gekoppeld via **contractendefinities**, waarbij gegevensbescherming boven gegevensdeling wordt gesteld.
- Metadata scheiden van gegevens, zodat hoge doorvoersnelheden bij de daadwerkelijke gegevensoverdracht mogelijk zijn.
- Ondersteuning van gegevens die zijn gestructureerd volgens consistente semantiek (**ontologieën**), de basis voor digitale waardecreatie.
- Waar mogelijk zorgen dat alle processen zijn **geautomatiseerd**; van identiteitsverificatie van deelnemers tot het waarborgen dat alle contractueel overeengekomen voorschriften voor gegevensoverdracht en gegevensgebruik worden nageleefd.
- Zoveel mogelijk voldoen aan **bestaande normen en protocollen** (IDSA en GAIA-X), waardoor ze interoperabel zijn met de EHDS en andere data space initiatieven.

Met de opkomst van data spaces zijn er verschillende open source communities en private bedrijven begonnen met het uitbouwen van bibliotheken die functioneel aan de IDSA-definities voldoen.
De keuze voor een data space connector heeft een impact op de werking van de data space. Niet alle connectoren werken namelijk op dezelfde wijze.

Om een keuze te maken binnen dit project is er voorafgaand aan de ontwikkelingsfase een **vergelijkende studie** uitgevoerd. Flexibiliteit en maturiteit zijn belangrijke criteria. De meest relevante data space platformen uit de vergelijkende studie vatten we samen in onderstaande tabel:

Naam	Onderhouder	Open source	Actief onderhoud	Uitbreidbaar / flexibiliteit	Documentatie kwaliteit	Opmerkingen
EDC	Eclipse foundation	Ja	ja	ja	matig	Meeste functionaliteiten out-of-the-box
Sovity	Sovity	deels	ja	nee	matig	Gratis en premium versie, gebouwd op oude versie van EDC
True connector	Trusted engineering	Ja	ja	matig	goed	Focus op het Fiware[425] ecosysteem, vendor lock-in
Trusted connector	Frauenhofer	Ja	ja	matig	matig	Meer focus op Internet of Things (IOT) use cases

8.1.2 Broker

De (metadata) broker is een component die toelaat om de beschikbare **metadata** op een gebruiksvriendelijke manier te **verkennen**, waardoor gebruikers gemakkelijker data kunnen vinden.
De broker bevat niet enkel de inhoudelijke informatie over een dataset, maar zal ook weergeven wie deze data aanbiedt en onder welke voorwaarden (usage policy). Het is de taak van de broker om de **aanvragers en aanbieders** van data **samen te brengen.**

De broker is een component die zich niet in de connector van een data consumer of provider bevindt, maar die op een andere locatie **centraal of decentraal** kan staan. De broker is niet te verwarren met een message broker die doorgaans berichten tussen componenten afhandelt en is ook niet actief betrokken bij de daadwerkelijke data-uitwisseling, maar heeft wel alles te maken met de uitwisseling van metadata.
Hij wordt gevoed met de metadata van verschillende connectoren binnen de data space en visualiseert de metadata in een gebruikersinterface. Het doel van de broker is het mogelijk maken om beschikbare datasets te ontdekken.

Belangrijk om op te merken is dat de connectoren van de providers de enige bronnen van waarheid (single source of truth) blijven op vlak van aangeboden datasets. De broker zal regelmatig **synchroniseren met alle connectoren** en op die manier steeds een up-to-date lijst van alle datasets ter beschikking hebben.

Er kunnen meerdere metadata brokers binnen een data space bestaan, bijvoorbeeld om assets per thema te organiseren. Ze kunnen ook verschillende zoekmogelijkheden en grafische interfaces bieden.

Volgens de referentiearchitectuur van IDSA is de metadata broker ook een connector en ondersteunt daardoor dezelfde communicatieprotocollen, maar daarnaast een extra service bevat die de metadata van de andere connectoren kan verzamelen. Bijgevolg is de broker zelf ook een participant met een identiteit in de data space.

[425] *Het Fiware ecosysteem is een framework met opensourceplatformcomponenten. De focus ligt vooral op smart city-oplossingen en duwt de gebruiker naar hun premiumoplossingen met vendor lock-in.*

Een connector die een bepaalde dienst of dataset aanbiedt, kan een beschrijving daarvan naar de broker sturen zodat deze ook door andere participanten kan gevonden worden. In de meeste gevallen dient de broker een gebruikersinterface aan te bieden, die in verbinding staat met een databank waarin alle metadata verzameld wordt, zodat efficiënt gezocht kan worden in de beschikbare metadata.

Aangezien de broker een optionele component is, kunnen er data spaces bestaan zonder broker of met meerdere brokers. Hoe synchronisatie tussen deze brokers opgezet dient te worden (bv. alle brokers zijn gelijkwaardig, of er is één master die gevolgd wordt door de rest) is niet gespecifieerd en te bepalen door de data space beheerder.

In de praktijk zijn er **weinig kant-en-klare brokerimplementaties** die al deze functies aanbieden (die bijvoorbeeld zowel een connector zijn als een user interface aanbieden). Er is de IDS Metadata Broker (van IDSA), maar deze wordt niet verder ontwikkeld. Bovendien zijn er heel wat bestaande datacatalogi die meer geavanceerde zoekfunctionaliteit aanbieden of misschien al gekend zijn door de gebruikers van een data space. Een integratie tussen een connector die de metadata van de andere connectoren verzamelt en een bestaande datacatalogus kan dus ook opgezet worden om de rol van broker te vervullen.

8.1.2.1 OpenMetadata vs DataHub

Er zijn verschillende datacatalogi op de markt die verschillende methoden bieden voor het oogsten en verzamelen van metadata. Elk product heeft unieke kenmerken en benaderingen voor het effectief beheren van metadata. Amundsen, Atlas, DataHub, Marquez, OpenDataDiscovery en OpenMetadata zijn de zes populaire open-source datacatalogi. [426]

Bij het overwegen van opensource datacatalogi voor implementatie in een organisatie, is het cruciaal om verschillende factoren te evalueren, waaronder de aangeboden functies, de identiteit van de ontwikkelaars, de mate van ontwikkelingsactiviteit en de voorkeuren van de gebruikers. Daarnaast kan het identificeren van welke bedrijven het product al gebruiken, nuttige inzichten bieden. Uiteindelijk is het van vitaal belang om ervoor te zorgen dat de gekozen oplossing aan de verwachtingen voldoet wat betreft schaalbaarheid en betrouwbaarheid.

Elk beschikbaar product heeft zijn eigen voordelen en nadelen. Al deze producten kunnen de essentiële functies aanbieden die een health data space broker moet hebben, met als belangrijkste de mogelijkheid om geselecteerde metadata aan te bieden aan aangewezen externe partijen (partijen die (nog) geen deel uitmaken van de health data space).

In deze context vergelijken we OpenMetadata[427] en DataHub[428] omdat ze sterke ondersteuning van de gemeenschap, uitgebreide integratiemogelijkheden en een aanzienlijke nadruk op realtime metadatabeheer bieden, waardoor ze bijzonder goed geschikt zijn voor dynamische data-omgevingen.

OpenMetadata en DataHub delen veel functies, maar ze hebben ook duidelijke verschillen. Hier is een korte samenvatting van de vergelijking[429].

[426] *https://atlan.com/open-source-data-catalog-tools/*

[427] *https://open-metadata.org/*

[428] *https://datahubproject.io/*

[429] *https://atlan.com/openmetadata-vs-datahub/*

Feature	OpenMetadata	DataHub
Search & discovery	Elasticsearch	Elasticsearch
Metadata backend	MySQL	MySQL
Metadata model specification	JSON Schema	Pegasus Definition Language (PDL)
Metadata extraction	Pull and push	Pull
Metadata ingestion	Pull	Pull
Data governance	RBAC, glossary, tags, importance, owners, and the capability to extend entity metadata	RBAC, tags, glossary terms, domains, and the Action Framework
Data lineage	Column-level (soon)	Column-level
Data profiling	Built-in with the possibility of using external tools	Via third-party integrations, such as dbt and Great Expectations
Data quality	Built-in with the possibility of using external tools like Great Expectations	Via third-party integrations, such as dbt and Great Expectations

Figuur 20: Vergelijking OpenMetadata en DataHub

8.1.3 Identity provider

In een data space is er een component noodzakelijk die instaat voor het 'identity & access management' (IAM). Om **toegang** te **krijgen tot een data space** en zijn datasets moet een identiteit geclaimd en geverifieerd kunnen worden (authenticatie). Daarnaast moet het ook mogelijk zijn om toegangsrechten te verbinden aan een identiteit (autorisatie).

Zo is het mogelijk ervoor te zorgen dat **enkel gecertifieerde partijen** toegang hebben tot de data space. Die certificatie kan op verschillende manieren gebeuren, zowel intern als extern aan de data space. Een partij zal een aanvraag moeten indienen bij de autoriserende partij om de certificaten te ontvangen. Deze kunnen dan geverifieerd worden en gekoppeld aan bepaalde rechten. Niet alle data space participanten hoeven dezelfde rechten te krijgen.

Er zijn **verschillende manieren** om de authenticatie en autorisatie te regelen. Het kan zijn dat een **centrale, betrouwbare en neutrale identity provide**r bij elke interactie tussen twee participanten betrokken is. Deze identity provider reikt een token uit met beperkte levensduur die de juiste rechten verleent, waarbij de tegenpartij dan kan controleren dat het daadwerkelijk afkomstig is van die identity provider, en dus betrouwbaar. Dit is een wijd gebruikte en mature oplossing die beschikbaar is in de meeste autorisatiestandaarden.

In de toekomst zullen **gedecentraliseerde oplossingen** belangrijker worden. Hierbij denken we aan decentralized identifiers (DIDs) en verifiable credentials (VCs). Het idee hierachter is dat een entiteit zoals een participant geïdentificeerd kan worden zonder tussenkomst van een centrale autoriteit en dat deze entiteit dan ook zelf kan bepalen welke informatie zij vrijgeeft aan anderen. In dit geval zijn er nog altijd externe partijen zoals de data space autoriteit die credentials uitreiken aan de participant om aan te geven welke toegang hij heeft, maar de participant kan deze zelf beheren.

Vergelijk het met een portefeuille: daarin zit meestal een rijbewijs, bankkaart en identiteitskaart. Als een gemachtigde instantie wil weten of de persoon in kwestie een bankrekening heeft, kan deze enkel zijn bankkaart tonen (misschien zelfs zonder het volledige rekeningnummer) zonder dat hij al zijn overige informatie hoeft te delen. Een nadeel is wel dat de participant in dit gedecentraliseerde geval zelf meer infrastructuur dient op te zetten.

In beide situaties (centraal of decentraal) maakt asymmetrische encryptie deel uit van de oplossing. Er is een private key die de participant geheimhoudt, en een public key die vrij toegankelijk is. De private key wordt gebruikt om berichten van de participant digitaal te tekenen, de public key kan dan gebruikt worden om te verifiëren dat ze daadwerkelijk van hem afkomstig zijn (bij de centrale identity provider die dan zelf een token uitreikt met de juiste rechten, of bij een andere participant in het gedecentraliseerde verhaal).

8.1.4 Clearing house

De clearing house component kan binnen het domein van data spaces een volledig verschillende betekenis hebben op basis van het gekozen ecosysteem. Om die reden bespreken we hier zowel het model van IDSA als dat van Gaia-X.

8.1.4.1 IDSA clearing house

Binnen de referentiearchitectuur van IDSA is het clearing house functioneel gedefinieerd als een data intermediary die ervoor zorgt dat zowel de data provider als de consumer hun **contractuele verplichtingen nakomen**, zoals het delen van gegevens met elkaar volgens een data sharing agreement en data usage policies.

De term "**data usage policies**" zal in het kader van een clearing house vaak vernoemd worden. Het verwijst naar de voorwaarden die gelden om data van een bepaalde dataset te mogen bezoeken.
De voorwaarden kunnen betrekking hebben tot bijvoorbeeld:

> Tijd
  - Bv. Een dataset mag maar 1x per dag en per participant bezocht worden.

> Identiteit, locatie
  - Bv. Enkel bepaalde participanten mogen de dataset bezoeken.

> Velden
  - Bv. Niet alle velden van de dataset mogen bezocht worden.

> Financiën
  - Bv. Enkel als bepaalde financiële transacties gebeurd zijn, kan een dataset bezocht worden.

> Locatie
  - Bv. Enkel Vlaamse organisaties mogen een bepaalde dataset bezoeken.

> …

Er zijn standaarden beschikbaar die het mogelijk maken om usage policies op een gestructureerde manier te beschrijven. Een veel gebruikte standaard is Open Digital Rights Language (ODRL)[430].

Vaak wordt een combinatie van verschillende voorwaarden gebruikt. Op een dataset kunnen bijgevolg meerdere sets van voorwaarden gelden, afhankelijk van wie de data consument is. **De lijst van voorwaarden** die geldig zijn tussen een data consument en een data producent worden vastgelegd in een "**data sharing agreement**" of kortweg contract. In de praktijk zal het de producent zijn die de voorwaarden vastlegt voor het gebruik van een dataset die hij aanbiedt en een data consument zal deze moeten aanvaarden of niet. Echter het systeem biedt ook de mogelijkheid voor bilaterale contractbesprekingen voor specifieke datadelingen.
Het is de taak van het clearing house om de data sharing agreements te bewaren en erop toe te zien dat datatransacties die plaatsvinden ten gevolge van een contract worden uitgevoerd volgens de voorwaarden die in het contract beschreven staan.

[430] *https://www.w3.org/TR/odrl-model/*

Daarnaast verzorgt het clearing house de **logging van alle transacties**. De loggegevens zijn transparant en kunnen door alle participanten geraadpleegd worden. Nuttig voor de werking van de data space, noodzakelijk voor auditdoeleinden.

De rol van het clearing house kan ook omschreven worden naargelang waar in het datadelingsproces de activiteiten plaatsvinden:

> Voorafgaand aan het delen van gegevens: clearingfuncties, zowel:
  - Juridisch: het verifiëren van gebruikscontract en data usage policy
  - Financieel: het verifiëren van betalingsvoorwaarden
  - Technisch: het mogelijk maken van de uitvoering van de transactie en het verbinden van de transactie aan een bepaalde gegevensdelingsovereenkomst en gebruikscontract
> Tijdens het gegevensdelingsproces: monitoring en logging (bv. voor auditing).
> Na het delen van gegevens: afwikkelingsfuncties; facturering/invoicing of conflictresolutie.

Het clearing house handhaaft niet noodzakelijkerwijs de usage policies. De data holder kan dit uitbesteden aan een clearing house, bv. om kosten te minimaliseren, maar het vereist garanties in termen van vertrouwen en gegevenssoevereiniteit. Afhankelijk van het soort policy kan deze geëvalueerd worden bij zowel de data provider of data consumer, of een neutrale derde partij zoals het clearing house.
Ook al outsourcet het clearing house sommige taken, ze is en blijft verantwoordelijk voor de uiteindelijke clearing van een datatransactie.

Gedurende de looptijd van dit project waren er **geen bruikbare implementaties** bekend van een clearing house volgens de IDSA-richtlijnen.

8.1.4.2 Gaia-X Digital Clearing House

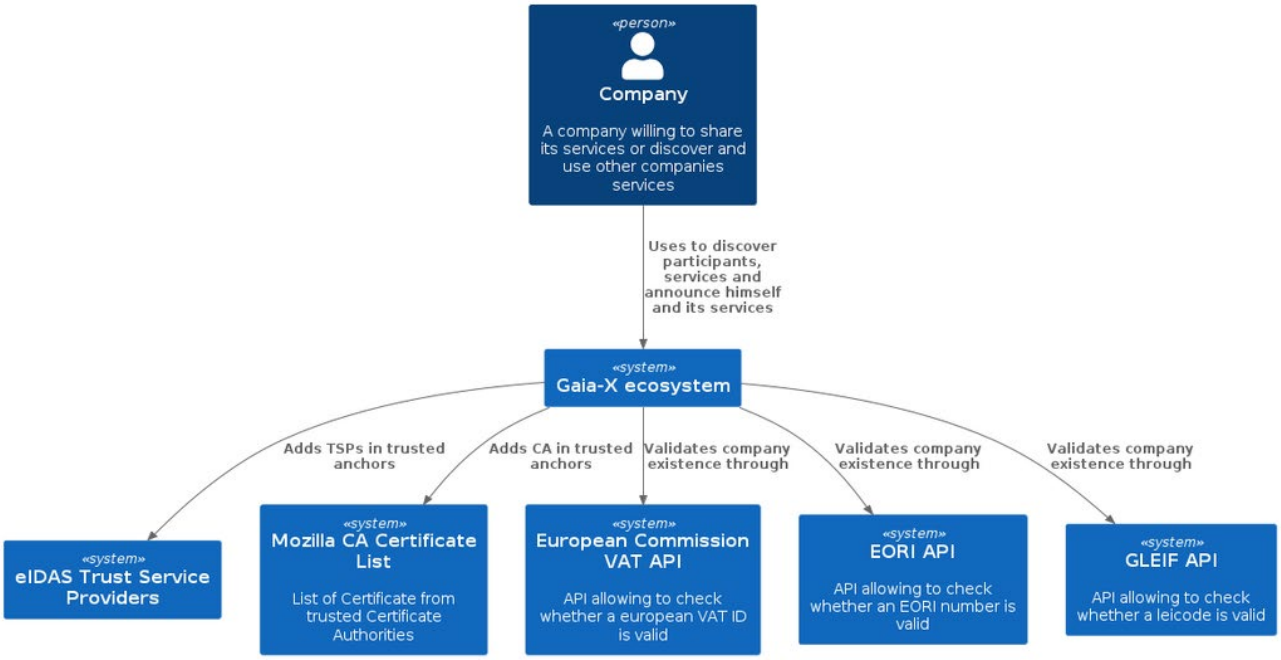
Het Gaia-X Digital Clearing House heeft een volledig **ander doel dan het IDSA RAM** Clearing House.

Het Gaia-X Clearing House **is gewijd aan toegang krijgen tot het Gaia-X ecosysteem** en het waarborgen van compliance. Het werkt samen met externe trust anchors (gezaghebbende en betrouwbare entiteit) voor identiteitsverificatie en andere bijbehorende functies.

Het clearing house bestaat uit verschillende componenten, die elk in hun eigen Git-repository[431] zijn ondergebracht:

> Gaia-X Registry: Deze service bevat een lijst van trust anchors die zijn erkend door het Gaia-X Trust Framework, samen met de vormen en schema's die nodig zijn voor het valideren van compliance, en andere relevante informatie zoals de algemene voorwaarden voor gebruikers van de compliance service.
> Gaia-X Compliance: Deze component valideert de structuur en inhoud van Gaia-X Credentials en ondertekent diegene die aan de criteria voldoen.
> Gaia-X Notarization Service for Registration Numbers: Deze tool wordt gebruikt om de geldigheid van alle registratienummers (denk hierbij aan verschillende soorten ondernemingsnummers) die door deelnemers in hun credentials worden verstrekt, te verifiëren.

[431] *https://gitlab.com/gaia-x/lab/gxdch/-/tree/main*



Figuur 21: Gaia-X Trust Anchors

Bovenstaande figuur geeft een aantal van de geaccepteerde trust anchors weer (eIDAS, trusted certificate authorities (CAs)), evenals enkele interfaces (API's) waar de Notarization Service mee integreert (om bijvoorbeeld na te gaan of een VAT/BTW-nummer geldig is).

Als zodanig ligt de focus op deelname aan het Gaia-X ecosysteem in plaats van op de traceerbaarheid van transacties.

Dit blijkt ook uit een rapport[432] van de Data Spaces Business Alliance dat de technische convergentie verkent onder haar leden, waaronder FIWARE, Gaia-X en IDSA. Een tabel uit het rapport benadrukt verschillende termen die niet op elkaar zijn afgestemd.

[432] https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.

FIWARE/TMForum	Gaia-X	IDSA
Party	Participant	Participant
Provider	Provider	Data Provider
Customer	Consumer	Data Consumer
Data Product (comprises resource and services)	Resource & Services	Data Asset
Trusted Participant List		IDS-DAPS + IDS-ParIS
(Data) Product Specification	Gaia-X Schema	IDS-Information Model + Vocabulary
(Data) Product Offering	Service Offering	Part of Self-Description
(Data) Product Catalogs.	Federated Catalogue	IDS-Meta-Data-Broker
Service Specification Characteristics.	Gaia-X Credentials (formerly known as Self-Description)	Connector Self Description
Logging Service	Data Exchange Services	Observability/Clearing House

Figuur 22: Verschillende terminologie tussen data space organisaties.

De documentatie over Data Exchange Services binnen Gaia-X[433] behandelt het concept van traceerbaarheid zoals we dit kennen van het IDSA Clearing House. Ook het document van de Data Spaces Business Alliance bevat een sectie gewijd aan provenance (herkomst) en traceerbaarheid, die ook verwijst naar het IDSA Clearing House.

Samenvattend richt het Gaia-X Digital Clearing House zich op het opzetten van een participatie-infrastructuur en Verifiable Credentials. Dit is een andere insteek dan wat IDSA vooropstelt als clearing house, waar de nadruk ligt op bewaren en bewijzen van de states in een transactie.

8.2 CONCEPTUELE ARCHITECTUUR

Het volgend beschreven conceptueel architecturaal model heeft als doel een model te presenteren van hoe een data space in een gezondheidssector kan opgebouwd worden. Het model is zo algemeen mogelijk opgesteld om verschillende use cases te kunnen faciliteren.

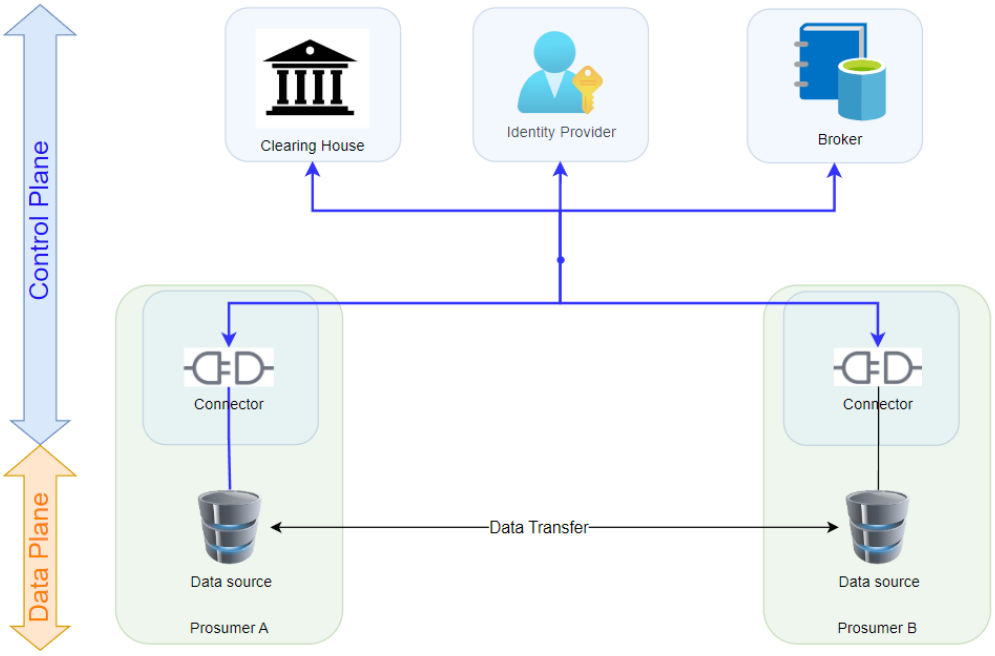
8.2.1 Conceptueel model

In dit onderzoeksproject baseren we ons op de IDSA-componenten die nodig zijn voor een **minimaal werkbaar product** dat toch de behoeften van een health data space invult: connector, broker, clearing house en identity provider.

Gezien de gevoelige data waarmee een health data space zal werken, zijn de behoeftes omtrent beveiliging en vertrouwen van zeer groot belang. Hierin verschilt een health data space met andere data spaces: het aspect **vertrouwen is belangrijk** in elke data space, maar in een health data space is dat vertrouwen van existentieel belang.

[433] https://docs.gaia-x.eu/technical-committee/data-exchange/22.10/dewg/

Om het nodige vertrouwen en de vereiste beveiliging te kunnen aanbieden, is het noodzakelijk dat de verschillende **componenten elk apart geïnstalleerd** kunnen worden. De installatie van de componenten kan gebeuren zowel in de cloud als on premise. Belangrijk is dat alle componenten **met elkaar kunnen communiceren**. Door componenten bij verschillende betrouwbare partijen te installeren en tegelijk te zorgen voor volledige transparantie, zal een health data space het nodige vertrouwen kunnen bieden aan de participanten.



Figuur 23: Conceptuele architectuur van een minimale health data space.

Figuur 23 toont een basisarchitectuur van een minimum viable health data space, met 2 prosumers met elk hun connector en 3 componenten (clearing house, identity provider, broker).
De functionele beschrijving van de componenten is terug te vinden in sectie 8.1 Analyse actuele data space componenten.

Elke prosumer biedt een databron aan op de data space. Een databron kan verschillende vormen aannemen. Enkele voorbeelden:

- een fysiek bestand (cf. csv bestand)
- een afgeleide geaggregeerde tabel in een conventionele databank
- een query die rechtstreeks op een databank tabel wordt uitgevoerd

Figuur 23 toont een eenvoudige en minimale setup van een health data space. In de praktijk is het aangeraden om de connector op een afgescheiden omgeving (bv. Demilitarized Zone (DMZ)) te plaatsen, gescheiden van de productieomgeving en om een beveiligde connectie op te zetten naar een databron.

8.2.2 Data plane en control plane

In het IDSA-model spreken we van een data plane en een control plane[434]. Deze zijn ook terug te vinden op Figuur 23.
De **data plane** omvat de componenten die nodig zijn voor **de fysieke datatransfer** zoals deze vandaag al in vele organisaties aanwezig is, bv. SFTP of API.

De **control plane** bevat alle componenten die samen **de basisprincipes van een data space** belichamen: controle van de identiteit, controle van de usage policies, beslissingen nemen over contract en data transfer aanvragen … De control plane vormt als het ware een laag boven de data plane. Alle data space componenten kunnen met elkaar communiceren. Het is de connector van de participant die ervoor zorgt dat er een connectie ontstaat tussen de data space en de infrastructuur van de participant.
Het fysiek aansluiten of onboarden van een participant op een data space is daardoor niet meer dan het installeren en configureren van de connector op de bestaande infrastructuur. Reeds bestaande datatransfersystemen kunnen blijven gebruikt worden.

8.2.3 Werking data space

In deze sectie geven we een korte samenvattende beschrijving van hoe een data space concreet werkt. De volgende hoofdstukken gaan dieper in op elke individuele component en het volledige proces van het opzetten van een data-uitwisseling gebruikmakend van een data space (zie 8.4 User journey).

Het opzetten van de data space start met het opzetten van de connectoren. De **connectoren** zijn het **startpunt** van het ecosysteem. Via een eigen connector is er verbinding mogelijk met de connector van een andere partij over het internet. In de connector zitten **verschillende functies** voor de werking van een datatransfer. Elke partij kan beslissen welke data hij beschikbaar stelt op de data space door deze toe te voegen via een policy aan de connector. De connectoren van alle partijen houden een soort **catalogus** bij waarin alle beschikbare data van alle partijen te vinden is. Deze component heet de broker en kan centraal bij één partij of decentraal op de data space draaien. Wanneer verschillende partijen data willen delen met elkaar dan worden de regels of policies eerst nagekeken door het clearing house. Het **clearing house** gaat na wat er in de policy staat van de data provider en zal uiteindelijk de data transfer goedkeuren of blokkeren. Eens goedgekeurd geeft het clearing house het bericht aan de connector van de provider om de effectieve data transfer te starten.

8.3 DESIGN COMPONENTEN

Dit hoofdstuk geeft een beschrijving van de technische uitwerking van de verschillende data space componenten, aangepast aan de behoeften binnen dit project. Een meer uitgewerkte user journey waarbij de opeenvolgende stappen en gebruik van de compomenten worden uitgelegd, is terug te vinden in een later hoofdstuk 8.4 User journey.

8.3.1 Connector

8.3.1.1 Eclipse Data Space Connector (EDC)

Op basis van het eerdere onderzoek naar data space connectoren is er gekozen voor het EDC-ecosysteem waarbij de **maturiteit** en **flexibiliteit** (aanpasbaarheid) de doorslaggevende redenen waren.

[434] *https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol/transfer-process/transfer.process.protocol#111-control-and-data-planes*

De Eclipse Dataspace Components (EDC) is een project van de Eclipse Foundation. Het implementeert een uitgebreid **framework** (concept, architectuur, code, samples) dat een basisset van functies biedt (functioneel en niet-functioneel) die data space implementaties kunnen hergebruiken en aanpassen door gebruik te maken van de gedefinieerde API's van het framework en dat met de garantie van interoperabiliteit met andere data space implementaties door het ondersteunen van het **IDSA Data Space Protocol**.

Er is op het moment van schrijven geen enkel ecosysteem dat alle nodige componenten en functionaliteiten aanbiedt om een minimale health data space te kunnen bouwen. Daarom werd gekozen om te vertrekken van een systeem dat toch al veel out-of-the-box heeft en vooral zeer aanpasbaar is. Verder werd ook vastgesteld dat de **meerderheid van de data space initiatieven** zich richten op het gebruik van EDC als technische component (cf. het SIMPL-project, zie 3.4.1.6 SIMPL-project).

Een andere conclusie van het onderzoek is dat er veel opensourcecomponenten zijn die functionaliteiten van een data space beloven, maar dat er nog enorm veel **onderzoek en ontwikkeling bezig** is binnen de data space wereld. De technologie is nog volop in ontwikkeling en nog niet alle bouwblokken uit de IDSA-architectuur bestaan al out-of-the-box waardoor op het moment van schrijven eigen ontwikkelingswerk nodig is om een minimale doch complete data space uit te werken. De protocollen van IDSA zijn ook nog continu in ontwikkeling en zullen later de blauwdruk leggen voor interoperabiliteit tussen verschillende data spaces.

De EDC heeft een waaier aan functionaliteiten die via een API te gebruiken zijn. Dit maakt het mogelijk om zelf **extensies** te maken die gebruik maken van de data in de connector. Meer specifiek biedt het EDC-platform veel functionaliteiten aan in de connector die out-of-the-box te gebruiken zijn. Een samenvattende lijst van de meest gebruikte API's wordt verder besproken bij de connector dashboard component.

Een niet gelimiteerde lijst van acties die via een API kunnen uitgevoerd worden:

- Data assets registreren;
- Usage policies aanmaken;
- Contractdefinities opstellen (linken van data asset met usage policy);
- Contractonderhandelingen starten;
- Data transfers starten.

De connector wordt gehost bij de data provider of de data consumer. Iedere partij die wil deelnemen aan de data space moet zijn eigen connector(en) hosten.

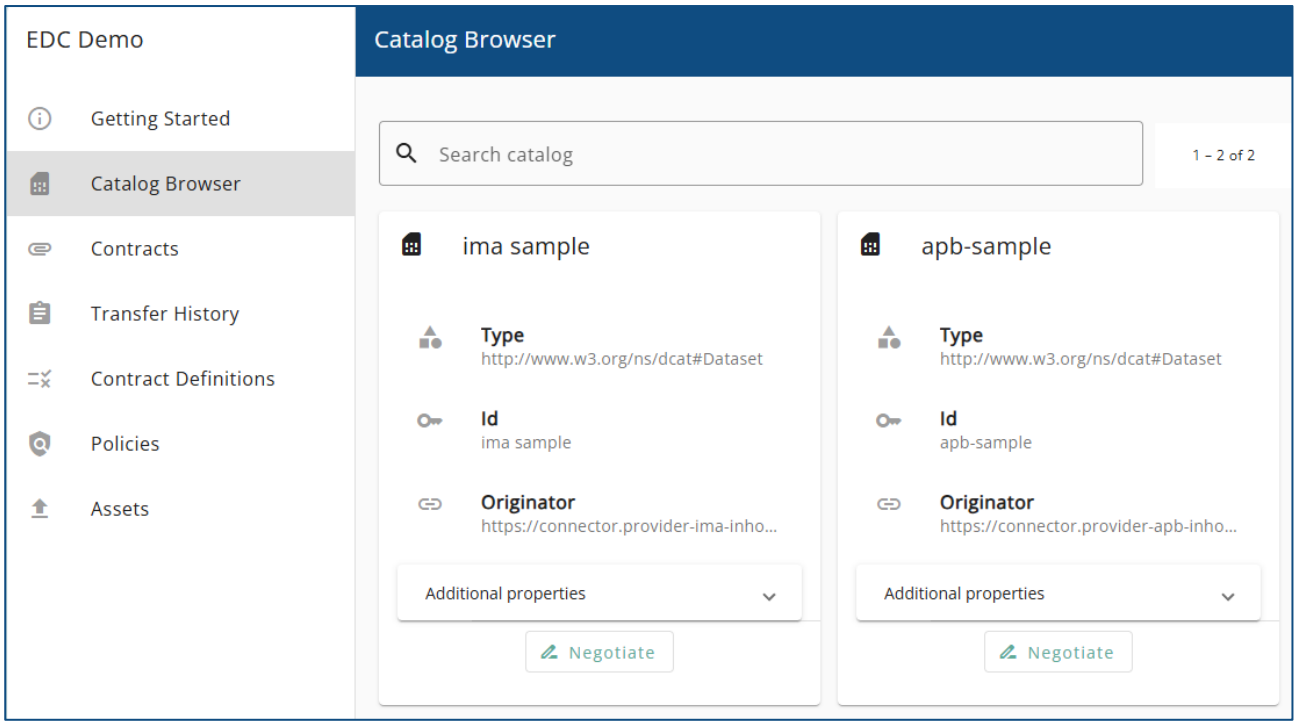
Met het selecteren van een bepaald type connector wordt er ook gekeken naar het ecosysteem en hoe de connector de data space theorie in praktijk omzet. Zo zal een EDC-connector andere proceskeuzes maken bij het opzetten van een data space dan een andere type connector (de FiWare connector ondersteunt bijvoorbeeld de DSBA specificatie). De consequentie is dat elke data space zijn eigen werking zal hebben en dat dit zal afhangen van het type connector. Zelfs binnen het EDC-platform zijn er verschillen in de concrete werking van bepaalde componenten tussen de verschillende **versies** van de EDC-platformen.

Binnen dit project zijn we begonnen met versie 0.6 en op het einde van het project heeft EDC versie 0.10.1 gereleaset. Om de continuïteit binnen het project te bewaken is gekozen om op versie 0.6.4 te blijven. Deze versie beschikte over een stabiele code voor het uitvoeren van de technische PoC. Door op eenzelfde versie te blijven, werd ook vermeden om de eigen ontwikkelde code van de uitbreidingen steeds opnieuw te moeten testen en eventueel aan te passen.
Op Europees niveau wordt er gewerkt aan het data space protocol[435] dat de werking tussen de verschillende types connectoren moet samenbrengen en gelijkstellen.

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

8.3.1.2 EDC connector dashboard

Het connector dashboard is een user interface die bovenop de management API van de connector is gebouwd. Het dashboard is een bestaande component van het EDC-platform en heeft als doel **de connector te visualiseren** en bepaalde taken gemakkelijk te laten uitvoeren. Zonder een dashboard zouden deze functies enkel aan te roepen zijn via code of een terminal.



Figuur 24: Connector dashboard / User interface

De basiscomponent waarvan vertrokken werd voor het dashboard is het EDC Data Dashboard.
Dit is een opensource webapplicatie die je kan installeren naast de EDC-connector. De standaardversie is een technologiedemo die enkel met een gedateerde versie van de EDC-connector kan verbinden en enkel transfers naar Azure Blob Storage (Microsofts' cloud oplossing voor opslag van grote binaire bestanden) toelaat. Voor dit project is een eigen versie gemaakt die met recente versies van de EDC-connector kan verbinden en toelaat meer algemene HTTP-transfers te verrichten. Ook zijn de configuratiemogelijkheden aangepast om de user interface (UI) te laten linken met zowel de catalogus van één enkele connector (rechtstreeks) als met een federated catalog.

De voornaamste functies van de connector die via het dashboard toegankelijk worden gemaakt, zijn:

> **Catalog Browser:** De catalog browser stelt de gebruiker in staat om de catalogus van andere connectoren te raadplegen. Er is een API voor datasets evenals contractaanbiedingen (= die laatste gebruikt men om overdraagbare assets te ontdekken). Als het dashboard is geconfigureerd om de federated catalog te gebruiken, worden onrechtstreeks de catalogi van alle connectoren waartoe deze toegang heeft, bevraagd, waardoor het mogelijk is om de contractvoorstellen (contract definities) van al deze connectoren te ontdekken. Na het vinden van de gewenste contractaanbieding wordt er steevast overgegaan op directe communicatie tussen de betrokken connectoren.
> De catalog browser kan gezien worden als een vereenvoudigde versie van de broker die enkel een lijst van contractaanbiedingen weergeeft.

- **Contract definition:** Dit is een CRUD (Create, Read, Update, Delete) API voor contract definities (= initiële contractvoorstellen van de data provider), waarmee deze aangemaakt, bijgewerkt en verwijderd kunnen worden. Een contractdefinitie koppelt een usage policy aan een data asset. Let op dat alleen de connector die de definities heeft aangemaakt, ze kan weergeven (d.w.z. de provider).

- **Contract negotiations:** Deze API wordt gebruikt door een data user om een onderhandeling te starten op basis van een contract definitie van een gegeven tegenpartij (= de data provider). Verder laat deze ook toe om bestaande contractonderhandelingen op te vragen, of om hun voortgangsstatus of de bijbehorende contractovereenkomst te verkrijgen. Standaard werden deze niet weergegeven in het dashboard, maar in de versie voor dit project kan men de voortgangsstatus van de lopende onderhandeling zien.

- **Contract agreement:** Deze API stelt de gebruiker in staat om alle contractovereenkomsten op te vragen (= de eindresultaten van succesvolle contractonderhandelingen). Het EDC-dashboard biedt de overeenkomsten aan onder "Contracts". Contractovereenkomsten hebben dezelfde ID op beide betrokken connectoren en kunnen op beiden worden opgehaald.

- **Policy definition:** Dit is een CRUD API voor policies. Hier kunnen bepaalde access policies gedefinieerd worden die via de contract definities aan assets gekoppeld worden. Deze policies zijn typisch vrij complexe documenten geformuleerd in Open Digital Rights Language (ODRL). De provider kan deze in het dashboard beheren onder “Policies”.

- **Transfer process:** Deze API maakt het mogelijk om een data-uitwisseling te initiëren, de status op te vragen, te pauzeren, te hervatten of te beëindigen. In het EDC-dashboard wordt deze API gebruikt voor de “Transfer” knop onder “Contracts”, evenals voor het bijwerken van de voortgangsstatus onder die knop (eigen toevoeging).

- **Transfer history:** Deze API van de connector wordt weerspiegeld onder “Transfer history” in het EDC-dashboard, en kan op beide connectoren worden aangeroepen. Hij laat toe een lijst van voorbije data-uitwisselingen op te vragen. Let op dat elke connector zijn eigen unieke ID heeft voor het uitwisselings-proces. De overeenkomstige ID op de connector van de tegenpartij wordt de “correlationId” genoemd. De ID van de overeenkomstige contractovereenkomst (weergegeven als “ContractId” in de lijst in het dashboard) is bij beiden identiek, zoals eerder vermeld. Bij de provider komt de “AssetId” overeen met de ID van de aangemaakte asset. Aan de zijde van de consument is dit echter de overeenkomstige parameter die werd opgegeven bij het initiëren van de data-uitwisseling.

- **Asset:** De CRUD API voor het aanmaken en beheren van assets, acties uitgevoerd door de data provider. Deze kunnen in het EDC-dashboard beheerd worden onder “Assets” in de menubalk.

Het dashboard is logisch opgebouwd volgens de belangrijkste functies van de connector die elk hun eigen API hebben. De keuze om voort te bouwen op het bestaande standaard EDC-dashboard was ingegeven door deze logische opbouw en de flexibiliteit die het te bieden heeft. Het dashboard is volledig opensource en gebruikt Angular[436]. Angular is een welgekende frontend library waarin applicaties op een voorgeschreven manier gestructureerd worden, zodat aanpassingen makkelijk te maken zijn. Het gebruik van het EDC-dashboard heeft het team tijdens het project tijd bespaard zodat er meer gefocust kon worden op andere data space functionaliteiten.

[436] *https://angular.dev/*

8.3.2 Broker

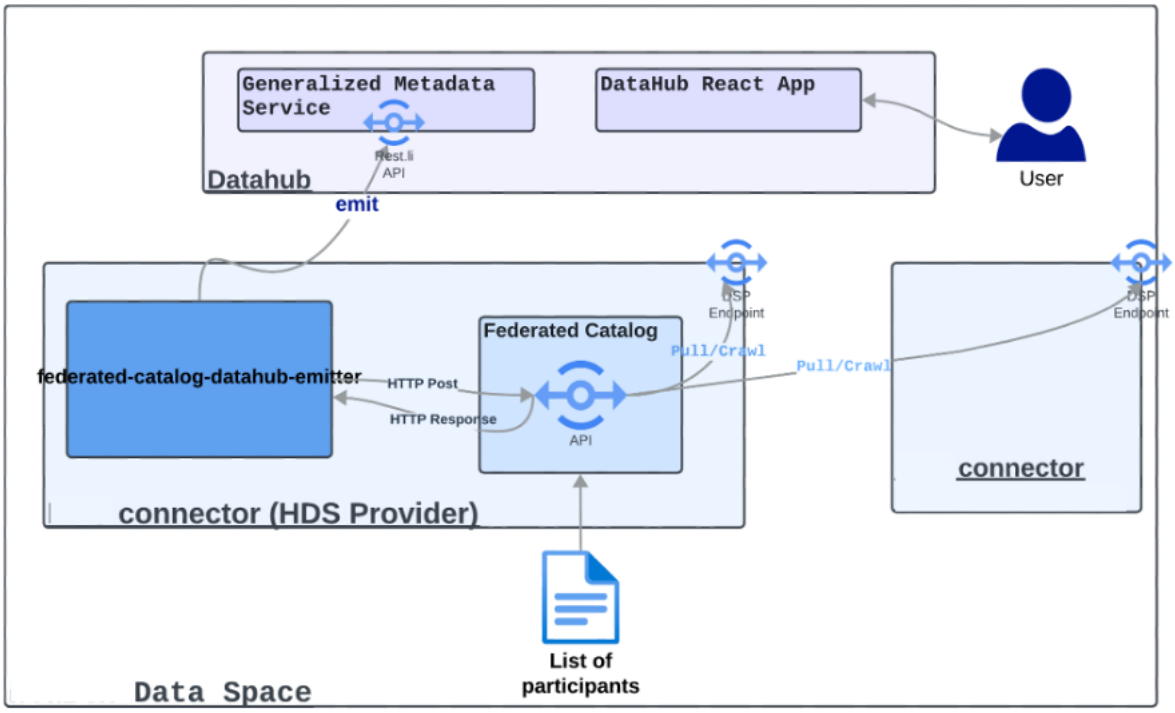
De EDC-connector voorziet ook broker-functionaliteit. Deze wordt aangeboden als een connectorextensie en gebruikt het **federated catalog** principe. Een federated catalog haalt periodiek de **catalogi** van een voorgedefinieerde lijst van connectoren binnen de data space op (**crawlen**). Op deze manier heeft de eigenaar van de connector met de federated catalog functie steeds een up-to-date lijst van beschikbare datasets. Er kan gekozen worden om de federated catalog beschikbaar te maken voor andere connectoren zodat deze connectoren maar met 1 connector moeten connecteren om de lijst van beschikbare datasets te verkrijgen. Er kan ook gekozen worden om verschillende federated catalogs te configureren in een data space en daarbij aan groeperingen van connectoren te doen binnen een data space. Het is aan de data space beheerder om de keuze te maken:

> 1 federated catalog op een connector van een prosumer en alle andere connectoren gaan de informatie omtrent datasets bij deze connector ophalen.
> 1 federated catalog op een afgescheiden connector (niet geïnstalleerd bij een prosumer) die dan fungeert als enige catalog binnen de data space.
> Een netwerk van federated catalogs.
> …

Voor dit project is gekozen om één afgescheiden connector op te zetten die enkel fungeert als federated catalog. Alle andere connectoren worden geconfigureerd om de lijst van beschikbare datasets bij deze federated catalog connector te komen ophalen. De federated catalog functie van een EDC-connector biedt echter een beperkte lijst van functionaliteiten aan. Vooral het gebruiksvriendelijk zoeken en verkennen van de aangeboden datasets ontbreekt.
Er is daarom gekozen om zelf een brokercomponent te bouwen die bestaat uit een EDC-connector met federated catalog en een user interface die het mogelijk maakt om datasets te ontdekken.

Als **user interface-component** is gekozen voor **DataHub**, een opensource software gespecialiseerd in het verwerken en presenteren van metadata. Het biedt een prettige gebruikersinterface en maakt het mogelijk om assets per domein en omgeving te organiseren. Het laatste zorgt ervoor dat niet telkens een nieuwe instantie hoeft opgezet worden voor bijvoorbeeld ontwikkeling versus gebruikerstesten, dergelijke omgevingen gescheiden houden is mogelijk binnen dezelfde DataHub-instantie. Verder was er eerdere ervaring met DataHub in het ontwikkelingsteam wat de keuze voor DataHub versterkte.

Een mogelijke opzet is hieronder weergegeven.



Figuur 25: Het gebruik van DataHub als broker in de Health Data Space (HDS)

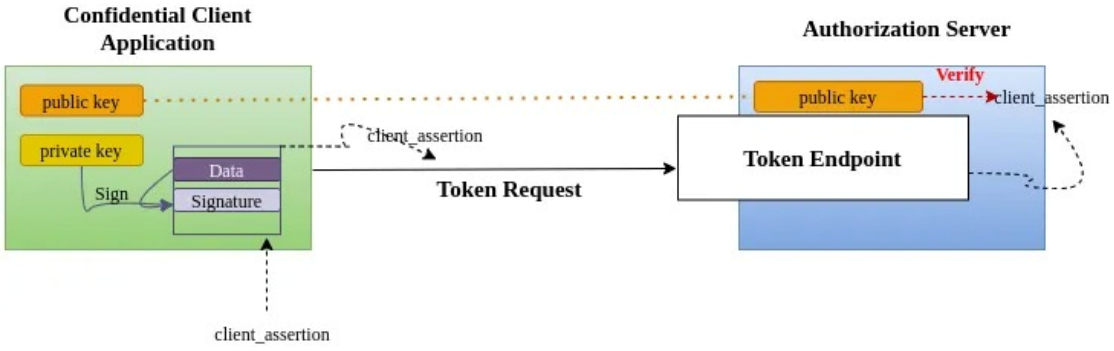
Op bovenstaande afbeelding is te zien hoe de federated catalog, user interface en connectoren zich tot elkaar verhouden. Eén connector heeft een federated catalog-extensie en een lijst van alle participanten in de data space. Dit kan een gespecialiseerde connector zonder andere functie zijn (dus bv. geen assets kan transfereren), of een connector die ook nog als provider of consumer dient. Het is ook mogelijk meerdere dergelijke connectoren op te zetten. Hoe het ontdekken van gegevensbronnen via één of meer federated catalogs en/of metadata-brokers wordt georganiseerd, valt immers vrij te bepalen door de data space beheerder.
Op basis van de lijst van participanten worden de metadata van hun beschikbare datasets periodiek opgevraagd en verzameld (gecrawld). Voor de synchronisatie met de user interface (DataHub) werd een custom connectorextensie gemaakt (“federated-catalog-datahub-emitter") die dan weer periodiek de federated catalog raadpleegt en die gegevens synchroniseert met DataHub (via de GMS - Generalized Metadata Service, de backend van DataHub).

8.3.3 Identity provider

Voor de praktische implementatie in het project werd gekozen voor een mature **IAM-oplossing** met een **centrale identity provider** en **OAuth 2**, een gekende open standaard voor autorisatie. Hoewel Verifiable Credentials meer en meer opgang maken, zijn er nog geen universele, mature oplossingen binnen het data space-landschap. Bij de start van het project was EDC bezig om een nieuw protocol op basis van Verifiable Credentials te verwezenlijken, maar tot op het moment van het schrijven van dit rapport is dit nog niet volledig geïmplementeerd (het uitgeven van de credentials door een centrale autoriteit is nog niet beschikbaar). Daarnaast is het zo dat de autorisatiestromen die gebruikt worden bij de OAuth 2-oplossing aangeboden door EDC ook ondersteund worden door de Toegangs- en Gebruikersbeheer (ACM/IDM) bouwstenen van de Vlaamse overheid.[437]

[437] *https://www.vlaanderen.be/digitaal-vlaanderen/onze-diensten-en-platformen/veiligheidsbouwstenen-applicatie-en-platformdiensten/acm-idm-standaard-aansluitingsproces*

De basis van deze autorisatie zoals aangeboden door EDC maakt gebruik van een “Private Key Json Web Token” (Private Key JWT) en wordt uitgelegd in onderstaande figuur.



Figuur 26: Private / Public key principe gebruikt door EDC.

De partij in de data space die geautoriseerd moet worden (bv. een connector) is hier aangeduid als “Confidential Client Application”. Deze heeft een public-private keypair. De private key is, zoals de naam aangeeft, geheim en wordt gebruikt om een tokenaanvraag naar de centrale identity provider (hier aangeduid als “Authorization Server”) digitaal te ondertekenen.

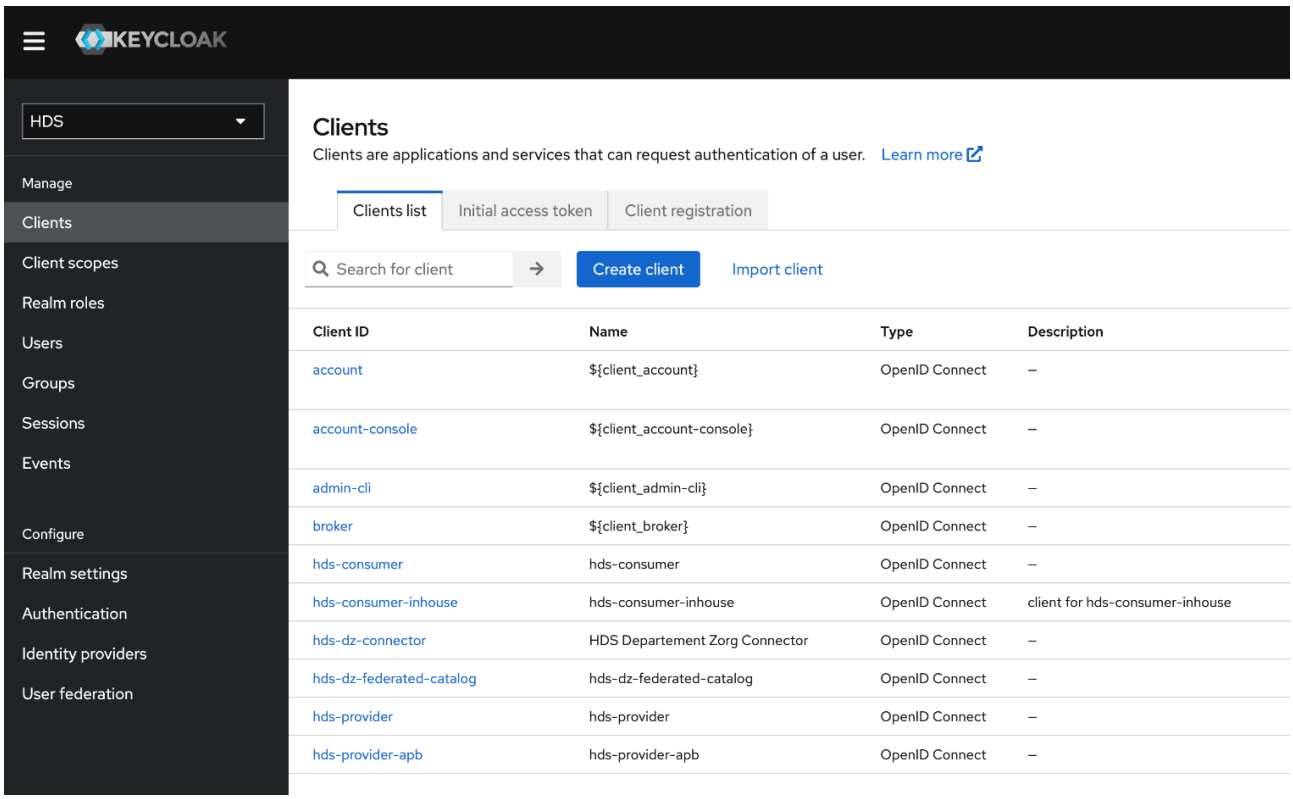
Het ondertekenen kan gezien worden als het genereren van een unieke “fingerprint” van de aanvraag die vervolgens geëncrypteerd wordt met de private key. De overeenkomstige public key kan openlijk verspreid worden (dus ook ter beschikking gesteld worden van de “Authorization Server”) en gebruikt worden om de geëncrypteerde fingerprint te decoderen (asymmetrische encryptie). De “Confidential Client Application” stuurt zowel deze geëncrypteerde signatuur als de tokenaanvraag naar de “Authorization Server”.
Die laatste kan vervolgens zelf de “fingerprint” van de inkomende aanvraag berekenen, en deze vergelijken met de gedecodeerde fingerprint die hij zelf decrypteert met de public key. Als beiden overeenkomen, is bewezen dat de “Confidential Client Application” de partij is die de aanvraag gegenereerd heeft (aangezien haar private key gebruikt is om de signatuur te genereren).

De eigenlijke tokens die de identity provider of “Authorization Server” uitreikt wanneer de aanvraag geverifieerd is, zijn gebaseerd op hetzelfde principe; ook de identity provider heeft een unieke private key en stelt zijn public key ter beschikking van de “Confidential Client Application” of connectoren. Daar kan dan geverifieerd worden of de identity provider daadwerkelijk de tokens heeft uitgereikt aan de partijen betrokken bij een transactie.

Belangrijk om te vermelden is dat bepaalde eigenschappen van een connector (zogeheten “claims”) bij deze vorm van autorisatie centraal beheerd kunnen worden in de identity provider. Deze kunnen dan gebruikt worden bij de evaluatie van policies (voorwaarde) bij het sluiten van een transactie. De locatie van de connector is één zo’n voorbeeld: de identity provider zou bijvoorbeeld in een claim kunnen bijhouden waar een connector zich bevindt (binnen de EU of daarbuiten), wat dan gebruikt zou kunnen worden in een policy om te bepalen of die participant al dan niet toegang heeft tot een welbepaald asset. De policy zou dan bijvoorbeeld kunnen dicteren dat een dataset enkel toegankelijk is voor connectoren binnen de EU.

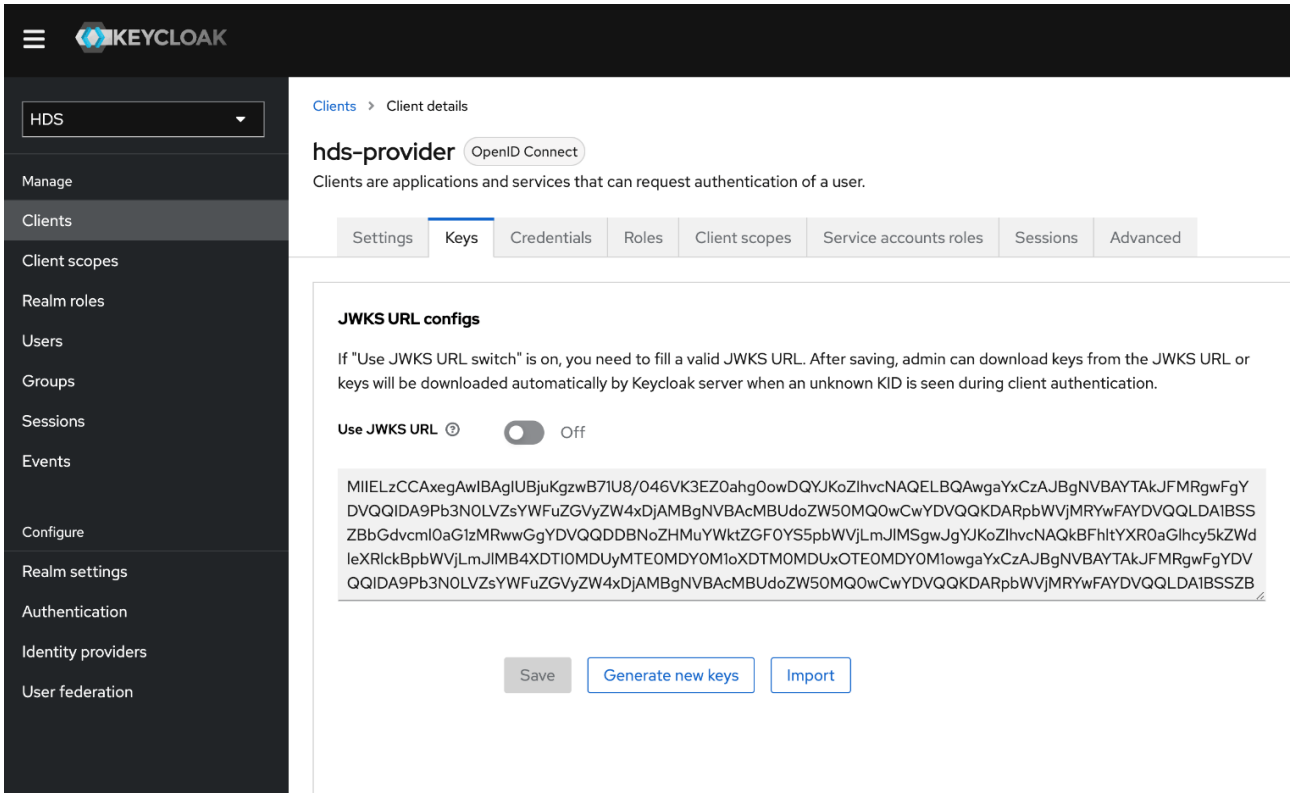
In dit project hebben we ervoor gekozen Keycloak[438] te gebruiken als OAuth 2 identity provider. Dit is een wijdverspreide opensource IAM-oplossing wat zorgt voor een snelle ontwikkeling zonder afhankelijkheden van andere partners. Er zijn verschillende Identity as a Service – IDaaS – oplossingen, maar deze bieden dikwijls niet alle nodige functionaliteit aan of zijn prijzig.
Hieronder nog enkele figuren die de configuratie in Keycloak demonstreren.

[438] *https://www.keycloak.org/*



Figuur 27: Keycloak UI – Klanten lijst

Elke connector heeft een eigen “Client” in Keycloak. Elk van deze “Clients” heeft een public key zodat Keycloak aanvragen van die connector kan verifiëren: de “Keys” tab in onderstaande afbeelding bevat de public key, enkel de connector heeft de bijhorende private key.



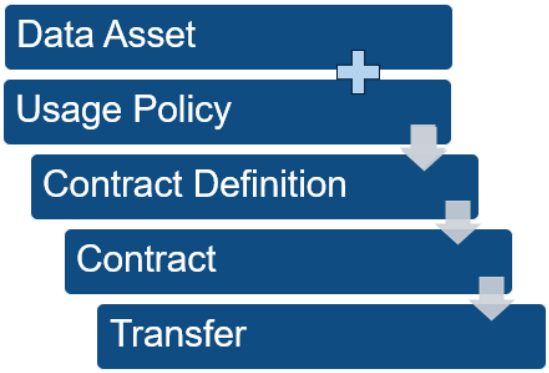
Figuur 28: Keycloak UI public key voorbeeld

8.3.4 Clearing house

8.3.4.1 Policies en contracten

Alvorens dieper in te gaan op het design van het clearing house, geven we even een korte uitleg over enkele definities die vaak aangehaald worden als er gesproken wordt over een clearing house. Volgende definities zijn opgesteld volgens het EDC framework.

> **Data Asset**: Fysieke toegang tot de data (csv bestand, API, database tabel …) bij de data provider.
> **Usage Policy**: de voorwaarden onder dewelke de data asset kan opgehaald worden (zie ook 8.1.4.1 IDSA clearing house). Ze worden bepaald door de data provider.
> **Contract definitie**: de combinatie van een data asset en een usage policy. Er kunnen meerdere contractdefinities gemaakt worden op hetzelfde data asset wanneer het data asset telkens gekoppeld wordt aan andere usage policies. Een contractdefinitie wordt opgesteld door de data provider.
> **Contract**: Een contract is gebaseerd op een contractdefinitie en is een overeenkomst tussen de data provider (die contract definitie heeft opgesteld) en een data consumer die akkoord is met de contract definitie.
> **Data transfer**: Eens een contract is afgesloten, kan er vanuit dat contract een datatransfer geïnitieerd worden.



Figuur 29: Relaties tussen data asset, usage policy, contract definition, contract en transfer

8.3.4.2 Custom clearing house

In het kader van dit project werd een overzicht gemaakt van de gewenste functies van een clearing house in een health data space. Deze zijn:

> **Loggen** van de transacties (contractnegotiaties en data-overdrachten).
> Verzamelen en loggen van de overeengekomen **contracten.**
> Policy Decision Point (PDP), bv. door een manuele **goedkeuring** te geven om verder te gaan met een negotiatie of data-overdracht
> Interactie verzorgen tussen een Policy Enforcement Point (PEP), de plaats in het proces waar de transfer van data of metadata wordt gestopt, en een PDP.

Zie IDSA-documentatie voor meer informatie omtrent PEP en PDP[439].

[439] *https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_4_process_layer/3_4_6_policy_enforcement*

Uit hoofdstuk 8.1.4 Clearing house is af te leiden dat deze gewenste functies het dichtst aanleunen bij de referentie architectuur zoals voorgesteld door IDSA, echter zoals eveneens vermeld, was er tijdens de duurtijd van dit project **geen bestaande bruikbare implementatie** hiervan beschikbaar. Er is daarom gekozen om binnen dit project **zelf software te ontwikkelen** die deze functionaliteiten aanbiedt.

Na studie van de processen binnen de EDC-connector is gebleken dat het mogelijk is te abonneren op connectorevents om transactie-metadata te onderscheppen, zodat deze veilig elders kan worden gelogd en gebruikt voor auditing. Dit gaat dan bijvoorbeeld over de start van een transfer, of het (on)succesvol afronden ervan. Verder werden ook nieuwe processen geschreven die het mogelijk maken om lopende communicatie tussen connectoren op te schorten en de controle aan een externe partij over te dragen. Zo wordt het mogelijk om elders policies af te dwingen (bv. in een clearing house) of een andere als betrouwbaar beschouwde partij toestemming te vragen om de transactie toe te staan.

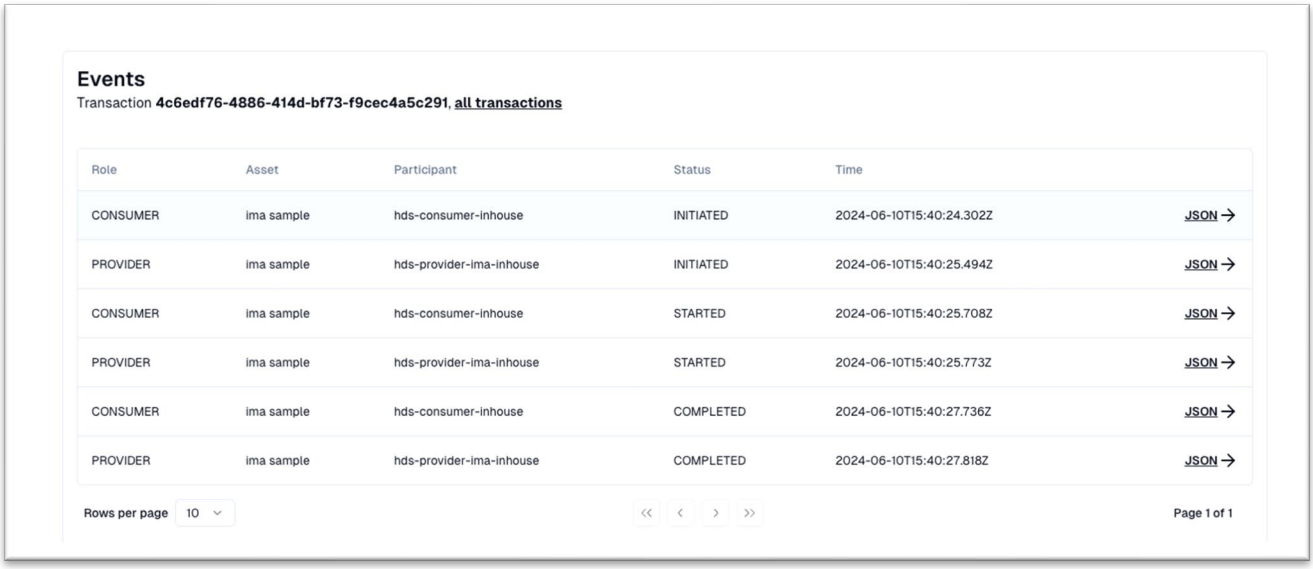
Wanneer we kijken naar het volledige proces van het registreren en transfereren van een data asset, kunnen we de volgende stappen identificeren:

- Dataprovider registreert asset met usage policies (=contractdefinitie).
- Dataconsument vindt asset in catalogus of broker.
- Dataconsument en provider onderhandelen een contract, wat resulteert in een overeenkomst indien de onderhandeling succesvol is (=contract).
- Consument start een overdracht, wederom succesvol of niet.

Met het eigen ontwikkeld proces om in te breken in de lopende communicatie tussen twee connectoren werd het mogelijk gemaakt dat het clearing house **meer logging** kan doen **én kan ingrijpen** tijdens de laatste twee stappen. Het biedt ook de mogelijkheid om een eigen front-end te bouwen voor het beheren van de transacties (loggen, goedkeuren, afkeuren). In de sectie 8.4 User journey zijn er screenshots te vinden van een eigen ontwikkelde user interface (binnen het kader van dit project). Voor deze PoC worden de onderbrekingen afgedwongen via usage policies en moet een goedkeuring manueel gebeuren.
In toekomstige implementaties kunnen dergelijk processen deels of volledige geautomatiseerd worden.

Het moet echter zorgvuldig worden overwogen hoever de bemiddeling door een clearing house gaat. Enerzijds is het onhoudbaar om manueel elke mogelijke transactie te gaan verifiëren, zeker als het gaat over grote aantallen data aanbieders of afnemers. Anderzijds is het ook steeds belangrijk om het aspect van gegevenssoevereiniteit, één van de basisvoorwaarden voor data spaces, in beschouwing te nemen. Deze laatste zorgt ervoor dat organisaties, overheden en individuen zelf bepalen hoe hun gegevens worden verzameld, opgeslagen, gedeeld en gebruikt door anderen.

Om een werkbare implementatie van een clearing house voor een health data space te realiseren werd daarom gewerkt in twee fases. In een eerste fase werd de focus gelegd op het loggen van transacties. Deze logging heeft als doel om een aantal events die door de verschillende connectoren bijgehouden worden te verzamelen. Door de events van de verschillende connectoren samen te brengen kunnen inzichten verworven worden, zoals bijvoorbeeld de duurtijd van een transactie (startevent van collector A en eindevent bij collector B).
De loggingfunctionaliteit van de connector werd verwezenlijkt door een eigen connectorextensie te implementeren: de “logging extension”. Deze laat toe de negotiaties en transfers te loggen naar een configureerbaar endpoint van het clearing house. Daarnaast kan deze extensie ook de controle aan een externe partij overdragen om te kunnen ingrijpen bij de contractonderhandeling of transfer.



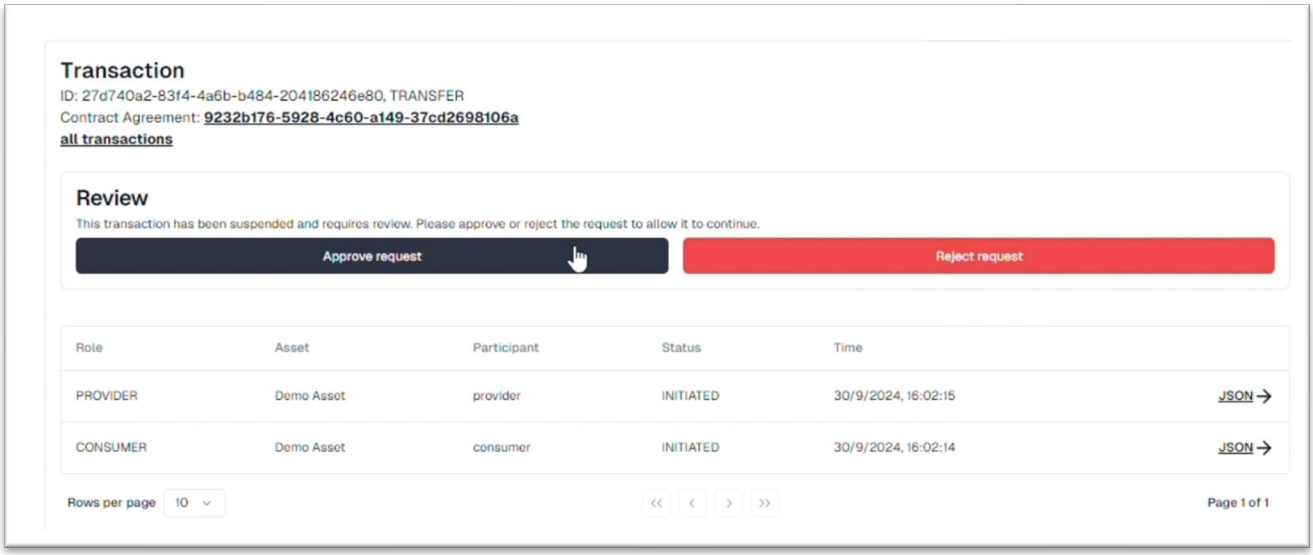
Figuur 30: Voorbeeld lijst van connector events.

In een tweede fase werd daarom naast het loggen van transacties ook gekeken naar het clearen of goedkeuren van een contractnegotiatie of een data transfer vanuit een goedgekeurd contract.
Hiervoor werd zoals eerder vermeld een eigen connectorextensie ontwikkeld die het communicatieproces tussen twee connectoren kan onderbreken. Via deze “consent API” is het ook mogelijk voor het clearing house om haar beslissing mee te delen aan de connector.

EDC-connectoren zijn uitgerust om zelf de contracten en de datatransfers goed te keuren.
Door het opzetten van deze laatste extensie is dit proces doorgeknipt en het clearing house ertussen geplaatst. Hierdoor is het mogelijk om:

> Contracten te laten goedkeuren (of afkeuren) voordat ze effectief in gebruik mogen genomen worden. Met deze stap kan er bijvoorbeeld gesimuleerd worden dat een contract (=data sharing agreement) eerst moet goedgekeurd worden door de HDA en het Informatie Veiligheidscomité (IVC).

> Data transfers goed te laten goedkeuren (of afkeuren). Hiermee kan er gesimuleerd worden dat een clearing house tijd nodig heeft om alle aspecten (technisch, legaal, financieel, …) van een data sharing agreement te controleren (manueel of automatisch) voordat een data transfer kan plaatsvinden.



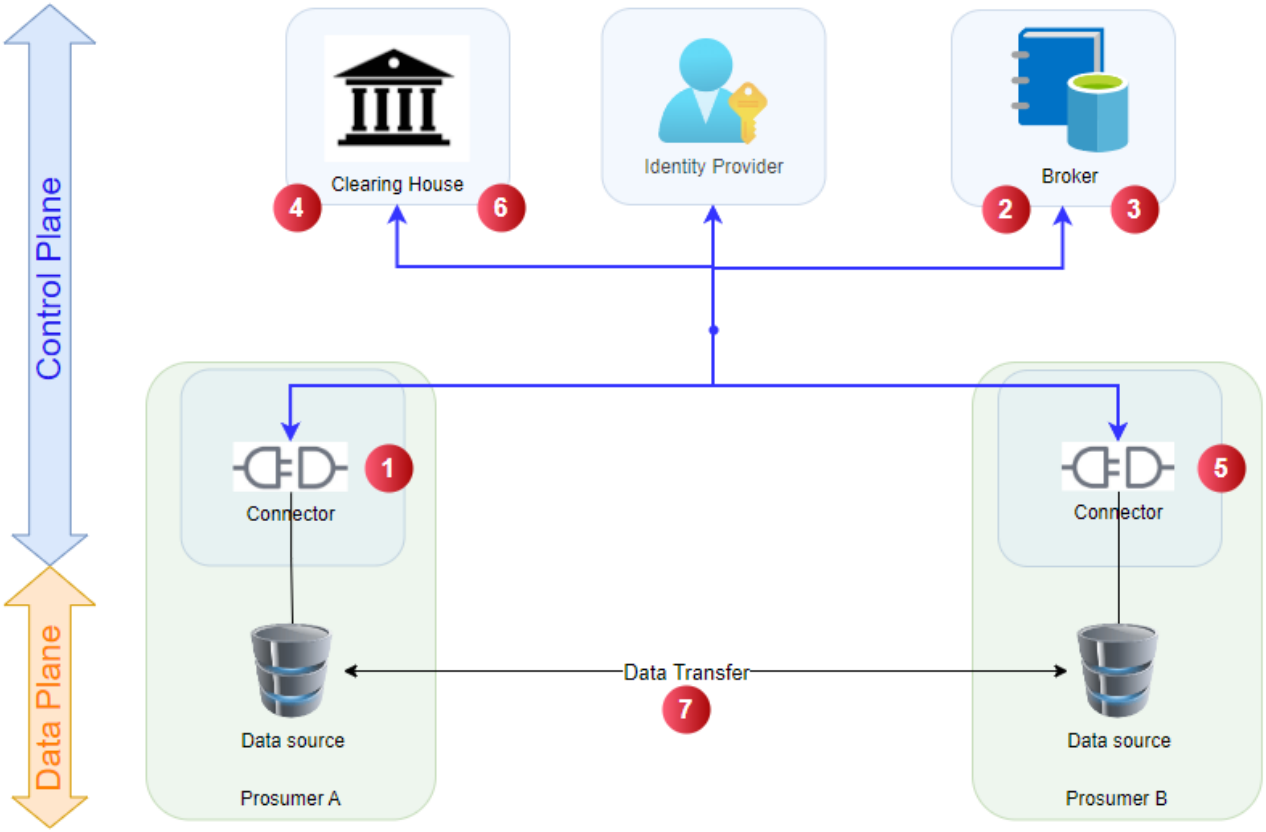
Figuur 31: Voorbeeld van (manueel) goedkeuren van transactie.

Onze implementatie van het clearing house bestaat uit een databank met een API voor het bijhouden van logs, en een gebruikersinterface waar de transacties geïnspecteerd kunnen worden en waar lopende transacties onderhevig aan een policy die dit vereist, manueel kunnen goed- of afgekeurd worden.
In onze implementatie worden, omwille van pragmatische redenen, de usage policies gecheckt door de policy engine die standaard in de EDC-connectoren aanwezig is. Het clearing house vraagt als het ware aan de connector om de policies te checken en het resultaat terug te geven aan haar. Het clearing house fungeert als een Policy Decision Point. Indien er een inbreuk is tegen een policy zal het clearing house de transactie onderbreken. In onze PoC-oplossing is het vervolgens mogelijk dat de transactie toch nog manueel wordt goedgekeurd.
Afhankelijk van de ingestelde policies zal het clearing house elke transactie onderbreken ook al zijn alle (andere) voorwaarden voldaan, of zal het transacties automatisch goedkeuren als alle voorwaarden voldaan zijn of onderbreken of er bepaalde voorwaarden geschonden worden.

8.4 USER JOURNEY

Deze sectie beoogt een overzicht te geven van hoe de hierboven beschreven **bouwblokken** zich tot elkaar **verhouden** en wat de **stappen** zijn die een gebruiker doorloopt tijdens het uitvoeren **van een data-uitwisseling** via een data space.

Vertrekkende van de conceptuele architectuur kunnen we volgende 7 stappen definiëren in een end-to-end data space proces.



Figuur 32: User journey stappen

- Prosumer A registreert zijn de databron in zijn connector.
- Connector A deelt metadata gegevens van de geregistreerde databron met de broker.
- Prosumer B gebruikt de broker om de datasets te ontdekken die gedeeld worden in de data space.
- Prosumer B sluit een contract af voor datadeling met prosumer A en registreert dat contract in het clearing house.
- Prosumer B start een data transfer op onder de voorwaarden afgesproken in het contract.
- Het clearing house controleert de aanvraag.
- Na goedkeuring van het clearing house, initieert de connector van prosumer A de datatransfer naar prosumer B.

Doorheen alle stappen van het proces zal de identity provider controleren of de entiteiten die acties verrichten op de data space gekend zijn en wel degelijk zijn wie ze beweren te zijn. Nieuwe gebruikers worden tijdens de **onboarding** procedure geauthentiseerd en maken een public/private keypair aan, waarbij de public key wordt doorgegeven aan de identity provider, zodat deze toegangsaanvragen van de gebruiker kan verifiëren en autoriseren.

Voor dit project is gebruikgemaakt van Keycloak om de taak van identify provider te vervullen. Keycloak heeft voldoende flexibiliteit om aan de eigenheid van een data space te voldoen.

Alle stappen kunnen geïnitieerd of opgevolgd worden in het connector dashboard, de broker of het clearing house. Voor deze PoC zijn de meeste stappen manuele acties, maar gezien het vaak gaat om het aanroepen van APIs van de connector, kunnen de meeste stappen geautomatiseerd worden.

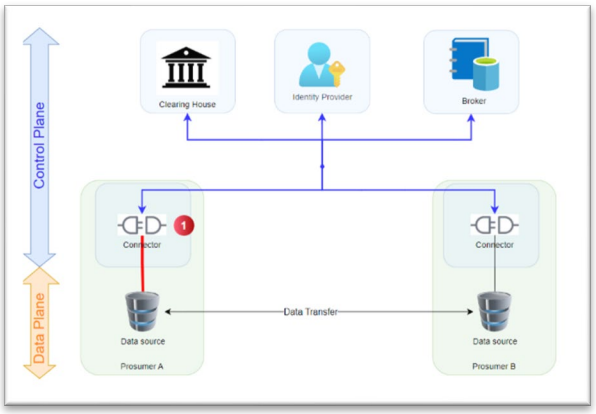
8.4.1 Technische onboarding

Als allereerste dient een participant aangesloten te worden op de data space. De **onboarding** procedure bestaat uit vier onderdelen:

- **Installatie van de connector**;
- **Configuratie** van de communicatie tussen connector en data plane;
- Nieuwe **identity registreren** bij identity provider;
- **Connector registreren** in het netwerk (bvb. bij federated catalog, broker …).

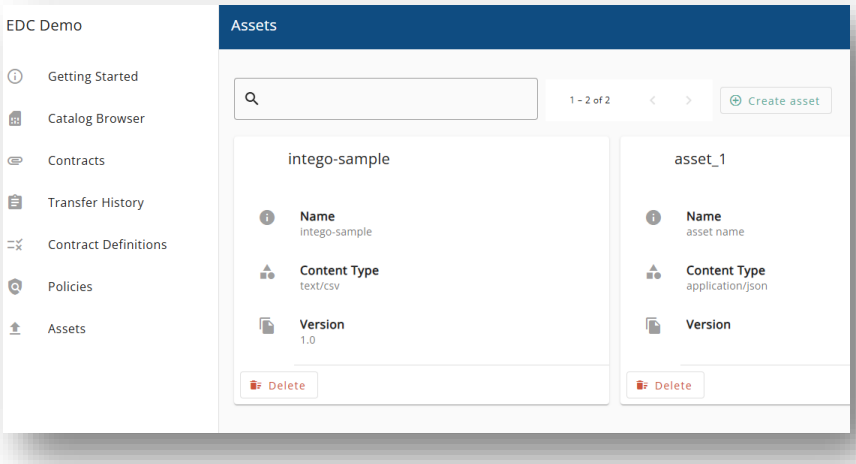
Gedurende dit onderzoeksproject verliepen de onboarding procedures relatief vlot. De installaties en configuraties gebeurden manueel, maar in een uiteindelijke productieversie van de data space zou het technisch onboarden van een participant veelal geautomatiseerd kunnen worden.

8.4.2 Registratie databron

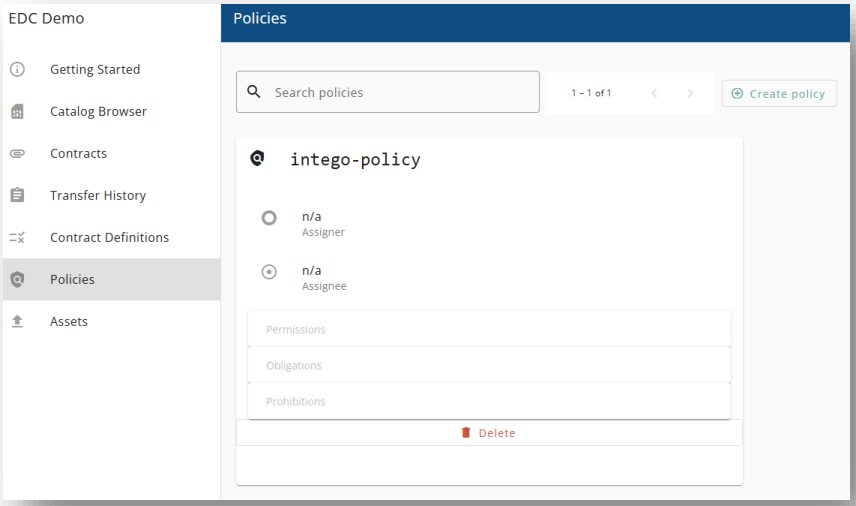


Een databron registreren op een connector verloopt in drie (manuele) stappen.

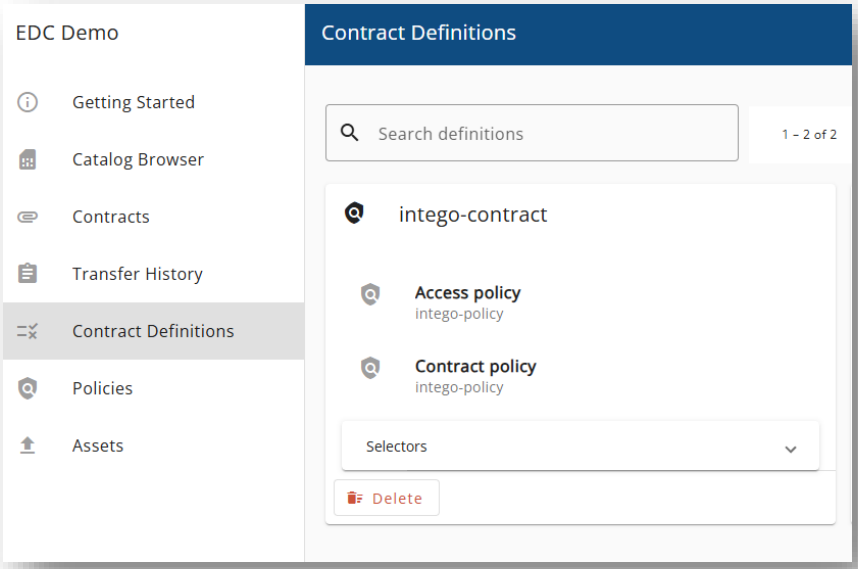
1) Het registreren van het (end-point) van de data asset.
   Bv. de url naar de data asset op een file server.



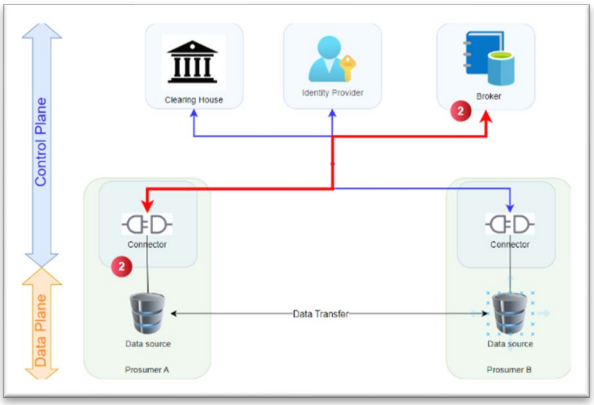
2) Het aanmaken van de gebruikers-voorwaarden (usage policy).



3) Het koppelen van de usage policy met de data asset.
Het resultaat is een contractdefinitie.

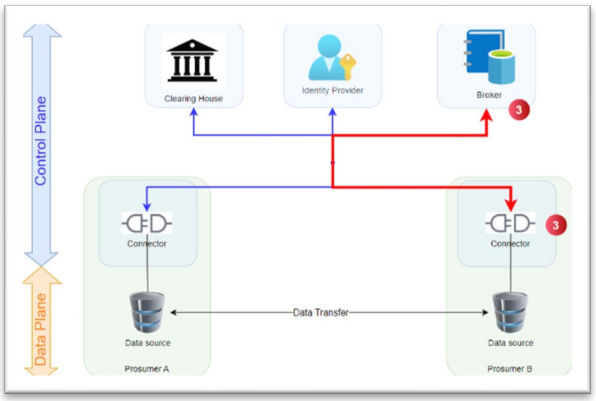


8.4.3 Delen van metagegevens met broker



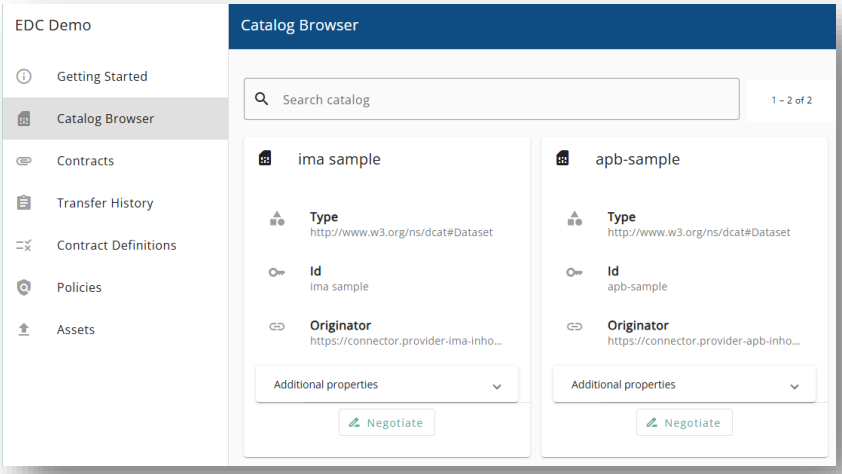
Eens de databron (via een contractdefinitie) geregistreerd is in de connector, zal de brokercomponent automatisch de contractdefinitie identificeren en de gegevens opnemen in zijn cataloog. Niet alleen de gegevens van de dataset, maar ook de usage policy alsook de identiteit van de provider worden genoteerd in de catalogus.
De gebruiker hoeft hiervoor niets speciaal te doen; de broker is geconfigureerd om op vaste frequenties te synchroniseren met alle connectoren in de data space.

8.4.4 Ontdekken van de databronnen

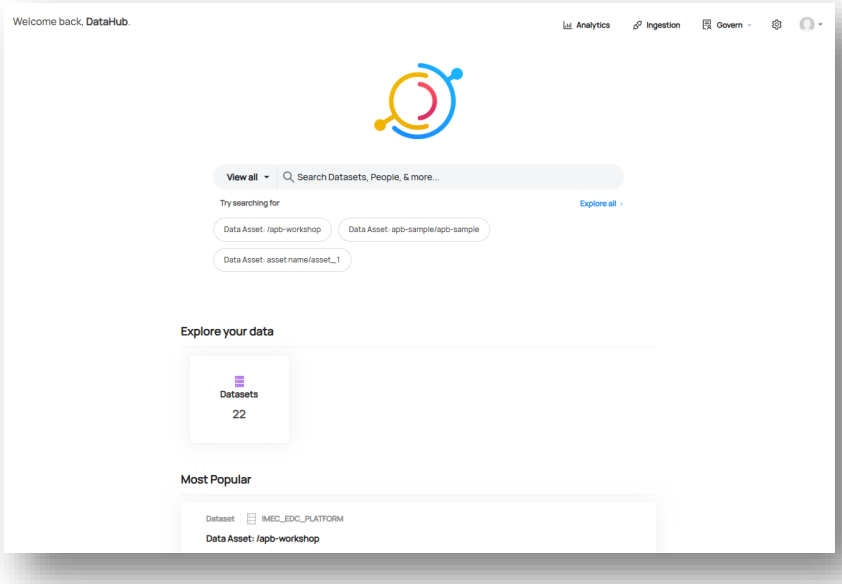


Door het frequente synchronisatieproces tussen de connectoren en de broker zijn de beschikbare datasets terug te vinden op twee plaatsen: in de catalog browser van de lokale connector of in de brokercomponent zelf van de data space.

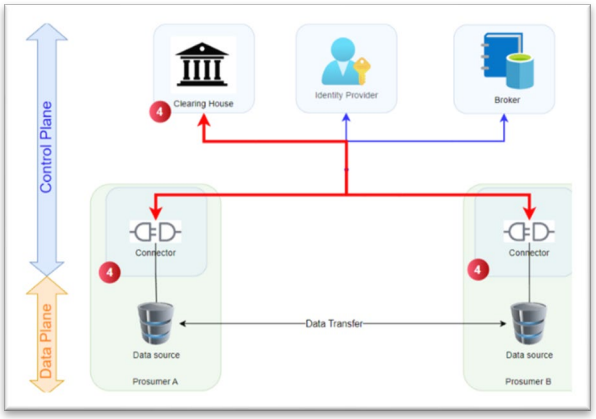
Datasets ontdekken via de catalog browser in het connector dashboard. Dit zijn alle beschikbare contractdefinities op de data space, maar enkel beperkte informatie over de dataset is beschikbaar.



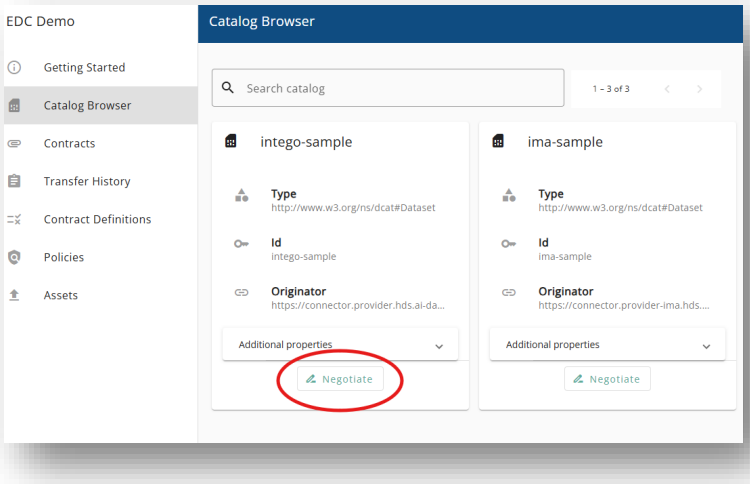
Uitgebreidere metadata van de datasets is terug te vinden in de broker. Via de user interface van DataHub, kan de gebruiker uitgebreide informatie terugvinden alsook bevragingen doen op de metadata.
De broker catalog is ook beschikbaar voor niet participanten van de data space, die (nog) geen connector op hun infrastructuur hebben draaien.



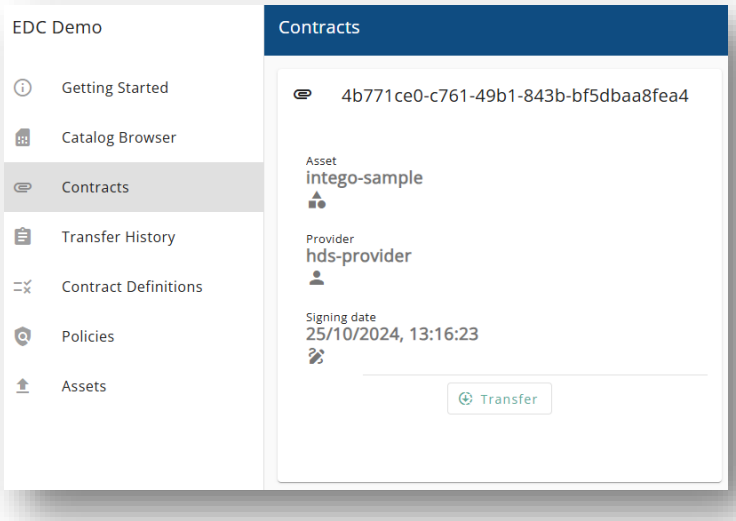
8.4.5 Datadeling contract afsluiten



Eens een datagebruiker de dataset gevonden heeft die hij wenst te gebruiken kan hiervoor een datadelingscontract afsluiten met de dataproducent. De consument is akkoord met de voorwaarden (usage policy) die de producent oplegt en vraagt via zijn connector een contract aan.
De aanvraag wordt doorgestuurd naar het clearing house. Het clearing house keurt de contractaanvraag automatisch goed of kan het aanvraagproces onderbreken en verder verifiëren met externe partijen (bv. checken of er een geldige data permit is afgeleverd door een privacy autoriteit).
Eens de contractaanvraag is goedgekeurd worden de producent en de consument hiervan op de hoogte gesteld en zal het contract als een actief contract in hun connectoren geregistreerd staan.

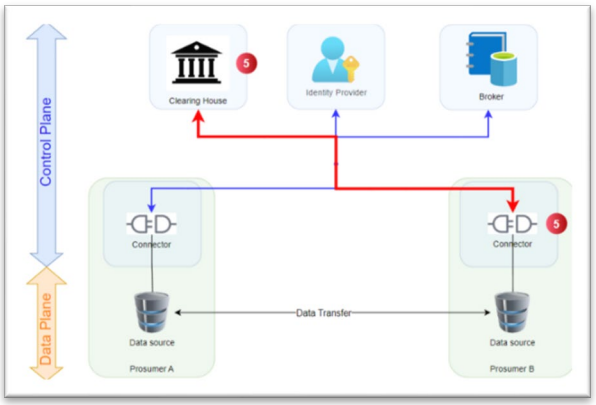


Contractenaanvragen (negotiaties) kunnen vanuit de catalog browser manueel geïnitieerd worden.



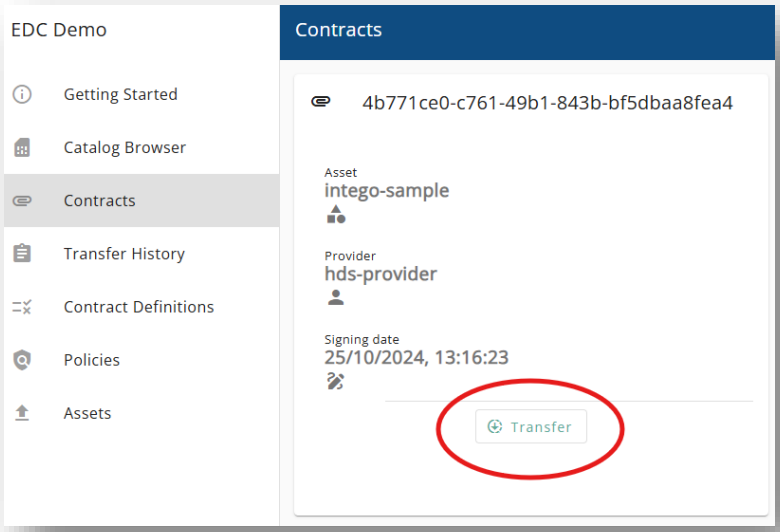
Actieve contracten worden op de connector geregistreerd en zijn te bekijken via het connector dashboard.

8.4.6 Initiëren datatransfer

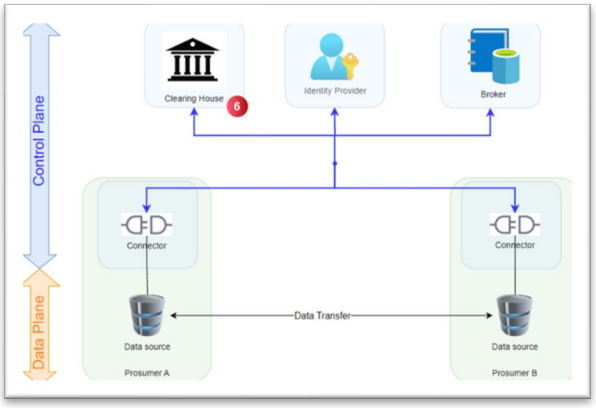


Na een succesvolle contractnegotiatie kan een datatransfer geïnitieerd worden. De aanvraag gaat vanuit de data consumer naar het clearing house.

Een datatransfer wordt geïnitieerd vanuit de lijst van actieve contracten.



8.4.7 Goedkeuren van datatransfer

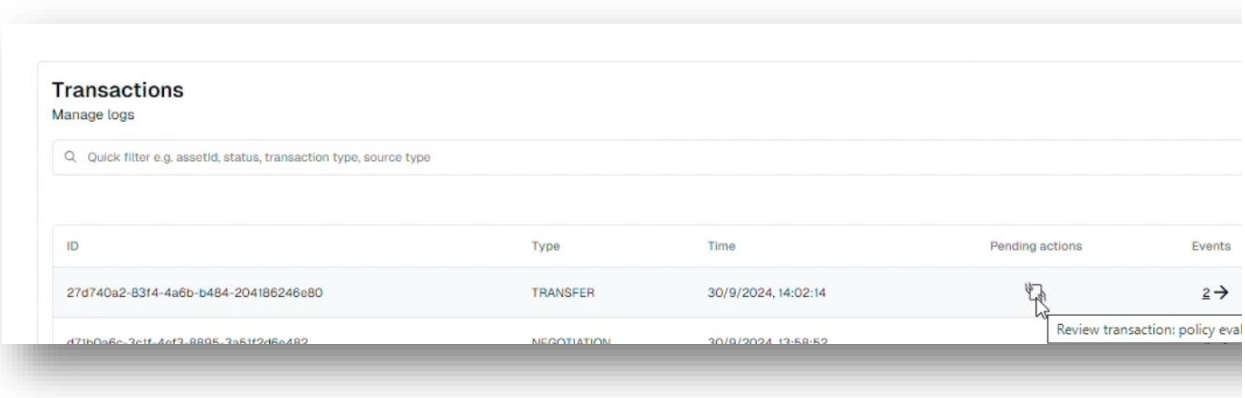


De transferaanvraag komt aan bij het clearing house waar de aanvraag zal gecontroleerd worden:

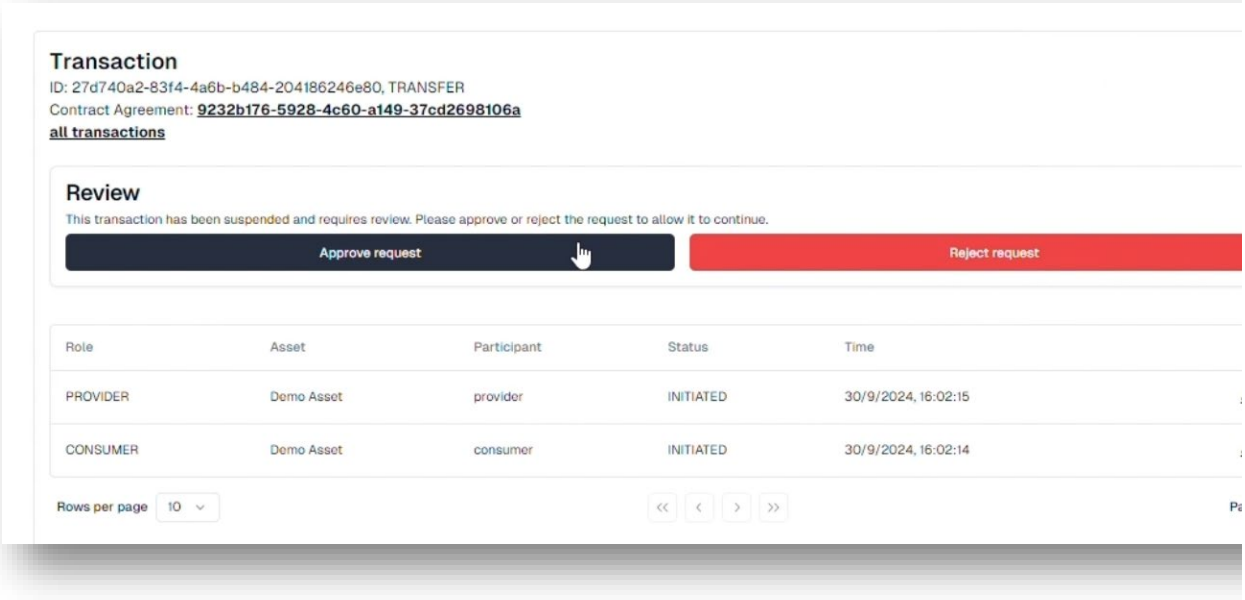
- Is het nog een actief contract?
- Zijn de actoren correct?
- Zijn de voorwaarden van het contract voldaan?

Het clearing house zal de aanvraag goedkeuren of afkeuren.

Het evalueren van de aanvraag verloopt standaard geautomatiseerd. Voor dit project is de mogelijkheid geïmplementeerd om het evaluatieproces te onderbreken en een manuele evaluatiestap te doen.
De functionaliteit wordt vervolgens ook gebruikt in het geval dat de evaluatie automatisch gebeurt en de evaluatie negatief is, om vervolgens de transfer manueel toch goed te keuren en alsnog te laten plaatsvinden.

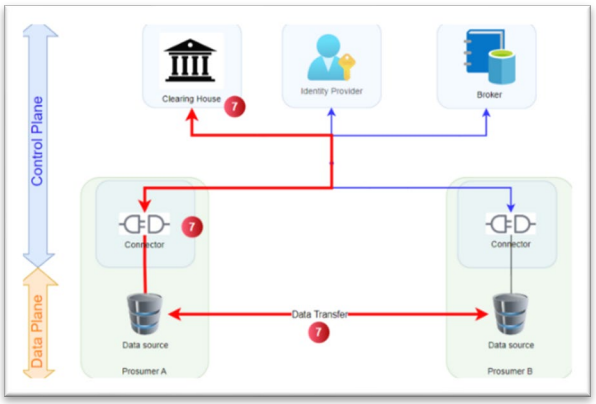


In het clearing house is een lijst van transacties beschikbaar. Een nieuwe aanvraag verschijnt in de lijst. Indien er een manuele goedkeuring nodig is, kan er doorgeklikt worden op de transactie.

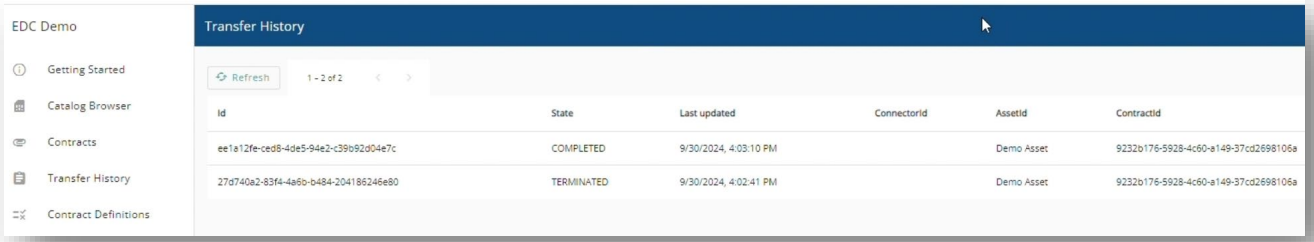


De transactie wordt goedgekeurd (of afgekeurd) door op de overeenstemmende knoppen te klikken.

8.4.8 Uitvoeren van datatransfer



Na de goedkeuring door het clearing house ontvangt de connector van de provider het bericht dat de datatransfer mag opgestart worden.



Via het connectordashboard kan de transactiegeschiedenis bekeken worden. Goedgekeurde en uitgevoerde transacties zijn zichtbaar in de transactiegeschiedenis van zowel de connector van de data consumer als de connector van de data provider. De volledige transactiegeschiedenis is ook beschikbaar in het clearing house.

8.5 DATASTANDAARDEN

Standaarden zijn bedoeld om **data probleemloos uit te wisselen** tussen verschillende systemen. Dit maakt het mogelijk om een ecosysteem op te bouwen waarin data vrij kan bewegen. In een economie waarin alles steeds meer draait om data, zijn standaarden cruciaal en een sleutel tot succes. Hetzelfde geldt voor data spaces. Data spaces worden specifiek opgezet in sectoren zoals energie, mobiliteit en gezondheid. De data spaces starten allemaal met hetzelfde idee: een solide basis, een gemeenschappelijke taal die ervoor zorgt dat gestructureerde data eenvoudig uitgewisseld en gekoppeld kan worden.

Om ervoor te zorgen dat data op een gemakkelijke manier gedeeld kan worden, is het belangrijk dat iedereen **dezelfde "taal"** spreekt. Dit geldt zeker in de medische en welzijnssector, waar data-uitwisseling vaak een grote rol speelt. Om een beter inzicht te krijgen in de standaarden die hierbij van belang zijn, is er een overzicht gemaakt van de meest gebruikte datastandaarden binnen de Vlaamse zorgsector en van die standaarden die Europa aanbeveelt (zie bijlage 8.C). Deze studie is niet bedoeld als een technisch document, maar juist als een toegankelijk hulpmiddel om een overzicht te krijgen van de standaarden die helpen om gegevens tussen verschillende partijen uit te wisselen.

Bij het samenstellen van het overzicht werd nagedacht over een aantal belangrijke vragen.
Welke standaarden zijn eigenlijk het meest relevant in de gezondheidszorg? Hoe werken die standaarden samen? En in welke situaties worden ze gebruikt? Daarnaast was het ook belangrijk om te kijken naar de sterke en minder sterke punten van iedere standaard. Enkele van deze standaarden werden ook gemapt op de data die afkomstig waren van de partners van dit onderzoeksproject.

Interessant is dat **niet elke standaard hetzelfde doel dient**. Sommige standaarden richten zich op het zorgen dat verschillende systemen dezelfde betekenis aan data geven, dit wordt semantische interoperabiliteit genoemd, terwijl andere standaarden juist bedoeld zijn om data veilig op te slaan, door te sturen of zelfs te vinden. Het is dus niet zo dat één enkele standaard alles kan oplossen. In de praktijk moet er **vaak een combinatie** van verschillende standaarden gebruikt worden om een systeem goed te laten werken.
Zo ontstaat een wereld waarin data vloeiend en efficiënt kan worden uitgewisseld, en dat is precies wat nodig is om de gezondheidszorg, en eigenlijk elke sector, efficiënter te maken.

Onderstaande tabel geeft een overzicht weer van alle standaarden die onderzocht werden:

	Doel		Internationale standaarden	Standaarden enkel in België/Vlaanderen (naast de internationale)
COMMUNICATIE	SEMANTISCHE INTEROPERABILITEIT VAN DATA	TERMINOLOGIE	*SNOMED CT (diagnoses, procedures, symptomen, medicatie,...)* *ICD-10, ICD-11 (diagnoses, procedures)* *LOINC (labo en klinische testen)* *ICPC (symptomen, diagnoses, interventies, in eerstelijn)* *ICF (classificatie voor functioneren, kinesitherapie)* *MEDDRA (nevenwerkingen)* *ATC (geneesmiddelen)* *CPT (procedures, enkel USA)* *CDISC SDTM (data model for structuring research data)*	*OSLO (linked data, overheen domeinen)*
	OPSLAAN VAN DATA	OPSLAG	*OpenEHR* *ISO 13606 (modeleren van data voor primary use)* *SOLID* *OMOP-CDM (secondary use)* *DICOM (imaging)* *IDMP (SPOR) (medicatie)* *ISO 800-110* *IHE XDS*	
	DOORSTUREN VAN DATA	DOORSTUREN	*HL7 FHIR* *LDES* *NGSI (LD)*	*KMEHR* *SUMEHR*
	VINDBAAR MAKEN VAN DATA	FINDABILITY	*DCAT-AP (metadata standaard)* *BBMRI-MIABIS* *Bio-image archive* *CESSDA CMM* *ECRIN-CRMDR* *FAIRSHARING* *INSPIRE* *PHIRI*	*DCAT-AP VL*

Figuur 33: Overzicht onderzochte datastandaarden

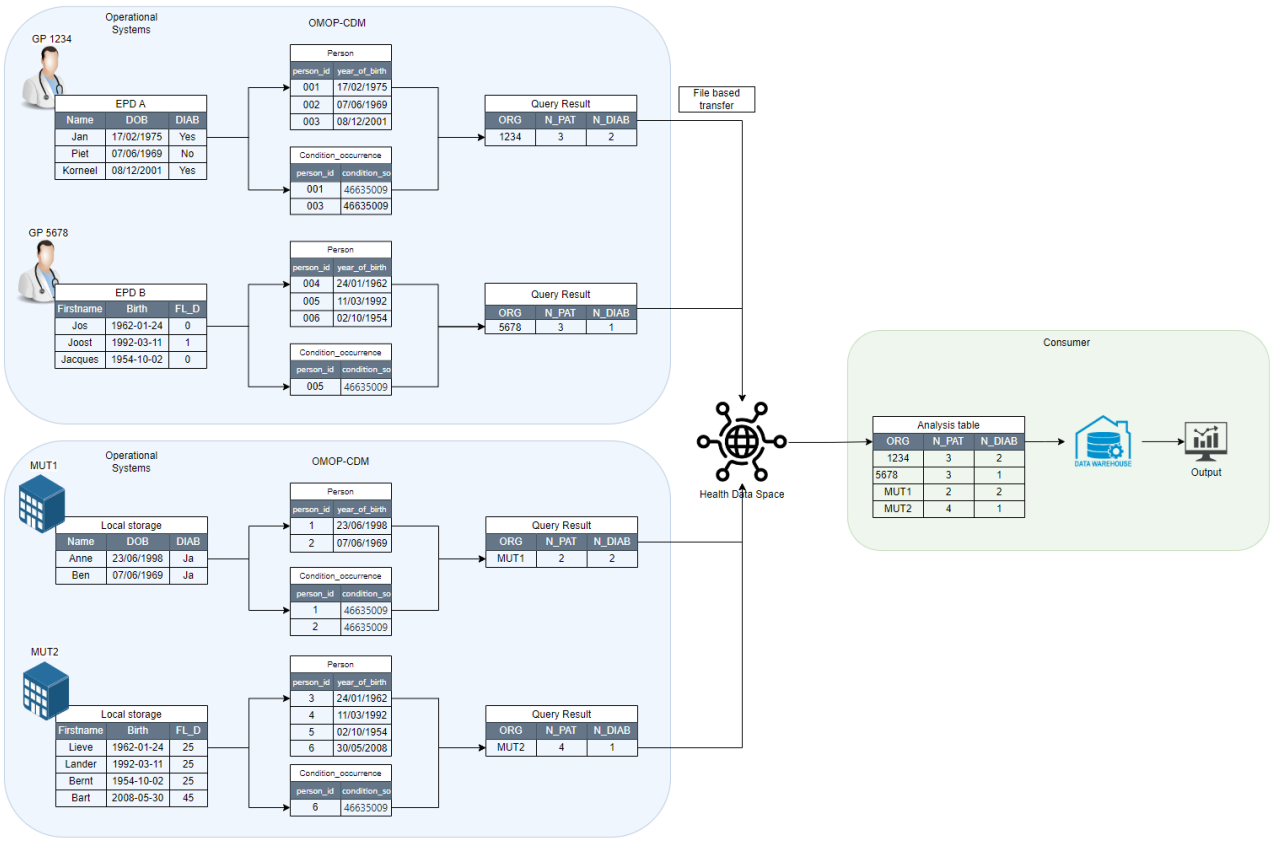
De **conclusie** is de volgende:

> Alle standaarden hebben hun **specifieke doel** en moeten ook daarvoor worden ingezet. Dit wordt momenteel te weinig onderkend. De keuze van een datastandaard is use case afhankelijk. Voorbeelden van meest geprefereerde standaarden naargelang het doel (niet-limitatief):
  - Primaire datagebruik: OpenEHR
  - Secundair datagebruik: OMOP-CDM
  - Data uitwisseling: HL7 FHIR
  - Metadata (opslag + uitwisseling): DCAT-AP
  - Codering medische patiënt data: SNOMED CT
  - Codering laboresultaten: LOINC
> Alle data laten stromen in het ecosysteem zoals het vandaag is, zal nooit lukken door één standaard te kiezen. Het zal altijd een **combinatie** zijn van verschillende standaarden om een end-to-end verhaal te onderschrijven. Een health data space zal daarvoor verschillende datastandaarden moeten kunnen ondersteunen.
> Het implementeren van een **(nieuwe) standaard** heeft consequenties voor (en impact op) het hele ecosysteem: het kost (veel) **tijd, inspanning en geld**. Het einddoel, dat de gezondheidszorg in België/Vlaanderen er beter van wordt, moet daarbij voorop gesteld worden.
> "We zijn niet slimmer dan de rest." Idealiter volgt men internationale (en federaal) ondersteunde keuzes. Daarbij hoort dan een lokale governance structuur die internationale opvolging doet en beslissingen neemt voor het lokaal gebruik.

Tijdens het uitwerken van de PoC werd een technische implementatie getest van de belangrijkste datastandaarden (FHIR – OMOP). De moeilijkheden lagen in het aggregatieniveau van de ontvangen data. Niet alle data bevonden zich op hetzelfde aggregatieniveau waardoor niet alle datasets gemapt konden worden op een datastandaard. Bijgevolg zijn geen datastandaarden toegepast op de datasets gebruikt in deze PoC.

8.5.1 OMOP-CDM in een health data space: theoretisch voorbeeld

In het onderstaande theoretisch voorbeeld is een scenario uitgewerkt hoe OMOP-CDM zou kunnen gebruikt worden in combinatie met een health data space. In het scenario heeft elke data provider een verschillend operationeel systeem en bijgevolg ook een verschillende manier van dataopslag.
Elke data provider heeft echter wel zijn gegevens **geconverteerd naar de OMOP-CDM-standaard voor secundair gebruik** van de gezondheidsgegevens. De data consumer is enkel geïnteresseerd in de geaggregeerde gegevens van de data providers en definieert een query op basis van de OMOP-CDM-standaard. Deze query wordt bezorgd aan de providers of wordt beschikbaar gemaakt op de health data space via de app store (zie 3.4.1.2 Technische bouwstenen volgens IDSA). Gezien de query gebaseerd is op de OMOP-CDM standaard, kan de query bij elke data provider probleemloos en gestandaardiseerd uitgevoerd worden en zal hetzelfde output formaat als resultaat hebben. Het resultaat wordt via de health data space gedeeld met de data consumer (aanvrager). De consumer kan de resultaten eenvoudig op elkaar 'leggen' en vervolgens de data-analyse starten.



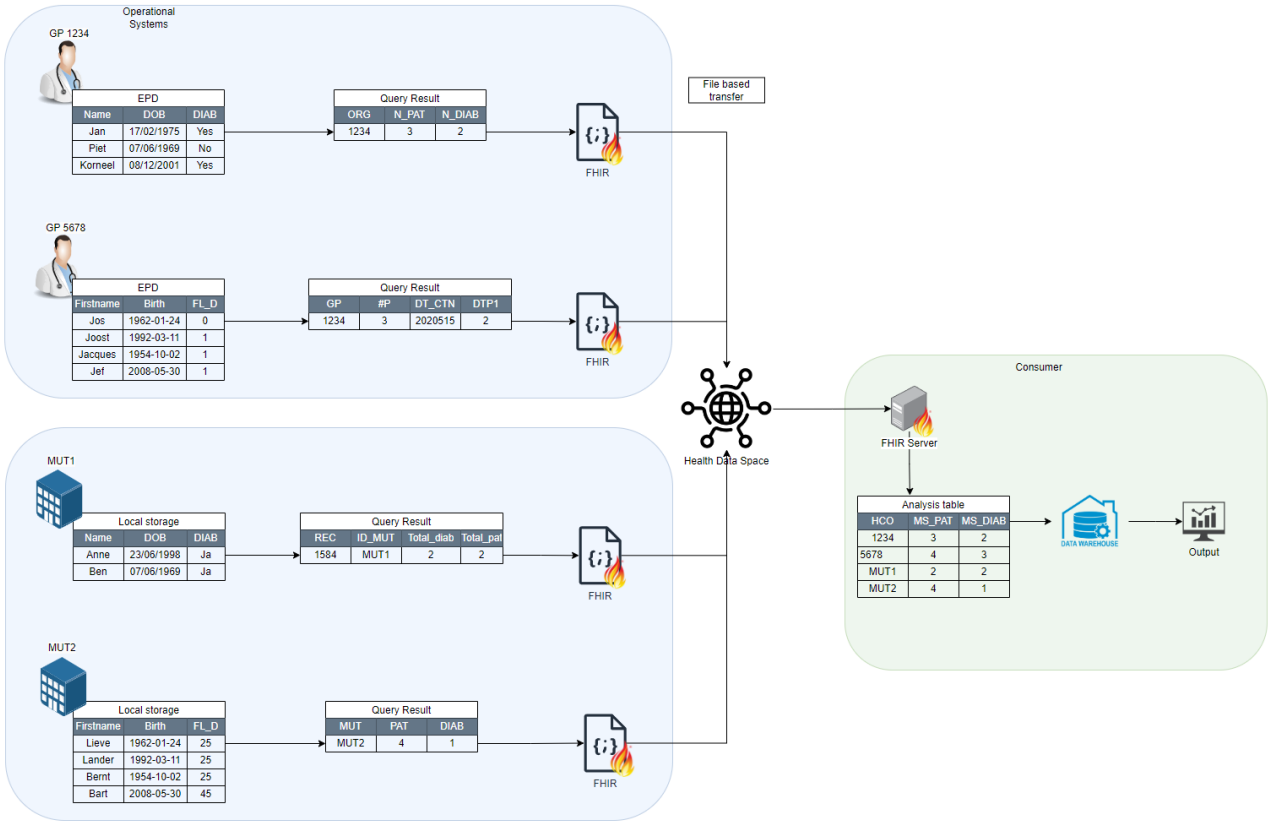
Figuur 34: Voorbeeld van het gebruik van de OMOP-CDM standaard gecombineerd met een data space

De datatransfer zelf kan een eenvoudig file-based (csv) data transfer zijn (bv. SFTP). Een extra standaardisatie tijdens het datatransferproces is in dit scenario niet nodig. De voordelen van werken met de OMOP-CDM zijn duidelijk uit het voorbeeld, maar er zijn ook nadelen aan verbonden. Zo zal elke provider de investering moeten doen om zijn data om te vormen naar de OMOP-CDM standaard. Daarnaast zijn er beperkingen aan OMOP-CDM: het is **minder geschikt voor primair data** gebruik en is ook **minder geschikt voor niet-diagnostische patiëntendata** zoals bijvoorbeeld labo resultaten.

8.5.2 FHIR in een health data space: theoretisch voorbeeld

Een ander mogelijk scenario wordt weergegeven in de figuur hieronder. Hierbij wordt geen gebruik gemaakt van OMOP-CDM, maar wel van HL7-FHIR om de **datatransfer te standaardiseren**. In dit scenario maakt elke data provider zijn eigen query op zijn datamodel. Vervolgens mapt de provider het resultaat op de FHIR standaard en maakt een FHIR bericht (XML of CSV bestand). Het FHIR bericht wordt vervolgens via de data space naar een FHIR server bij de data consumer gestuurd. De FHIR server controleert het bericht op zijn correctheid (file formaat en datastructuur) en laadt de inhoud in een gestandaardiseerde analysetabel, waarna de data-analyse kan starten.

De voordelen aan de FHIR-standaard is dat deze geschikt is voor meerdere soorten van medische data en het is zeer **flexibel en uitbreidbaar**. Nadelen zijn de investeringen die moeten gedaan worden in het converteren naar een FHIR-bericht en de installatie van een FHIR-server. Bovendien zijn er in België al **verschillende FHIR-implementatiegidsen ontwikkeld**, wat een **extra complexiteit** toevoegt aan het gebruik van FHIR als standaard uitwisselingsstandaard.

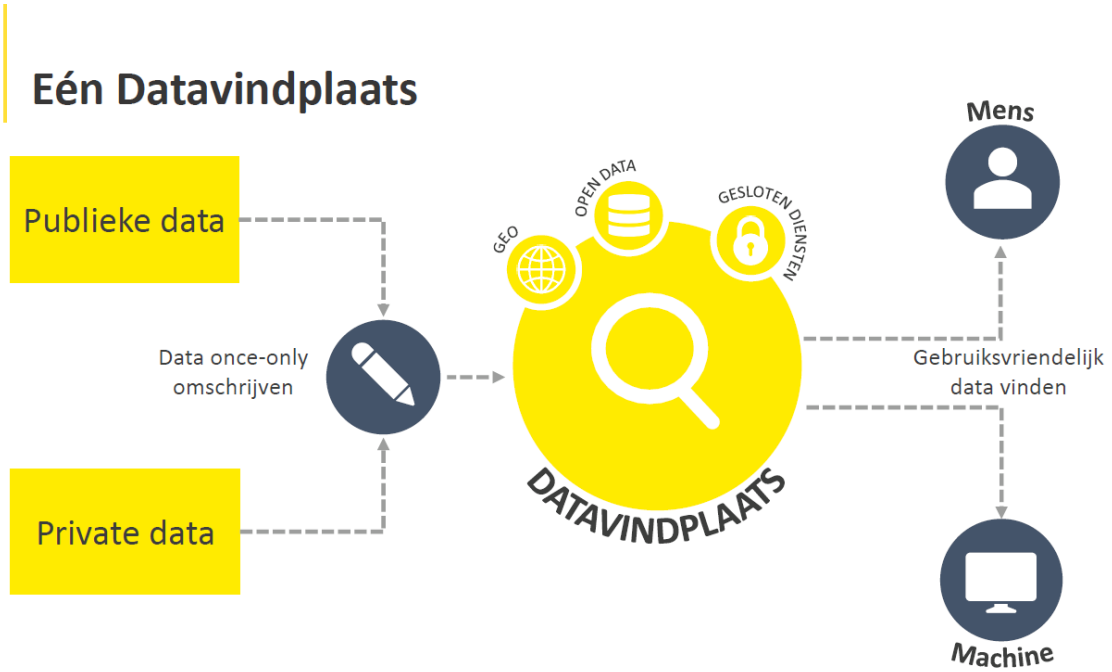


Figuur 35: Voorbeeld van het gebruik van FHIR gecombineerd met een data space

8.6 METADATA.VLAANDEREN

Metadata.Vlaanderen[440] is het **centrale knooppunt** voor het beschrijven en benaderen van allerhande **gegevens in Vlaanderen**. Het biedt gedetailleerde beschrijvingen van datasets en diensten, voornamelijk afkomstig van bestaande Vlaamse metadataknooppunten, die dagelijks worden gesynchroniseerd.

Datavindplaats is de centrale opslagplaats voor open data van Vlaamse overheden. Door gebruik te maken van het **DCAT Application Profile for Europe** (DCAT-AP), specifiek DCAT-AP Vlaanderen (DCAT-AP VL), wordt consistente metadata-uitwisseling op lokaal, Vlaams, federaal en Europees niveau gegarandeerd.



Figuur 36: De Datavindplaats van Metadata.vlaanderen

Binnen het huidig onderzoek werd technisch onderzocht hoe de health data space kan linken met het Vlaamse metadataplatform, aangezien de metadatacatalogus van de **HDA** via Datavindplaats de Vlaamse metadata wenst op te halen.

8.6.1 Linken met Datavindplaats

Datavindplaats is gebaseerd op de open source GeoNetwork[441] specificatie. Dit maakt het mogelijk om op twee verschillende manieren datasets en/of API's beschikbaar te maken op de Datavindplaats:

> Via Metadata Vlaanderen is het mogelijk **'once only'** een dataset en/of API te beschrijven. Na publicatie zijn ze beschikbaar op de Datavindplaats.

> Indien de aanbieder zelf al een metadata-oplossing ter beschikking heeft, is het mogelijk deze te laten **harvesten** in Metadata.Vlaanderen. Na publicatie en harvesting van de aangeboden API's en datasets zijn deze beschikbaar op de Datavindplaats.

Binnen dit project werd een metadata-oplossing uitgewerkt op basis van de EDC-connector en datahub. Er werd daarom gekozen voor de optie harvesten in Metadata.Vlaanderen.

[440] *https://metadata.vlaanderen.be/*

[441] *GeoNetwork is een catalogustoepassing voor het beheren van bronnen met ruimtelijke referenties. Het biedt krachtige functies voor het bewerken van metadata en zoekfuncties, evenals een interactieve webkaartviewer.*

8.6.2 Harvester

Om een verbinding met Metadata.Vlaanderen op te zetten volstaat het om een open **DCAT endpoint** op te zetten van de federated catalog (broker) van de health data space.
Deze stap is cruciaal voor Metadata.Vlaanderen om toegang te krijgen tot de Health Data Space-catalog en deze te integreren in hun ecosysteem. Dit kon op twee mogelijke manieren:

- een DCAT endpoint opzetten in Turtle[442]-formaat of
- integratie met de LDES DCAT-AP feed.

Een eerste optie is het creëren van een service die een **open endpoint** opzet die alle metadata-informatie in DCAT-AP formaat bevat in Turtle-formaat. Een Turtle-document maakt het mogelijk om een RDF-grafiek in een compacte tekstuele vorm op te schrijven. Het Resource Description Framework (RDF) is een universele taal voor het representeren van informatie op het web. De metadata in het Turtle-document dient in sync gehouden te worden met de federated catalog van de Health Data Space. Deze aanpak zorgt ervoor dat de gegevens van de federated catalog beschikbaar zijn in een machine leesbaar formaat (Turtle), dat toegankelijk en geoogst kan worden door Metadata.Vlaanderen. Deze methode kan echter leiden tot hogere crawlbelastingen voor de harvesters, omdat de hele catalog pagina mogelijk regelmatig moet worden geüpdatet.

Gedurende dit onderzoeksproject zijn de eerste stappen gezet voor het opzetten van een endpoint met een Turtle-bestand. Daarbij is het onderzoeksteam erin geslaagd om een endpoint te voorzien met een Turtle-bestand dat opgepikt (geharvest) is geworden door Metadata.Vlaanderen. Het gegenereerde Turtle-bestand was nog niet helemaal leesbaar door Metadata.Vlaanderen en zal in een mogelijks vervolgproject verder gefinetuned moeten worden.

Een tweede optie is de integratie met de **LDES DCAT-AP feed**. Deze feed-specificatie maakt incrementele synchronisatie van catalog gegevens mogelijk, waardoor harversters de hele catalog niet herhaaldelijk hoeven te parsen. De LDES-specificatie introduceert een efficiëntere methode voor het beheren en distribueren van catalog gegevens door deze op te splitsen in kleinere stukken. Harvesters hoeven alleen te synchroniseren met de nieuwste node in de feed, wat resulteert in:

> Verminderde belasting: harvesters hoeven niet elke keer de volledige catalog opnieuw te parsen[443]. Dit leidt tot een snellere verwerking en een lagere benodigde rekenkracht.

> Incrementele updates: catalogs kunnen worden opgedeeld in beheersbare stukken, waardoor gedeeltelijke updates mogelijk zijn in plaats van de hele catalog als één grote pagina te publiceren.

Om deze overgang te vergemakkelijken zouden VSDS[444]-bouwblokken gebruikt kunnen worden om de federated catalog van de Health Data Space als een DCAT-stream te publiceren. Deze stream zou dan beschikbaar kunnen worden gesteld als een open portaal dat dan kan geoogst worden door het Metadata.Vlaanderen-platform. Op die manier kan de federated catalog worden gepubliceerd op een manier die compatibel is met toekomstige standaarden voor het verzamelen van metadata, waardoor compatibiliteit op lange termijn kan worden gegarandeerd met de evoluerende vereisten van Metadata Vlaanderen.
Gedurende de looptijd van dit onderzoeksproject is door Metadata.Vlaanderen aangegeven dat de infrastructuur momenteel nog niet klaar is metadata via de LDES-stroom te ontvangen.

[442] *https://www.w3.org/TR/turtle/*

[443] *Invoer converteren naar een bruikbare datastructuur*

[444] *Zie 3.4.3.2 Digitaal Vlaanderen en de Vlaamse Smart Data Space en 8.7 Link met de Vlaamse Smart Data Space*

8.7 LINK MET DE VLAAMSE SMART DATA SPACE

De Vlaamse Smart Data Space (VSDS) is ontworpen om de fundamentele componenten op te zetten die nodig zijn voor de verspreiding en het gebruik van **Linked Data Event Streams (LDES)**.
Bovendien vergemakkelijkt het de integratie van deze LDES als datareservoirs binnen een data space framework. Het project wordt naar verwachting afgerond tegen het eerste kwartaal van 2025.

Volgende **VSDS-bouwstenen** zijn gedefinieerd:

> **LDES-server:**
  - De LDES-server, toegankelijk via de LDES-client, ondersteunt de publicatie en fragmentatie van linked data. Het bevat ook een retentielaag voor effectief datalevenscyclusbeheer.

> **VSDS-Linked-Data-Interactions:**
  - Deze component fungeert als een ETL-tool voor linked datasets en biedt Java- en NiFi-diensten om gegevens om te zetten naar een linked data-formaat. Daarnaast bevat het een LDES-client voor het chronologisch consumeren van gegevens.

> **VSDS-Dataspace-Connector:**
  - Gebouwd op de EDC-connector, vergemakkelijkt deze extensie de consumptie van gepubliceerde linked data streams binnen het EDC-ecosysteem.

Vanaf juli 2024 omvat het onboardingsproces voor het VSDS-project het publiceren van de klantgegevens vanuit hun oorspronkelijke formaat en het toegankelijk maken ervan via een Linked Data Event Stream met behulp van de eerdergenoemde componenten.
Momenteel omvat het onboardingsproces geen opzet van een data space, omdat VSDS geen infrastructuur-componenten biedt voor authenticatie, autorisatie en deelnemersbeheer binnen de data space.
Deze aspecten zijn echter geanalyseerd en kunnen in toekomstige fasen van het project worden opgenomen. Je kan dus op de VSDS onboarden als je enkel een LDES-setup hebt.

Om gegevens uit te wisselen met VSDS-deelnemers die zijn geonboard op VSDS, is het een vereiste dat de gegevens zijn geformatteerd als een Linked Data Event Stream (LDES) en voldoen aan de OSLO-modellen voor de domeincontext. Binnen dit onderzoeksproject werd eveneens onderzoek gevoerd naar wat nodig is om een health dataset om te zetten naar linked data.
In de planning van VSDS zal aan het einde van het project ook een testbed-service worden aangeboden. Deze service zal een conformiteitscontrole uitvoeren van de dataset tegen het LDES en OSLO-model.

VSDS mist momenteel een data space-infrastructuur voor de onboarding en authenticatie van deelnemers. Hoewel verifiable credentials met DID Web zijn onderzocht en gedemonstreerd in het project, is daadwerkelijke implementatie nog in afwachting.
Gezien de hoge uitbreidbaarheid van de EDC-component die door de health data space wordt gebruikt, zou het integreren van deze configuratie met VSDS geen technische uitdagingen mogen opleveren zodra VSDS zijn implementatie vanuit een authenticatieperspectief heeft voltooid.

VSDS maakt ook gebruik van de EDC data space component, echter, de huidige versie van VSDS is 0.4.1 EDC in hun ontwikkelrepository, terwijl voor dit onderzoeksproject versie 0.6.4 van de EDC-connector gebruikt wordt. Er is geen garantie voor interoperabiliteit tussen componenten van verschillende EDC-versies. Naarmate beide projecten vorderen in samenwerking met EDC, zal interoperabiliteit worden gegarandeerd bij de release van een stabiele versie van EDC op de markt.

In de praktijk echter blijkt dat het omzetten van gezondheidsdata naar het LDES-formaat, samen met de installatie van de LDES-client nodig om gebruik te kunnen maken van deze VSDS-bouwblokken, een extra drempel is voor data aanbieders.

8.8 ZORGATLAS

Het ZorgAtlas Data Platform van Departement Zorg biedt een **platform** aan dat **data** kan **ontvangen, stockeren, analyseren en visualiseren**. Bij aanvang van dit project werd aangenomen dat het ZorgAtlas Data Platform een vergaande integratie met de VHDS zou moeten ondergaan. Echter het decentrale karakter van een data space, samen met het feit dat bestaande fysieke datadelingsmechanismen kunnen blijven bestaan (= data plane), hebben deze aanname ontkracht.
De installatie van een **connector** is voldoende om te kunnen deelnemen aan de VHDS. De connector van het Departement Zorg zal aan andere connectoren laten weten waar en hoe de data gedeeld kan worden. Tijdens het onderzoeksproject is ook de **brokercomponent** geïnstalleerd op de infrastructuur van het Departement Zorg (AWS). Naast de configuratie van de connectiegegevens naar de andere componenten, was er geen verdere integratie nodig in het bestaande ZorgAtlas Data Platform.
Gezien alle VHDS-componenten individueel installeerbaar zijn, worden er ook geen problemen verwacht om ook deze te installeren op het bestaande ZorgAtlas Data Platform.

De volgende bedenking moet wel in acht genomen worden: volgens de EHDS-regulering kan een data holder of een data user geen HDAB zijn, en omgekeerd. Een HDAB is een entiteit die één of meerdere functies uitvoert waarvoor volgens de EHDS de coördinerende HDAB van een Europese lidstaat verantwoordelijk is. De functies omvatten o.a. beheren van de datacatalogus, bepalen van datastandaarden en kwaliteit, pseudonimisatie, beheer SPE's … Om EHDS-compliant te zijn, zal er daarom een keuze gemaakt moeten worden welke rol (data holder/user, HDAB …) Departement Zorg wil gaan opnemen in de VHDS.

8.9 RISICOANALYSE

Zoals te lezen is in vorige hoofdstukken werd binnen de PoC van dit onderzoeksproject gekozen om verder te bouwen op de opensource **EDC connector** van de Eclipse Foundation. Als onderdeel van deze keuze voor EDC werd eveneens een risicoanalyse uitgevoerd.

8.9.1 Eclipse Foundation

De **Eclipse Foundation** (EF) staat bekend om een zeer gestructureerde aanpak van projectsamenwerking en governance. Elk EF-project moet voldoen aan een **gemeenschappelijk ontwikkelingsproces** nadat er een adequate opleiding is gegeven aan de betrokkenen. Het gemeenschappelijke ontwikkelingsproces biedt duidelijke en beknopte regels, **transparante** en **controleerbare** praktijken voor structuur, organisatie, rollen en verantwoordelijkheden, en ontwikkelingscyclus, zodat iedereen goed geïnformeerd en bewust is van de structuur en organisatie van het project.

EF-projecten zijn niet verplicht om hun **beveiligingsaanpak** te documenteren, maar ze moeten zich wel houden aan de richtlijnen van het projecthandboek over beveiligingsontwikkeling, beveiligingstests en het ontdekken en beheren van kwetsbaarheden. Elk project documenteert hoe de beveiliging is geïmplementeerd in een security.md bestand binnen de code repository.

8.9.2 Tractus-X

Tractus-X is een project van de Eclipse Foundation geïnitieerd door **Catena-X consortia**, waar specifieke (Caten-X gerelateerde) EDC-extensies kunnen worden uitgevoerd onder duidelijke governance en regels door de EF. Tractus-X heeft de belangengroep **SIG Security** opgericht, die proactief de beste beveiliging praktijken definieert en de codebase van de EDC connector en zijn extensies evalueert. Dit zorgt ervoor dat het publiek verzekerd is van de robuuste beveiliging van het project.

8.9.3 SSDF

De beoordeling van de EDC-connector is gemodelleerd naar de **National Institute of Standards and Technology** (NIST) SP.800.218 publicatie, ook bekend als SSDF of **Secure Software Development Framework**. Het Secure Software Development Framework (SSDF) is een reeks fundamentele, degelijke en veilige softwareontwikkelingspraktijken op basis van richtlijnen voor veilige softwareontwikkeling van organisaties zoals BSA, OWASP en SAFECode.

Hoewel EDC zijn eigen secure code richtlijnen niet expliciet documenteert, neemt het wel **dezelfde richtlijnen van het Tractus X-project** over. Het integratiepunt van de huidige release van de EDC-connector zoals gebruikt in het Tractus X-project (waarbij beide projecten het grootste deel van hun ontwikkelingsteams delen), dient als een fundamentele referentie voor het testen van de EDC-connector en zijn uitbreidingen.

Deze beoordeling omvat de Eclipse Software Development-praktijken en de Tractus X project Secure Development-praktijken als basislijn. Om redenen van beknoptheid laten we de details over die praktijken in elk beoordelingsgedeelte achterwege, maar we bieden links naar beschikbare documentatie en voorbeelden.

Een voorbeeld van de EDC-beoordeling volgens het SSDF is weergegeven in onderstaande figuur.
Het volledige verslag is terug te vinden in bijlage 8.B.

Practice	Tasks	Implementation
Prepare the Organization (PO)		
Define Security Requirements for Software Development (PO.1). This includes requirements from internal sources (e.g., the organization's policies, business objectives, and risk management strategy) and external sources (e.g., applicable laws and regulations).	**PO.2.1**: Create and review new roles and alter responsibilities for existing roles as needed to encompass all parts of the SDLC.	Eclipse Common Development Process and Eclipse Project Handbook define roles, communication and responsibilities.
	PO.2.2: Provide role-based training for all personnel with responsibilities that contribute to secure development.	Training is required using the Eclipse Committer Training, knowledge of Eclipse Project Handbook is a requirement.
	PO.2.3: Obtain upper management or authorizing official commitment to secure development.	In the Eclipse Project Handbook we can find a description of the EMO (Eclipse Management Organization).

8.10 INSTALLATIE VAN DE CONNECTOR

Er zijn verschillende manieren om een EDC-connector te installeren:

> **Java-installatie op een server**
De connector is geprogrammeerd in Java en kan worden geïnstalleerd op een server waarop Java-programma's kunnen draaien.

> **Gecontaineriseerde applicatie**
De connector wordt ook aangeboden als een gecontaineriseerde applicatie. Hierbij worden de connector en alle bijbehorende afhankelijkheden samengevoegd in één container, die vervolgens op het besturingssysteem van de server kan draaien.

Voordelen van de container-aanpak
Alle afhankelijkheden, inclusief hun specifieke versies, zijn voor iedere installatie gelijk. Dit verkleint de kans op incompatibiliteitsproblemen. Een voorbeeld: als de connector alleen getest is met Java-versie 17, maar een deelnemer (participant) Java-versie 21 gebruikt, kan dit problemen veroorzaken. In een container wordt de juiste Java-versie meegeleverd, waardoor dergelijke problemen worden voorkomen.

Configuratie van de connector
De connector heeft een configuratiebestand nodig om parameters te definiëren die specifiek zijn voor de betreffende participant. Denk hierbij aan:

- De ID waaronder de connector bekend is bij de identity provider.
- Het adres waarop de connector bereikbaar is.

Daarnaast moet er een public-private keypair worden aangemaakt. De publieke sleutel wordt ter beschikking gesteld aan de centrale identity provider. De beheerder van deze provider moet de nodige rechten toekennen door de participant toe te voegen.

Netwerkinfrastructuur-aanpassingen
Bovenop het installeren en configureren van de connector zelf, zijn er mogelijk aanpassingen in de netwerkinfrastructuur van de participant nodig. Andere connectoren moeten verbinding kunnen maken met de geïnstalleerde connector. Dit betekent o.a. dat de gebruikte netwerkpoort toegankelijk moet zijn.

Tijdsinvestering
Het installeren van een connector is afhankelijk van de gekozen installatiemethode en van de complexiteit van het eigen platform. Gedurende dit onderzoeksproject zijn verschillende installaties van connectoren uitgevoerd. Hieronder een beknopt overzicht van de installaties en de gemiddelde tijd die nodig was om de installatie en configuratie tot een goed einde te brengen.

PARTICIPANT	MD
Imec (gemiddelde per simulatie)	3
Departement Zorg (connector+ dashboard + MSA)	9,5
FarmaFlux (setup zonder creatie data assets)	4

9 UITWERKING DATA4PHM USE CASE

Zoals reeds besproken in hoofdstuk 5 Use cases werd de **diabetes type 2** use case van het Data4PHM-consortium gekozen als use case voor dit health data space project. In deze use case wordt een **dashboard** gebouwd waarin population health managers en zorgverleners gegevens omtrent diabetes kunnen raadplegen om zo hun beleid en zorg aan te passen. Om dit dashboard te voeden, worden gegevens van **drie verschillende databronnen samengebracht** (Intego, IMA en FarmaFlux). Het samenbrengen van deze data maakt **diepgaande inzichten** tot op **regioniveau** mogelijk, iets wat tot nu toe niet (efficiënt) mogelijk was. Aan de hand van deze use case werd onderzocht of een health data space geschikt is om moeilijk combineerbare data uit verschillende bronnen samen te brengen en een dashboard te voeden. Om deze analyse te maken werd beroep gedaan op de input van de Data4PHM use case partners. Bijgevolg is dit een scope, behoefte-, juridische gap-, governance- en architecturale analyse, die specifiek geënt is op deze use case en de input van deze partners. Voor elke andere use case kunnen andere belangen spelen en dienen dus ook andere stakeholders mee in rekening worden gebracht. Ook voor een eventuele feitelijke implementatie van deze use case, kunnen nog gesprekken met andere stakeholders nodig zijn.

9.1 VISIE, MISSIE EN SCOPE

Het Data4PHM-consortium was reeds van in den beginne intern gealigneerd, met een duidelijke missie en visie geënt op het bevorderen van een **datagestuurde** en **geïntegreerde gezondheidszorg** die **populatiemanagement ondersteunt**. Data4PHM ziet een toekomst waarin diabetesgegevens uit diverse databronnen op een **veilige** en **efficiënte** manier worden samengebracht om betere gezondheidsresultaten te behalen op populatieniveau. Huisartsen en apothekers spelen hierbij een cruciale rol, aangezien zij vaak de eerste lijn vormen in de zorg en toegang hebben tot waardevolle en patiëntgerichte gegevens. Het combineren van de gegevens van huisartsen en apothekers met die van de mutualiteiten, die een landelijke dekking bieden, geeft een mooi inzicht in de prevalentie en indicatoren van diabetes type-2.

Om echt beleidsondersteunend te werken, moet men ook een toegankelijk **dashboard** kunnen voorzien dat de naadloze **integratie en analyse** van die data mogelijk maakt. Daarnaast is er ook nood aan een **onderzoeksplatform** dat de samenwerking en kennisdeling tussen onderzoekers en experten stimuleert. Dit alles vereist voldoende financiering en ondersteuning vanuit ethische en juridische instanties om de databeveiliging en privacy doorheen het proces te waarborgen.

Voor de realisatie van bovenstaande, zijn enkele principes van cruciaal belang voor het Data4PHM consortium.

Integratie en interoperabiliteit
Gegevens uit verschillende zorgsystemen (zoals huisartsenpraktijken, apotheken, ziekenhuizen en andere zorginstellingen) moeten op een **gestandaardiseerde** manier **verzameld** en **uitgewisseld** worden.
Alleen door data samen te brengen krijgen population health managers, beleidsmakers en zorgverleners een volledig en actueel beeld van de gezondheidstoestand van populaties.

Preventieve zorg en populatiemanagement
Om de gezondheidszorg in Vlaanderen (en bij uitbreiding België) betaalbaar te houden, is er nood aan een overgang van een reactief naar preventief zorgsysteem. De verzamelde data dienen daarom gebruikt te worden om **trends** in gezondheid en ziekte te analyseren, **risico's** in kaart te brengen, en **gepersonaliseerde preventieve maatregelen** te nemen. Population health managers en zorgverleners hebben data nodig om specifieke groepen te identificeren zodat ze deze de juiste gepersonaliseerde zorg aan kunnen bieden.
Dit draagt uiteindelijk bij aan een betere gezondheid van de **bevolking** als geheel.

Patiëntgerichtheid

In een meer proactieve en patiëntgerichte zorg, staat de patiënt centraal, en wordt data gebruikt om zorg op maat te bieden. Dit betekent dat data wordt gebruikt om de zorgervaring en uitkomsten voor elke patiënt te optimaliseren. De **burger** speelt zelf ook een rol in het beheren van de eigen gezondheidsgegevens.

Vertrouwen

Datadeling vereist robuuste systemen die de **privacy** van patiënten beschermen en die de zekerheid bieden dat de data ***niet*** worden gebruikt om het werk van individuele zorgverleners te **controleren of te bestraffen**. Er is immers nood aan een systeem dat ondersteuning en motivatie biedt om de kwaliteit van zorg te verbeteren.

Onderzoek en innovatie in zorg

Het is belangrijk dat het **beleid door data ondersteund** wordt, en dat de overheid daartoe een kader voor innovatie uitwerkt. Daarnaast moeten onderzoekers, experten en industrie zich kunnen toeleggen op innovatieve zorgconcepten, de ontwikkeling van geneesmiddelen, en de betere afstemming van bestaande geneesmiddelen op de noden van patiënten.

9.2 BEHOEFTEANALYSE

Bij aanvang van deze PoC werd een diepgaandere behoefteanalyse gedaan bij het Data4PHM-consortium. Het consortium was initieel op zoek naar een partner om een **dashboard** te bouwen, waarin data van de consortiumpartners samenkomt en dat door de population health managers gebruikt wordt om **specifieke zorg op maat van een regio** aan te bieden. Het dashboard geeft informatie over de prevalentie van diabetes type 2 in een bepaalde regio, gerichte screeningsmogelijkheden voor patiënten met een verhoogd risicoprofiel, zorgtrajecten, korte- en langetermijnopvolging, de effectiviteit van preventieve maatregelen, medicatiegebruik, complicaties, (medische) kosten, enzovoort. Dit dashboard is **gebruiksvriendelijk** voor de eindgebruikers. Dit zijn population health managers, zorgverleners en zorgraden. Deze eindgebruikers bezitten niet per se doorgedreven kennis in population health management of diabetes(indicatoren). Het dashboard is daarom **intuïtief** en **visueel aantrekkelijk**. In het dashboard zitten geavanceerde **analysetools, zoals predictie,** om de inzichten uit de diabetesgezondheidsdata om te zetten in praktische acties en benchmarking mogelijk te maken.

In dit dashboard moeten de **diabetesdata** van de verschillende partners worden **samengebracht**. Intego, IMA en FarmaFlux bezitten immers complementaire gegevens omtrent diabetes, die samen rijkere inzichten en zorg op maat van een regio kunnen sturen. Intego bezit gegevens over de Vlaamse prevalentie van diabetes, BMI, bloeddruk, rookgedrag, bloedsuikerspiegels, enzovoort. IMA bezit de diabetesgegevens van alle Belgische burgers omtrent onder meer de terugbetaalde zorg, demografische gegevens en socio-economische gegevens. Via hun gegevens kunnen analyses op regioniveau gemaakt worden. FarmaFlux bezit onder meer de afleveringsgegevens van terugbetaalde en niet-terugbetaalde medicatie en gegevens omtrent farmaceutische zorg voor diabetes. Voor de use case in dit project wordt enkel gewerkt met **geaggregeerde** gegevens.

Op het moment van de initiële gesprekken, werkte men aan de hand van individuele koppelingen om data te delen, voornamelijk tussen Intego en IMA. Om een geïntegreerd dashboard te kunnen bouwen, is er echter nood aan een efficiëntere **infrastructuur** voor data te kunnen delen. De data samenbrengen via een health data space, leek een ideale oplossing. De **decentrale** eigenschappen van een data space, de **standaardisatie-mogelijkheden**, het potentieel naar het verbeteren van **interoperabiliteit** en het werken met "**usage policies**" bieden het potentiële **vertrouwen** dat de sector mogelijks nodig heeft, aldus het consortium.

De volledige behoefteanalyse, exact zoals deze werd uitgevoerd en gecapteerd eind 2023, is terug te vinden in annex. Doorheen de maanden die daarop volgden werden bepaalde nuances verder scherp gesteld, of bijgestuurd op basis van voortschrijdend inzicht (zie ook bijlage 9.A).

9.3 FAIR DATA EN METADATA

Vooraleer men databronnen kan samenbrengen, is het zinvol te weten hoe FAIR die databronnen zijn, aangezien FAIRness (zie ook hoofdstuk 6.2.12 FAIR principles) de herbruikbaarheid sterk ondersteunt. Sommige van de voorgestelde richtlijnen uit de FAIR-data-principes zijn eenvoudig te implementeren en vormen zogenaamd "laaghangend fruit" dat met minimale inspanning kan worden gerealiseerd. Andere richtlijnen zijn daarentegen complexer en vereisen diepgaande kennis en expertise op het gebied van data-technologie. Daarom werd voor deze Data4PHM use case een FAIR assessment gemaakt aan de hand van de door imec ontwikkelde FAIR data scan voor gezondheidsdata[445]. Voor de toepassing van de FAIR principes werd één van de databronnen van het consortium aan de hand van haar metadata doorgelicht op de FAIR data principes. Op basis van deze evaluatie werden een aantal verbeterpunten genoteerd die het consortium konden helpen deze bron meer FAIR te maken. Het gaat onder andere over volgende suggesties:

1. **Vindbaarheid** van de metadata en de data verhogen door het toevoegen van:
   - De **naam** van een contactpersoon, de organisatie waartoe deze persoon behoort, een **persoonlijke identifier** (zoals bv. een ORCHID) en **contactgegevens**.
   - Informatie omtrent de context van de dataverzameling, zoals een **projectnaam**, eventuele **projectreferentienummer, financieringskanaal**, en de gevolgde **procedures** voor de dataverzameling.
   - Een **beschrijvende naam** van de dataset: op basis van de naam moet duidelijk zijn voor een buitenstaander welke data er in de dataset zit (dus niet: “dataset 01_01_2023”).
   - Een korte **samenvatting** van de data, vergezeld door een aantal relevante **sleutelwoorden**. Hierbij moeten de **semantische standaarden** zo goed mogelijk gevolgd worden.
   - Informatie over **waar** en binnen welke **tijdspanne** de data en metadata **vindbaar** zijn, en hoe (en wanneer) eventuele **updates** van de data gebeuren.
   - Een ***unique en persistent identifier*** voor de metadata en de data.
   - Als laatste kan de metadata in een **index** komen, waardoor de vindbaarheid van de metadata (en daardoor ook onrechtreeks de data) verhoogt.

2. **Toegankelijkheid** van de metadata en de data verhogen door het toevoegen van:
   - Een **omschrijving** van wie, **onder welke voorwaarden** en **hoe** men toegang kan verkrijgen tot de data, aangevuld met de **tijdspanne** waarbinnen de data en metadata toegankelijk zullen zijn.

3. **Interoperabiliteit** van de metadata en de data verhogen door:
   - Aanbieden van de data in **domeinspecifieke standaarden**. Dit gaat zowel over **semantische** standaarden (die naast de vindbaarheid ook de machineleesbaarheid en de algemene interoperabiliteit verhogen) als over standaarden voor **dataopslag**, **metadataopslag**, **datatransfer**, en **dataharmonisatie**.[446]
   - Gebruikmaken van linked data om vocabularia en documenten te linken, waardoor de machineleesbaarheid van de data en metadata significant verhoogt.

[445] *https://www.imec.be/nl/vlaamse-innovatiemotor/impactdomeinen/smart-health/fair-health-data*

[446] *Op dit moment zijn er nog geen finale beslissingen genomen rond de te hanteren standaarden in het gezondheidsdomein, al lijkt het wel richting compliance met FHIR en OMOP te evolueren.*

4. **Herbruikbaarheid** verbeteren door:
    - Zoveel mogelijk informatie toe te voegen. Dit laat potentiële (her)gebruikers van de data toe om te bepalen of de data effectief herbruikbaar zal zijn voor hun specifieke use case. Veel van deze extra informatie kan op het eerste gezicht overbodig lijken. Nochtans is het ontbreken ervan één van de belangrijkste redenen waarom gevonden data (die soms aan alle bovenstaande criteria voldoet), toch niet hergebruikt wordt. Voorbeelden van deze additionele informatie kunnen zijn:
        - Documenten en details rond **copyright, intellectuele eigendom** en hoe men **erkenning** wenst te krijgen voor de dataverzameling.
        - Gegevens en documentatie rond de **details van de dataverzameling**. Het gaat dan bijvoorbeeld over de gedetailleerde protocollen, gefaalde protocollen, technische fiches van gebruikte materialen en toestellen, hoe de data werd verwerkt, welke software en softwareversies er werd gebruikt, laboratoriumcondities, fouten die tijdens het proces werden gemaakt, etc.

Uit de gemaakte scan van de data en metadata blijkt dat er nog heel wat items aangepast kunnen worden om het FAIR-niveau van de gebruikte datasets in de use case te verhogen En alhoewel sommige van deze items complex en tijdrovend zijn, zijn heel wat andere suggesties slechts kleine ingrepen die met een minimum aan effort de latere herbruikbaarheid van de reeds beschikbare data exponentieel kan vergroten.
Voor deze analyse werd slechts één dataset geëvalueerd, die dient als voorbeeld voor andere.
Van de andere datasets was op dat moment geen (meta)data beschikbaar, maar de oefening is uiteraard ook nuttig voor de andere datasets in deze use case.

9.4 JURIDISCH KADER

De Data4PHM use case richt zich op het creëren van kennis door onderzoek te doen op bestaande geanonimiseerde gegevens. Dit kan worden gekwalificeerd als statistisch onderzoek in het algemeen belang. Het juridische kader dat van kracht is op de Data4PHM use case betreft voornamelijk gegevensbeschermings-wetgeving, samen met de veelheid aan gegevensdelingsinstrumenten die door de Europese Unie werden uitgevaardigd afgelopen jaren. Deze worden allen besproken in hoofdstuk 6 Juridische en ethische principes, waarbij de belangrijkste bepalingen in de Datagovernanceverordening (DGA) zijn opgenomen, aangezien de Health Data Space zal kwalificeren als een databemiddelingsdienst. Zij dient zich daarom te registreren overeenkomstig artikel 11 van de DGA via het hiervoor voorziene formulier bij de FOD Economie (zie 6.2.5.2 Relevante definities), en te voldoen aan de vereisten opgenomen in artikel 12 van de DGA.

De Data4PHM use case op zich triggert nog niet de definitie van een volwaardige health data space zoals bedoeld onder de EHDS-verordening. Een herziening van dit juridische kader is noodzakelijk wanneer er een uitbreiding plaatsvindt van het secundaire gegevensgebruik dat wordt voorzien in de Data4PHM use case, naar een volwaardige Health Data Space waarbij ook primair gebruik wordt ondersteund. Er zijn uiteraard wel tal van interessante aspecten waarmee best al rekening wordt gehouden met het opzetten van deze specifieke use case met het oog op een volwaardige uitbreiding. Zo zal de structuur van de Health Data Space zelf wellicht overeenkomen met de figuur van een Health Data Access Body (HDAB), met alle nodige taken en verantwoordelijkheden van dien. Hoewel dat op dit moment dus nog niet van tel is, zal bij de concrete oprichting van de Health Data Space wel gelet moeten worden op dergelijke aspecten.

Voor wat betreft het creëren van een volwaardige Health Data Space zal, gezien de verdeling in bevoegdheden, een samenwerking tussen het Vlaamse niveau en het federale echelon vereist zijn.
Wat betreft het secundair gebruik van gegevens in de Data4PHM use case, lijkt dit een bevoegdheid voor de Vlaamse Gemeenschap, aangezien deze bevoegd is voor bijvoorbeeld preventieve gezondheidszorg.[447]

[447] *Artikel 5, §1, I, eerste lid, BWHI.*

9.5 GOVERNANCE STRUCTUUR EN FRAMEWORK (DATA4PHM USE CASE)

De Data4PHM use case werd ook onderworpen aan het onderzoek rond governance dat werd gevoerd in dit health data space project. De (voorlopig) eerder gelimiteerde scope van de use case beperkt echter sterk de nood voor het opzetten van een uitgebreide governance structuur en framework. Hieronder wordt beschreven hoe de huidige governance structuur en framework er uitziet, op het moment van dit schrijven.

Wanneer de health data space uitbreidt met partners buiten dit bestaande consortium, zal de governancestructuur uiteraard wijzigen en complexer worden, zoals besproken in hoofdstuk 7.3 Governance structuur van een health data space.

9.5.1 Governance structuur (Data4PHM use case)

De use case kadert in een bestaande samenwerking tussen Intego, IMA en FarmaFlux. Deze samenwerking kadert niet binnen een bepaalde wettelijke of organisatorische entiteit, en is dus niet gekoppeld aan specifieke rapporteringsverplichtingen of formele structuren. Alle strategische en operationele beslissingen worden **in onderling overleg** met de verschillende partners besproken. Dit is de grote kracht van dit consortium en is, gezien de kleine schaal, operationeel goed werkbaar.

9.5.2 Governance framework (Data4PHM use case)

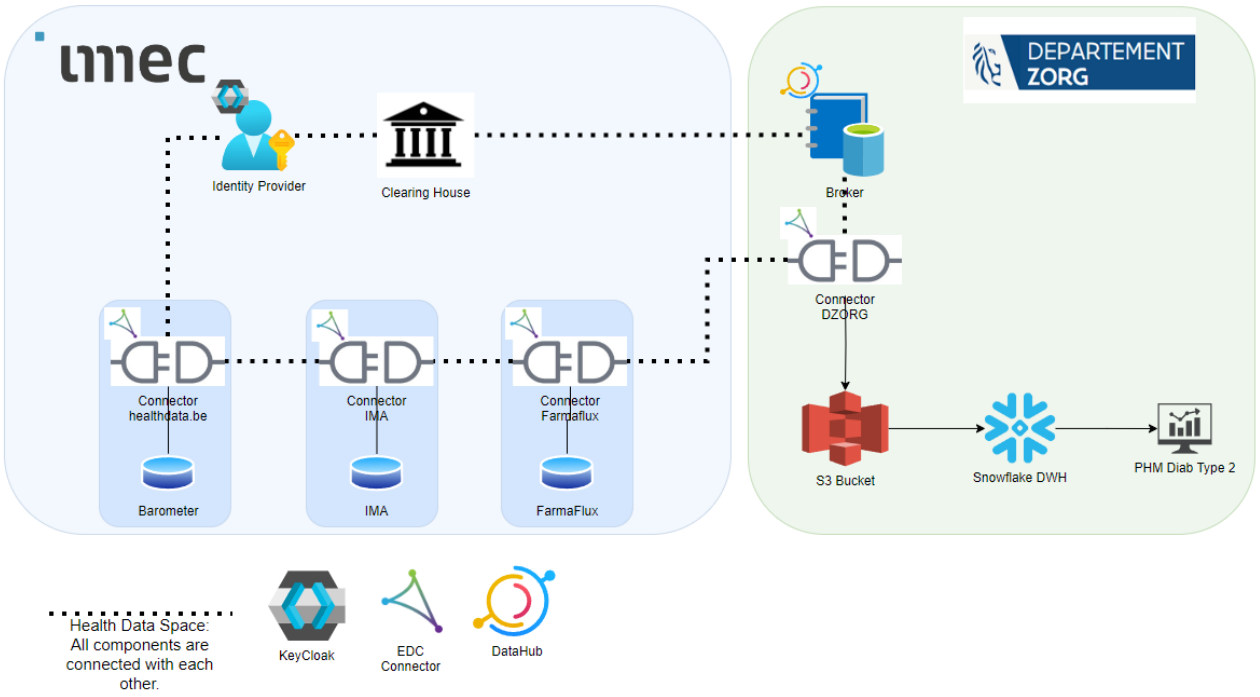
Het project loopt via individuele **samenwerkingsovereenkomsten** of engagementsverklaringen die de partners bij toetreding ondertekenen. Bij onderlinge gegevensuitwisseling worden de nodige **juridische documenten** opgesteld (bijvoorbeeld verwerkersovereenkomsten), maar verder zijn er **geen bijkomende algemene regels** opgesteld die de interne werking vormgeven. Men werkt **op basis van vertrouwen**, wat ook inhoudt dat elke partner de vrijheid heeft om individuele beslissingen te nemen en op ieder moment uit het consortium of de use case kan stappen.

Bovenstaande manier van werken heeft uiteraard als groot voordeel dat men erg **wendbaar** is, en zich steeds snel kan aanpassen aan de omstandigheden. Het nadeel is dat alle samenwerkingen erg vrijblijvend zijn, en dat er aan het zich niet houden aan (onderlinge) afspraken weinig directe consequenties verbonden zijn, tenzij dan het breken van het opgebouwde vertrouwen met de andere partners. Het mag duidelijk zijn dat waar deze vorm van samenwerking zich leent tot het uitvoeren van een kleinschalige use case met een beperkt aantal partners zonder al te complexe samenwerkingsverbanden of data-uitwisselingsprotocollen, dit voor een grotere data space met meerdere actoren en complexe datatransacties niet meer het geval zal zijn. Naarmate de data space zelf meer geformaliseerd wordt, zal dit ook voor de governance structuur en het bijhorende framework het geval moeten zijn.

9.6 ARCHITECTURALE SET-UP

9.6.1 Infrastructuur

Gebaseerd op het conceptueel model van een health data space (zie sectie 8.2 Conceptuele architectuur) is een architectuur uitgewerkt en geïmplementeerd om een concrete datadeling te verwezenlijken gebruik makend van de data space principes.



Figuur 37: Architectuur voor Data4PHM use case.

Connectoren

Gedurende de looptijd van het project is getracht om connectoren te installeren bij de verschillende partners die de rol van data holder opnemen. Het was de bedoeling om halfweg dit project de nodige connectoren geïnstalleerd en geconfigureerd te krijgen. Het nog immature karakter van de connectoren en de nodige effort om de connectoren te installeren was voor partners op dat moment nog een te hoge drempel om over te gaan tot een effectieve installatie. Daarom is gekozen om de verschillende partners te **simuleren** op de infrastructuur van imec. In bovenstaande figuur zijn daarom drie silo's te zien die elk een connector en een dataset bevatten, telkens voor één van de drie partners.

Als data user is ook bij Departement Zorg een connector geïnstalleerd en geconfigureerd zodat de data vanuit de infrastructuur van imec gedeeld kan worden met de infrastructuur van de afdeling Beleidsinformatie en Data van Departement Zorg. Een extra eigen ontwikkelde toevoeging in de vorm van microservices[448] op data plane niveau bij zowel imec en Departement Zorg was nodig om de effectieve datadeling te verwezenlijken.

Broker

De broker (federated catalog + DataHub) werd initieel geïnstalleerd op de infrastructuur van imec, maar werd gedurende de loop van het project verhuisd naar de infrastuctuur van het Departement Zorg.

[448] *Microservices zijn een architectuurstijl waarbij een applicatie wordt opgedeeld in kleine, onafhankelijke diensten die afzonderlijk ontwikkeld, ingezet en geschaald kunnen worden en met elkaar communiceren via goed gedefinieerde API's.*

Identity provider
De identity provider is opgezet op de infrastructuur van imec. Hiervoor is zoals vermeld in de beschrijving van de architectuur de tool Keycloak gebruikt.

Clearing house
Het clearing house, dat zoals beschreven in het architectuur hoofdstuk een volledig eigen gebouwde applicatie is, werkt vanop de infrastructuur van imec.

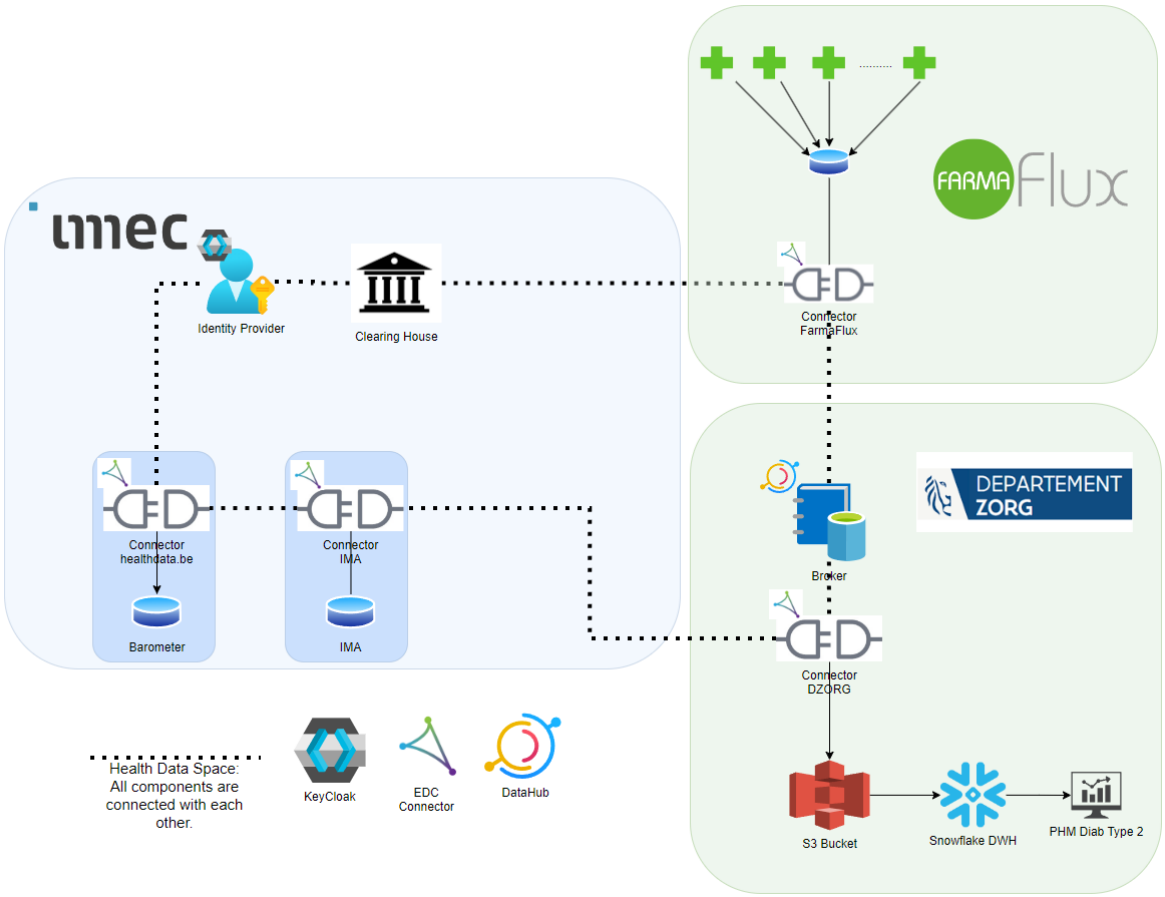
Alle componenten zijn succesvol geïnstalleerd en geconfigureerd. Het technische onderzoeksteam is er daarbij ook in geslaagd om een succesvolle datadeling te doen tussentwee verschillende (fysieke) infrastructuren, volgens het principe van een health data space, waarbij Departement Zorg als data user de drie datasets bij de gesimuleerde data holder is kunnen gaan ophalen en ontvangen op hun dataopslagomgeving (AWS S3 Bucket[449]). De ontvangen data worden vervolgens verwerkt (gecombineerd en geprepareerd) in het data warehouse van de afdeling Beleidsinformatie en Data van het Departement Zorg (Snowflake[450]) om vervolgens te visualiseren in een dashboard.

9.6.2 FarmaFlux connector

Aan het einde van dit onderzoeksproject is het installatieproces van de FarmaFlux-connector opgestart als extra leerervaring voor het installeren van een connector. De connector werd net als bij imec geïnstalleerd op een Kubernetes-cluster. Hoewel de installatie succesvol is afgerond, is er geen volledige end-to-end test uitgevoerd wegens het einde van het project. Wat wel getest werd, is het transfereren van bestaande, op het internet publiek beschikbare documenten van de FarmaFlux- naar een imec-connector.
Onderstaande figuur geeft de situatie weer indien een volledige onboarding bij FarmaFlux afgerond was. In een mogelijks vervolgtraject kan dit een eerste volgende stap zijn in verdere uitwerking van de Data4PHM use case.
De figuur geeft ook weer dat FarmaFlux de rol van data intermediary kan opnemen voor alle apotheken. In een latere fase zou er, naast het dashboard, ook via de FarmaFlux connector feedback (data) kunnen bezorgd worden aan de apothekers.

[449] *https://aws.amazon.com/s3/*

[450] *https://www.snowflake.com/en/emea/*



Figuur 38: Architectuur voor Data4PHM use case met FarmaFlux connector.

9.6.3 Datastandaarden

Het IDSA-regelboek biedt gedetailleerde instructies over de verplichte en optionele criteria voor data spaces, waarbij vocabularia en semantische modellen worden benadrukt als belangrijke elementen van het core framework.

In de context van de health data space worden de volgende domeinspecifieke datamodellen geanalyseerd om de interoperabiliteit van data binnen de gezondheidszorgsector te verbeteren.

Samenvatting en slotopmerkingen over OMOP
Het Observational Medical Outcomes Partnership (OMOP) datamodel is een gestandaardiseerd, versiegestuurd raamwerk dat is ontworpen om de analyse van gezondheidsgegevens voor observationeel onderzoek te ondersteunen.

Als onderdeel van dit onderzoeksproject werd een experiment uitgevoerd om een van de datasets uit de Data4PHM use case in kaart te brengen volgens het OMOP CDM-model, waarbij een casestudy werd gebruikt om de effectiviteit te beoordelen. De conclusie is dat, hoewel het OMOP CDM mogelijk niet de meest geschikte oplossing is voor de zeer specifieke use case van Data4PHM, waar de focus ligt op statistisch geaggregeerde data in plaats van persoonsgerichte informatie, het significant potentieel heeft als de VHDS in de toekomst van plan is persoons-/patiëntgerichte gegevens op te nemen. In dat geval zou het OMOP CDM kunnen dienen als een ideaal raamwerk voor het beheer van grootschalige elektronische medische dossiers. Meer gedetailleerde informatie is te vinden in bijlage 9.B.

Samenvatting en slotopmerkingen over FHIR
FHIR (Fast Healthcare Interoperability Resources) is een standaard ontwikkeld door HL7 voor de elektronische uitwisseling van gezondheidsinformatie. Het biedt een set "resources", of data-elementen, die verschillende aspecten van gezondheidsgegevens vertegenwoordigen, zoals patiënten, medicijnen en observaties.

Als onderdeel van dit onderzoeksproject werd een experiment uitgevoerd om een van de datasets uit de Data4PHM use case in kaart te brengen volgens de FHIR-standaard, waarbij een casestudy werd gebruikt om de effectiviteit te beoordelen door een FHIR-profiel voor een Vlaamse Health Data Space te implementeren. De conclusie is dat het ontwikkelen van een FHIR-implementatiegids een haalbare strategie is voor het vaststellen van data governance binnen een Vlaamse Health Data Space. Er worden echter aanzienlijke uitdagingen erkend, aangezien het maken van een nieuwe implementatiegids een complex proces is dat meerdere jaren in beslag kan nemen. Deze verlengde tijdlijn is te wijten aan de complexe aard van het FHIR-ecosysteem en de noodzaak om meerdere belanghebbenden op één lijn te brengen voor het succesvolle ontwikkelen van de gids. Meer gedetailleerde informatie is te vinden in bijlage 9.C.

Conclusie
De studie benadrukt dat er momenteel **geen one-size-fits-all datamodel** is dat geschikt is voor alle gezondheidscontexten binnen de Health Data Space en dat een oplossing hiervoor gerust een op zich staand project zou kunnen zijn. De noodzaak voor op maat gemaakte ontwikkeling en aanpassing is duidelijk, vooral bij het aanpakken van diverse belanghebbenden en uiteenlopende internationale vereisten. Ondanks deze uitdagingen worden er vorderingen gemaakt door middel van samenwerkingsverbanden tussen tal van organisaties en projecten die zich richten op het verbeteren van de interoperabiliteit, zoals EEHRxF, RWD4BE en FHIR-gemeenschappen.

9.7 EINDPRODUCT: DASHBOARD

Het uiteindelijke doel van de Data4PHM use case is om tot een geïntegreerd dashboard te komen waarbij verschillende databronnen met elkaar gecombineerd worden en verschillende actoren in het zorglandschap die te maken hebben met diabetes type 2 de nodige antwoorden kunnen vinden voor het ondersteunen en optimaliseren van hun werkzaamheden.
Het gaat om een Proof-of-Concept dashboard dat niet in productie is geplaatst tijdens de looptijd van dit project. Na positieve evaluatie van de proefgebruikers (Zorgzaam Leuven) kan een vervolgproject worden opgestart om de databronnen uit te breiden (bvb. met meer historische data) en het dashboard naar een breder zorgpubliek te brengen. We verwijzen hierbij naar de PROSPeCD studie in opdracht van FOD Health en EU (TSI funding)), waarin waardevolle bevinden zijn geformuleerd inzake het opstellen van een geïntegreerd en uitvoerbaar (actionable) dashboard.

In overleg met het Data4PHM onderzoeksteam is een eerste ontwerp van het dashboard besproken om een antwoord te bieden aan 7 onderzoeksvragen. De 7 **onderzoeksvragen** zijn geselecteerd uit een lijst van 42 en zijn geselecteerd op een manier waarbij de verschillende databronnen aangesproken worden.

1. Hoeveel % van de populatie is gediagnostiseerd met type 2 diabetes (T2D) ouder dan 40 jaar?
   - Gegevensbronnen: Intego, FarmaFlux, IMA
2. Hoeveel % van de T2D patiënten hebben deelgenomen aan een diabetes zorgtraject: voortraject, zorgtraject, diabetes conventie?
   - Gegevensbronnen: IMA
3. Hoeveel % van de T2D patiënten laten jaarlijks een HbA1c meeting doen?
   - Gegevensbronnen: Intego, IMA

4. Hoeveel % van de T2D patiënten laten jaarlijks een griepvaccinatie zetten?
   - Gegevensbronnen: Intego, FarmaFlux, IMA
5. Hoeveel % van de T2D patiënten tussen 55 en 80 zijn behandeld met statinen?
   - Gegevensbronnen: FarmaFlux, IMA
6. Hoeveel % van de T2D patiënten laten jaarlijks LDL meeting doen?
   - Gegevensbronnen: Intego, IMA
7. Wat is de totale jaarlijkse gezondheidskost van diabetespatiënten?
   - Gegevensbronnen: IMA

9.7.1 Databronnen

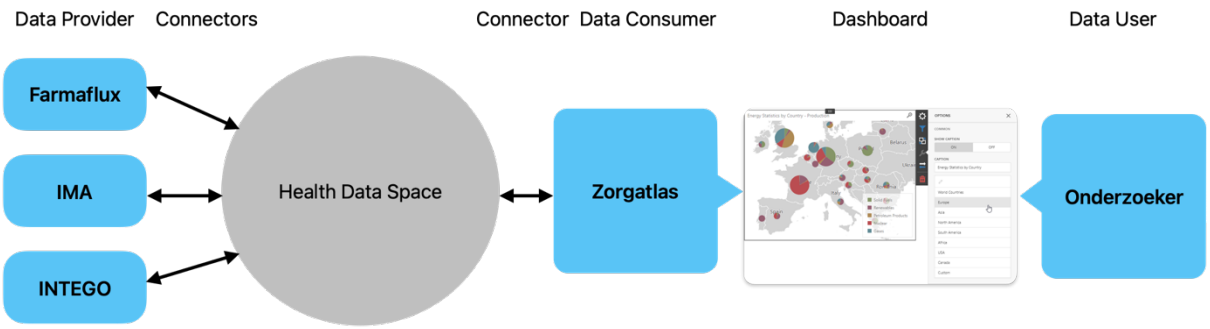
De drie verschillende databronnen zijn geaggregeerd tot op gemeenteniveau (post- of NIS-code).
De gemeente is gebruikt om de drie databronnen met elkaar te linken.

BRON	OMSCHRIJVING	CONCLUSIE
Intego	Diabetes barometer Geaggregeerde praktijkdata vanuit huisartsenpakket. Bevat teller- en noemergegevens die volgende info kunnen weergeven: • Prevalentie diabetes • Patiënten die binnen x tijd een bloedwaarde test gehad hebben. (5 verschillende waarden van belang) • BMI, bloeddruk, rookgedrag, HbA i c waarden, prevalentie diabetes Data eigenaars: INTEGO consortium Technische partij: healthdata.be Tijdsperiode: 2023	Legale basis: Het Data4PHM-consortium heeft al een data sharing agreement waarin Departement Zorg werd opgenomen als dashboardbouwer (cf. compliance).
FarmaFlux	Geaggregeerde data op apotheekniveau • Prevalentie diabetes • Aflevering van statines • Aflevering van griep vaccines Technische partij: Farmaflux Tijdsperiode: Ongekend	Legale basis: Geen. De huidige ontvangen dataset bevat pseudodata en is geen extractie van productie of afgeleide van productie gelijkende data.
IMA	Geaggregeerde data op regioniveau • Prevalentie diabetes obv terugbetaalde zorg Technische partij: IMA Tijdsperiode: 2022	Legale basis: Data wordt al gebruikt voor een IMA-atlas. Dit gaat over publieke data.

<u>Aandachtspunt: verschillende tijdsperiodes</u>
De databronnen Intego en IMA beslaan niet dezelfde tijdsperiode. De huidige FarmaFlux dataset heeft geen tijdsindicatie (test data). In de visualisaties zal daarom bij elke databron duidelijk gemaakt worden over welke tijdsperiode het gaat zodat correcte vergelijkingen en conclusies getrokken kunnen worden.

9.7.2 Projectarchitectuur

Een beknopt architecturaal overzicht van de dataflow achter het dashboard.



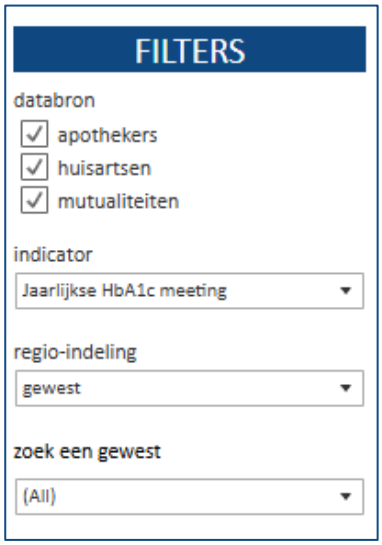
Figuur 39: Projectarchitectuur Data4PHM Dashboard.

De individuele brondata staat bij de drie dataproviders. Via de VHDS kan vanuit de ZorgAtlas een aanvraag gelanceerd worden om de brondata te bevragen en het geaggregeerd resultaat de delen met de Zorgatlas via de VHDS.

Het dashboard zal enkel beschikbaar gemaakt worden aan de zorgverleners en onderzoekers van **Zorgzaam Leuven** en zal enkel gebruikt worden om te bepalen of het dashboard de verwachte inzichten kan verschaffen. Op geen enkel moment zal het dashboard publiek toegankelijk gemaakt worden. Er is geen row-level-security ingesteld.
De aangeleverde data is reeds geaggregeerd tot op woonplaatsniveau (NIS-code). Cellen met minder dan 10 eenheden zijn ofwel niet meegestuurd of zullen niet getoond worden in het dashboard.

9.7.3 Visualisaties

De 7 onderzoeksvragen kunnen ingedeeld worden in **vier dashboards**. In elke dashboard kan gekozen worden welke dataset(s) gebruikt moet(en) worden. Standaard zijn alle mogelijk datasets geselecteerd. Indien een dataset niet beschikbaar is voor een bepaald dashboard of indicator, dan wordt deze selectie gedeactiveerd (in het grijs gezet) of niet getoond.



Alle dashboards, behalve deze i.v.m. de gemiddelde kost, zijn geografisch en zijn voorzien van een kaart van Vlaanderen.

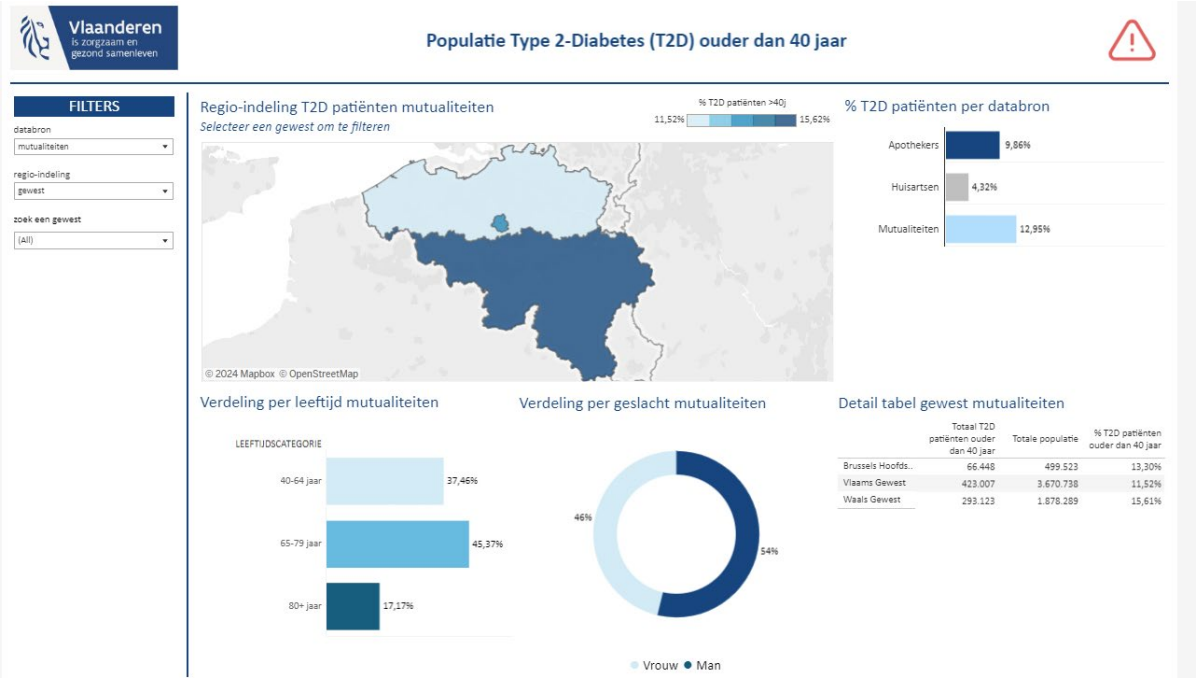
Er is telkens één visualisatie op het dashboard voorzien die de verschillen tussen de verschillende datasets toont. Dit help de gebruiker om snel te zien of er significante verschillen zijn tussen de verschillende datasets en om zo te bepalen of een diepere analyse van één bepaalde databron nodig is.

De filter is bij elk dashboard gelijkaardig. Er is de keuze van databron, de keuze voor regio-indeling (gewest, provincie, eerstelijnszone en gemeente). Het dashboard omtrent de indicatoren (dashboard 3 in de volgende lijst) is een extra keuze lijst waar de gewenste diabetes indicator kan geselecteerd worden.

9.7.3.1 *Dashboard 1: Prevalentie*

Onderzoeksvraag:

- Hoeveel % van de populatie is gediagnostiseerd met type 2 diabetes (T2D) ouder dan 40 jaar?

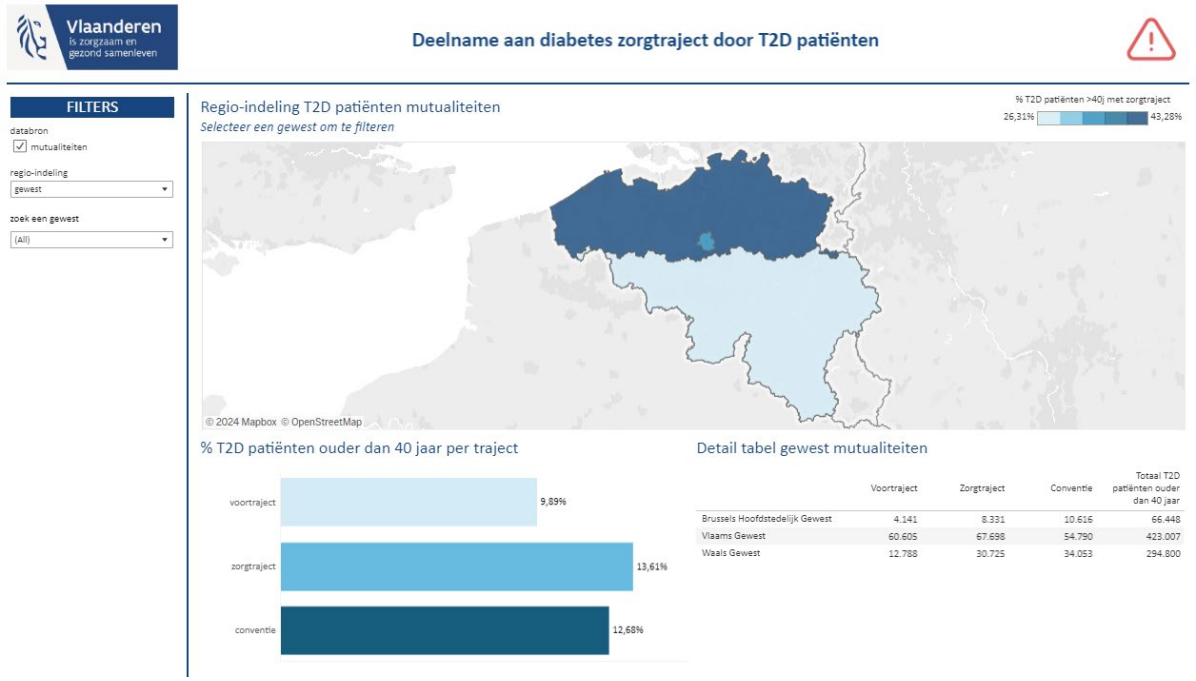


Figuur 40: Data4PHM Dashboard 1 - Prevalentie.

9.7.3.2 *Dashboard 2: Zorgtraject*

Onderzoeksvraag:

- Hoeveel % van de T2D patiënten hebben deelgenomen aan een diabetes zorgtraject: voortraject, zorgtraject, diabetes conventie?

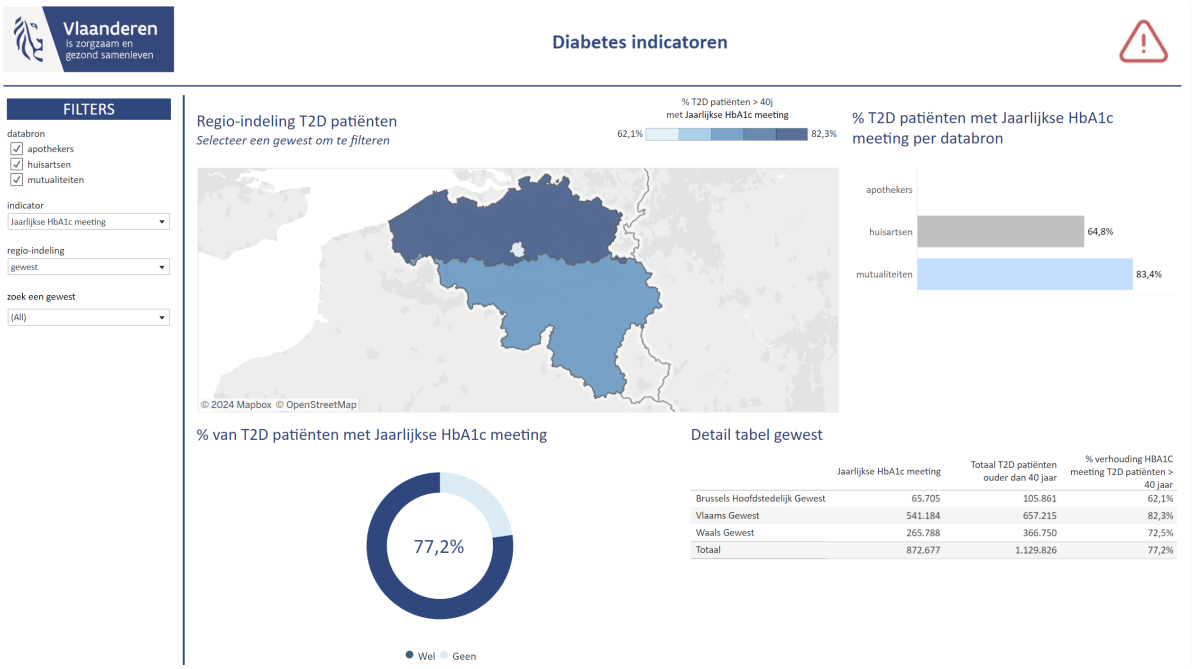


Figuur 41: Data4PHM Dashboard 2 - Zorgtraject.

9.7.3.3 *Dashboard 3: Diabetesindicatoren*

Onderzoeksvragen:

- Hoeveel % van de T2D patiënten laten jaarlijks een HbA1c meeting doen?
- Hoeveel % van de T2D patiënten laten jaarlijks een griepvaccinatie zetten?
- Hoeveel % van de T2D patiënten zijn behandeld met statinen?
- Hoeveel % van de T2D patiënten laten jaarlijks een LDL-meeting doen?

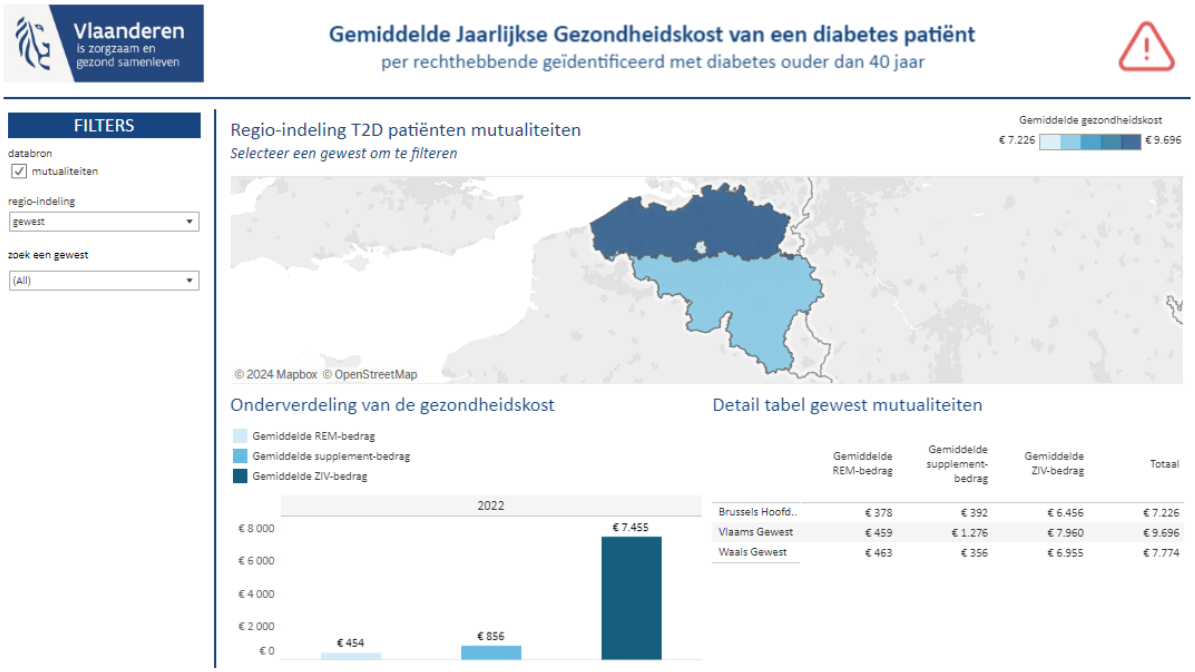


Figuur 42: Data4PHM Dashboard 3 - Diabetesindicatoren.

9.7.3.4 *Dashboard 4: Gezondheidskosten*

Onderzoeksvraag:

- Wat is de totale jaarlijkse gezondheidskost van diabetespatiënten?



Figuur 43: Data4PHM Dashboard 4 - Gezondheidskosten.

10 GO-TO-MARKETSTRATEGIE - ROADMAP - ACTIEPLAN

10.1 STRATEGIE

In dit hoofdstuk worden de algemene vervolgstappen beschreven voor een vervolgproject.
Dit vervolgproject kan verschillende vormen aannemen. Het kan gericht zijn op verder onderzoek naar meer concrete onderwerpen die verduidelijkt moeten worden om de implementatie van een health data space succesvol te laten verlopen. Indien mogelijk, kan het ook een concreter implementatieproject zijn, waarin een governance-structuur wordt opgezet voor de data space en business use cases op technisch niveau worden uitgewerkt en in productie worden genomen. De vervolgstappen zijn onderverdeeld in een go-to-marketstrategie, een roadmap en een actieplan.

In de go-to-marketstrategie gaan we dieper in op het creëren van een data space en de actoren die hierbij betrokken zijn. Verder bekijken we de datamarkt waarop de health data space impact zal hebben, en hoe de data space zich het beste kan positioneren om zo waardevol mogelijk te zijn binnen het gezondheids-landschap van België en Vlaanderen.

In de roadmap werken we een praktisch plan uit met als doel het implementeren van een health data space in productie. Dit plan is opgedeeld in mijlpalen die in een bepaalde volgorde behaald moeten worden om de praktische implementatie van de health data space tot een succes te maken.

Tot slot is er het actieplan. Dit plan bevat een overzicht van de stappen die al zijn genomen zijn of nog genomen kunnen worden om dichter bij de uitvoering van de roadmap te komen. Dit kan variëren van het uitwerken van use cases waarvoor een vervolgfase is ingepland tot het aanvragen van nieuwe projecten om de implementatie van de health data space verder te bevorderen.

10.2 GO-TO-MARKETSTRATEGIE

10.2.1 Indeling

De go-to-marketstrategie raakt aan veel verschillende aspecten van het onderzoek. Dit betekent dat we veel informatie kunnen gebruiken uit andere onderdelen van het onderzoek. Het is een strategie die de kans op succes van de health data space moet vergroten. Het implementeren van een health data space in Vlaanderen is niet eenvoudig. Er zijn veel obstakels te overwinnen om de implementatie succesvol af te ronden. Wat belangrijk is om te benadrukken, is dat dit geen actieplan, implementatieplan of roadmap is. Het doel van dit hoofdstuk is om een beter begrip te krijgen van de verschillende uitdagingen die spelen bij het lanceren van een Vlaamse health data space.

10.2.2 Oprichting, onboarding van early adopters en opschaling

Eerst en vooral moet er een duidelijk verschil gemaakt worden tussen de oprichting van de health data space met bijhorende bestuursorganen, het onboarden van de early adopters en het opschalen van de data space na verloop van tijd.

10.2.2.1 Oprichting

Wat verstaan we onder oprichting? Tijdens het onderzoek is het duidelijk geworden dat het oprichten van de health data space op verschillende manieren kan gebeuren. Er zullen eerst beslissingen op het niveau van governance moeten worden genomen om te bepalen wat het vertrekpunt is van waaruit de data space zal worden opgericht. Dit kan bijvoorbeeld binnen een departement of agentschap van de Vlaamse overheid zijn, of een volledig nieuwe organisatie die al dan niet met ondersteuning van de overheid wordt opgebouwd. In ieder geval moet er een groep governance bodies en implementatiepartners worden

aangesteld om de health data space op te richten, uit te rollen en te onderhouden. Op dat moment is er nog niet onmiddellijk sprake van het uitvoeren van use cases. Er is een kans dat de organisaties die deelnemen aan de oprichting ook meteen één van de eerste early adopters zullen worden, maar dit is geen vereiste. Het is ook mogelijk dat een organisatie deel uitmaakt van de oprichting en de uiteindelijke health data space zonder ooit zelf data te delen of te ontvangen via de data space.

10.2.2.2 Onboarding van early adopters

Zodra de health data space is opgericht, is het mogelijk om toegang te verlenen aan de eerste organisaties. Deze early adopters zijn organisaties die willen bijdragen aan de groei van de data space. Ze hebben als missie om health data op een efficiënte, veilige en innovatieve manier te delen met hun partners. Het gaat niet alleen om de organisatie zelf, maar ook om de use case die in productie wordt genomen binnen de data space, en die uniek is voor het early adopter-principe. Deze use case heeft verschillende eigenschappen:

> Er is positieve impact voor de bevolking in Vlaanderen.
> Er is onmiddellijke impact op de kost voor de gezondheidszorg.
> Het is een use case die volledig end-to-end kan worden uitgewerkt, met als doel de data space interessanter en waardevoller te maken voor andere dataproviders en consumenten binnen het landschap.

De ervaring van deze early adopter-organisaties en de eerste use cases is ook zeer belangrijk. Indien er problemen, opmerkingen of nieuwe verwachtingen opkomen, kan de health data space organisatie deze eerst oplossen om zo een stevige basis te creëren die de groei van de health data space in de toekomst ten goede komt. Daarnaast fungeren deze organisaties en use cases als uithangborden en referenties naar de buitenwereld. Hun doel is om zekerheid en vertrouwen te bieden aan toekomstige organisaties en use cases.

10.2.2.3 Opschaling

Zodra de health data space een solide basis van deelnemende organisaties en actieve use cases heeft, kan er gekeken worden naar opschaling. Opschaling kan op verschillende manieren plaatsvinden.
Enkele voorbeelden:

> Er kunnen organisaties uit andere sectoren worden toegelaten tot de data space om de combinatie van verschillende datasets te verbreden. Dit kan de innovatieve mogelijkheden op het gebied van data-onderzoek vergroten.
> De geografische scope van de data space kan worden uitgebreid naar bijvoorbeeld heel België of de Benelux, om het delen van data binnen een groter gezondheidsgebied te uniformeren.
> Nieuwe services kunnen worden aangeboden aan de deelnemende organisaties binnen de data space. Deze services kunnen bijvoorbeeld een meer op maat gemaakte ervaring bieden voor organisaties bij het delen of ophalen van data. Bijvoorbeeld: analyse services, pseudonomisatie …

De uitbreidingen die bij opschaling komen kijken, verschillen sterk van het creëren van een basis data space en kunnen daarom worden gezien als een volledig nieuwe fase. Elke vernieuwing in dit stadium brengt unieke uitdagingen en problemen met zich mee. Het is daarom cruciaal dat bij het invoeren van deze vernieuwingen zowel de zakelijke, bestuurlijke als technische aspecten zorgvuldig worden beoordeeld op hun impact en risico's. Zo kunnen we kernwaarden zoals vertrouwen en veiligheid behouden gedurende het verdere groeiproces van de data space.

10.2.3 Het doelpubliek

Het doelpubliek waarmee we willen connecteren, hangt af van het perspectief dat we aannemen.
Er zijn drie perspectieven:

- De oprichters van de data space: dit zijn organisaties die de data space mee beheren en onderhouden.
- De early adopters: dit zijn de eerste organisaties die gebruik zullen maken van de data space als tool om data uit te wisselen.
- Alle andere organisaties: eens de fundamenten van de data space er zijn, kunnen andere organisaties toetreden. Ook organisaties die in eerste instantie niet in aanmerking komen tot de data space kunnen er nu gebruik van maken.

doelpubliek van een data space is zeer dynamisch. Het kan duidelijk afgebakend zijn, bv. in de automobiel-industrie, maar het kan ook zeer breed gaan. Theoretisch gezien kan "iedereen" deel uitmaken van de Vlaamse health data space. Praktisch gezien zal dit zich aanvankelijk eerder beperken tot organisaties binnen het Vlaamse en Belgische zorg- en welzijnslandschap, meer specifiek tot organisaties die voldoen aan bepaalde technische en governance-gerelateerde vereisten. Daarnaast moet er ook een use case zijn voor de toetredende organisaties. Natuurlijk is dit slechts het begin. Op termijn zal de scope van het doelpubliek groeien: enerzijds naar andere sectoren binnen Vlaanderen en België, en anderzijds, met de European Health Data Space (EHDS) in gedachte, naar de mogelijkheid om op Europees niveau toegang te bieden tot de health data space.

10.2.4 Profiel van de ideale organisatie

Om duidelijk te maken welk soort organisaties in aanmerking kunnen komen voor deelname aan de health data space, hebben we een persona tabel gemaakt. Deze tabel bevat het “ideale” type organisatie voor één van de drie specifieke momenten. De oprichting, de early adopters en de opschaling van de health data space.

	OPRICHTING	EARLY ADOPTERS	OPSCHALING
Doel/missie	Deel uitmaken van een netwerk dat ondersteuning biedt aan het delen van health data op een veilige en efficiënte manier.	Zorg en welzijn voor elke burger staan centraal, met data als hulpmiddel om beleid, innovatie en onderzoek te bevorderen en zo dit doel te bereiken.	Hoewel zorg en welzijn niet direct centraal staan, is het delen van data met zorgactoren wel een belangrijk doel om beleid, innovatie, productie en onderzoek te stimuleren.
Grootte en structuur	De organisatie is op technisch vlak voldoende matuur om een fundamentele bijdrage te leveren aan de oprichting van de data space. Dit kan bijvoorbeeld in de vorm van een trusted third party of als technische implementatiepartner …	De organisatie is technisch voldoende matuur om zowel data te delen met andere organisaties als data op te vragen. Dit kan in de rol van data consumer, data provider of een combinatie van beide.	De organisatie is technisch voldoende ontwikkeld om zowel data te delen met andere organisaties als data op te vragen. Dit kan in de rol van data consumer, data provider of een combinatie van beide. Als dit niet het geval is kan de organisatie nog steeds beroep doen op een data intermediary.

Cultuur	De cultuur van de organisatie richt zich op innovatie en toont de nodige integriteit bij het nakomen van verplichtingen met betrekking tot nieuwe initiatieven.	De organisatiecultuur richt zich op het maken van doordachte beleidskeuzes, met een sterke focus op innovatie.	De cultuur van de organisatie streeft naar het verbreden van de organisatiescope door middel van toevoeging van nieuwe data.
Diensten en onderzoek	De organisatie moet minstens één van de volgende taken kunnen opnemen: - Trusted third party. - Technische implementatiepartner. - Data catalogus. - Controle-entiteit op legaal niveau.	De organisatie moet zich minstens bezighouden met één van de volgende activiteiten: - De organisatie levert diensten binnen de gezondheidszorg en welzijn. Bv. ziekenhuis, zorgverzekeraars, koepelorganisaties in de zorg, labo's … - De organisatie focust op onderzoek omtrent zorg en welzijn. Bv. universiteiten, onderzoeksinstellingen … - Medische industrie. - Overheidsinstantie met als werkveld gezondheidszorg en welzijn.	De organisatie levert diensten en/of onderzoek waar data in het proces van toepassing is
Geografische scope	De organisatie is actief in Vlaanderen en wordt ook bestuurd vanuit Vlaanderen.	De organisatie is actief in Vlaanderen en/of België.	De organisatie is actief binnen Europa.
Business model	Non-profit	Non-profit / For-profit	Non-profit / For-profit

10.2.5 Vertrouwen tussen de data space en de deelnemende organisaties

Natuurlijk gaat het niet alleen om de ideale organisatie binnen de data space, maar ook om de relatie tussen de Founding fathers en de betrokken organisatie. Het doel is niet om van de Vlaamse health data space een "vriendenclub" te maken, maar om een sterk wederzijds vertrouwen op te bouwen tussen beide partijen. Er moet een gezamenlijke visie zijn over de toekomst en de meerwaarde van de data space. Alle organisaties die vanaf het begin betrokken zijn bij de Vlaamse health data space, worden niet alleen gezien als pioniers op het gebied van efficiënt en veilig delen van health data, maar fungeren ook als voorbeeld. Andere organisaties kunnen naar hen kijken en zich baseren op hun ervaringen om meer informatie te krijgen over de health data space: wat hun bevindingen zijn en hoe de data space hen op de beste manier kan ondersteunen. Daarom is het belangrijk dat we, vooral in het begin, organisaties hebben die aan het gezondheidszorg- en welzijnsecosysteem in de praktijk kunnen tonen wat de meerwaarde van de health data space is.

10.2.6 Waardepropositie van de data space

Het is niet eenvoudig om de echte waardepropositie van de health data space te definiëren zolang deze nog niet actief is. Wat we wel hebben gedaan, is een groeipad beschreven dat de data space kan volgen om de waardepropositie te ontwikkelen. We maken hierbij gebruik van een strategie genaamd "het netwerkeffect." Deze strategie houdt in dat hoe meer organisaties gebruikmaken van de health data space, hoe waardevoller deze wordt voor het bredere ecosysteem.

Als we dit in de praktijk gaan bekijken, ziet het er ongeveer als volgt uit. We beginnen met één use case. Deze use case volgt de eigenschappen zoals beschreven in hoofdstuk 10.2.2.2 Onboarding van early adopters. Zodra deze use case succesvol is uitgevoerd, kunnen de deelnemende organisaties binnen deze use case als referentie dienen, zowel op Vlaams als federaal niveau. In een vervolgtraject kunnen deze referenties worden samengebracht in een concrete en duidelijke getuigenis, waarmee de waardepropositie van de health data space verder kan worden gevormd.

10.2.7 Toetreding tot de data space

In de go-to-marketstrategie mag het toetreden tot de health data space niet ontbreken. Dit proces moet glashelder zijn voor de organisaties binnen het Vlaamse zorg- en welzijnsecosysteem. De drempel moet zo laag mogelijk worden gehouden, zodat de return on investment (ROI) voor de deelnemende organisaties maximaal is. Tegelijkertijd fungeert het als een belangrijke barrière om de efficiëntie en vooral de veiligheid van de data space te waarborgen.
Het proces bestaat uit drie delen. Het is niet noodzakelijk om deze delen in serie uit te voeren; sommige kunnen parallel plaatsvinden, afhankelijk van de verantwoordelijkheden van de betrokken partijen.
Het proces omvat het business-, governance- en technische deel.

10.2.7.1 Business

Een organisatie kan alleen toetreden tot de data space als er een concrete use case is. Dit kan variëren van eenvoudige data-uitwisseling tussen twee organisaties tot complexe combinaties van data tussen meerdere partijen. Hierbij zijn de volgende punten van belang:

- Welke organisaties zijn betrokken bij de data-uitwisseling?
- Wat is het doel van de data-uitwisseling, en wat gebeurt er achteraf met de data?
- Zijn de financiële en technische middelen aanwezig bij elke partij om de use case correct te implementeren?
- Zijn alle organisaties akkoord met de beschreven use case?

Pas als alle bovenstaande punten uitgeklaard zijn, kan men overgaan tot het toetreden van de data space. Het heeft geen zin om een organisatie toe te voegen aan de data space als deze geen actieve datastromen heeft (ook wel een "slapende" of inactieve data space actor genoemd). Om dit te voorkomen is het essentieel dat alle betrokken organisaties vooraf akkoord gaan met de vastgestelde businessregels.
Dit benadrukt ook dat er eerst overeenstemming moet zijn voordat wordt overgegaan tot de technische implementatie.

10.2.7.2 Governance

Naast een geldige use case moet de organisatie ook voldoen aan specifieke governance-regels.
Welke regels dit precies zijn zal moeten worden vastgelegd door de founding fathers bij de oprichting van de data space. Voor meer informatie over dit onderwerp zie 7 Governance. De focus van deze regels zal voornamelijk gericht zijn op de veiligheid en het vertrouwen binnen de huidige use case en de verwachting om actief deel te nemen aan de governance van de volledige health data space. Daarnaast zal in dit stadium ook de contracteringsfase plaatsvinden. Dit proces wordt ook onderzocht in het governance hoofdstuk en moet ervoor zorgen dat enkel organisaties die voldoen aan bepaalde eisen op vlak van veiligheid en databeheer kunnen toetreden tot de data space. Het is bovendien mogelijk om deze stap parallel te laten verlopen met het businessproces.

10.2.7.3 Technisch

Natuurlijk is er ook een belangrijk technisch aspect waaraan voldaan moet worden. Dit betreft voornamelijk het inrichten van een goed geconfigureerde en functionerende connector. Daarnaast moet er aandacht zijn voor het veilig faciliteren van datadeling, bijvoorbeeld via een geauthentiseerde API. Het veilig opslaan van data is eveneens cruciaal, waardoor de aanwezigheid van bijvoorbeeld een S3-bucket niet onbelangrijk is. Tot slot is het noodzakelijk dat er overeenstemming wordt bereikt over het formaat waarin de data wordt gedeeld. De gekozen datastandaard kan in overleg met de betrokken partijen worden bepaald of door de data space organisatie zelf worden opgelegd. Zodra de nodige afspraken op het gebied van business en governance zijn gemaakt, kan direct worden begonnen met het opzetten van de vereiste technische infrastructuur.

10.3 ROADMAP

10.3.1 Input

De roadmap is opgesteld op basis van informatie die verzameld is tijdens het onderzoek, de opgestelde use cases en de input uit verschillende vormen van stakeholdercommunicatie, zoals behoefteanalyse-interviews, EHDS-werkgroepen en validatiegesprekken. Deze roadmap combineert drie informatiestromen die overeenkomen met de drie onderzoek tracks binnen dit project en één algemene stroom.

Op **businessvlak** komt de informatie voornamelijk uit interviews met actoren uit het gezondheidslandschap. Op **governance vlak** vormen de bouwblokken, de governancestructuur en het governance framework de basis voor de roadmap. Voor het **technische luik** schetsen de praktische use cases, koppelingen met externe partijen en de volledige basisinfrastructuur van de data space een mogelijke roadmap.

Gezien de complexiteit en het voortdurend veranderende landschap is de roadmap opgesteld op een **hoog abstractieniveau**. Naarmate er vanuit Europa en haar lidstaten meer richtlijnen worden uitgewerkt op het gebied van technologie, governance en wetgeving, kan de roadmap verder worden verfijnd.

10.3.2 De roadmap

	VOORSTUDIE / VOORBEREIDEND WERK	OPZET VAN DE DATA SPACE	PRE-PRODUCTIE VAN DE DATA SPACE	POST-PRODUCTIE VAN DE DATA SPACE
Algemeen	• Constante opvolging van de EHDS & bijhorende acts • Constante netwerking met andere datadelingsinitiatieven	• Constante opvolging van de EHDS & bijhorende acts • Constante netwerking met andere datadelingsinitiatieven	• Constante opvolging van de EHDS & bijhorende acts • Constante netwerking met andere datadelingsinitiatieven • Continue evaluatie & bijsturing van de data space organisatie en actieve use cases	• Constante opvolging van de EHDS & bijhorende acts • Constante netwerking met andere data delings initiatieven • Continue evaluatie & bijsturing van de data space organisatie en actieve use cases
Business	• Netwerken met actoren voor interessante use cases • Opvolgen van de HDAB's	• Business-luik voorzien binnen de governance structuur • Relatie met HDAB's afstemmen • Financiële resources voor de opstart van de organisatie beheren	• Ondersteunen van de zoektocht naar nieuwe use cases • Project- en budgetbeheer binnen de data space • Nieuwe use cases voorbereiden	• Ondersteunen bij de zoektocht naar nieuwe use cases • Feature roadmap opstellen • Algemeen data space beheer
Governance	• Beslissen omtrent missie, visie, scope en principes • Beslissen omtrent legale en organisatorische entiteit • Use case definitie bottom-up vanuit ecosysteem	• Beslissen omtrent organisatorische structuur • Beslissen omtrent legaal en ethisch kader (governance framework) • Kijken welke implicaties de governance keuzes hebben op het technisch niveau	• "Implementatie": opstart/ creatie van nieuwe use cases • Organisatie beheren • Nieuwe use cases voorbereiden	• Algemene governance van de organisatie beheren • Nieuwe use cases voorbereiden • Bestaande use cases opvolgen
Technisch	• Set-up PoC omgeving op basis van studieproject • Verder onderzoek door middel van PoC's • Opvolgen van SiMPL-bouwblokken • Opvolgen van praktische uitwerking HDAB's in België	• Keuze maken op vlak van technologie • Opzetten van architectuur op basis van gekozen technologie • Technische uitwerking opzetten op basis van gekozen architectuur • Kijken welke implicaties de technische keuzes hebben op governance niveau	• Ondersteuning bij technische implementatie van nieuwe use cases • Onderhoud van het technisch landschap in de data space • Nieuwe use cases voorbereiden	• Ondersteuning bij technische implementatie van nieuwe use cases • Onderhoud van het technisch landschap in de data space

10.3.2.1 Voorstudie/voorbereiding

Tijdens de voorstudie of voorbereidingsfase is het essentieel dat de Proof-of-Concept (PoC) omgeving bij de Vlaamse overheid wordt opgezet op basis van de ervaring die in dit project is opgedaan. Op die manier kunnen nog onduidelijke topics verder worden onderzocht door middel van nieuwe technische PoC's en kan er gefocust worden op onderzoek dat meer gericht is op het bepalen van de uiteindelijke productiebouwblokken.

Tegelijkertijd kunnen er alvast belangrijke governance beslissingen worden genomen die cruciaal zijn voor het opzetten van een data space. Denk hierbij aan het definiëren van de visie, missie, scope en het vaststellen van de juridische en organisatorische entiteit.

Op **businessvlak** is dit ook het juiste moment om verder te zoeken naar potentiële use cases, net zoals in dit project werd gedaan.

Daarnaast is het van groot belang om, naast de algemene opvolging van de EHDS, ook andere initiatieven te blijven volgen. Voorbeelden hiervan zijn het **SIMPL-project, THEDAS2**, andere datadelingsinitiatieven en de HDAB's in België.

10.3.2.2 Opzet van de data space

Zodra alle informatie is verzameld, kan men overgaan tot het opzetten van de data space. Op **businessvlak** betekent dit vooral het beheren van lopende projecten, budgetten en de planning. Daarnaast moet er gecommuniceerd worden met externe stakeholders, zoals potentiële data space-actoren en de HDAB's.

Op **governance- en technisch vlak** wordt het concreter. Het is essentieel om eerst de juiste keuzes te maken met betrekking tot technologie en de organisatorische structuur. Vervolgens kan men overgaan tot het implementeren van de structuur en het aanwerven van de nodige profielen.

Voor het **technische aspect** houdt dit in dat men, op basis van de gekozen technologie, een passende technische architectuur opzet. Dit wordt daarna gevolgd door de technische uitwerking volgens de eerder genomen beslissingen.

In dit deel van de roadmap is het duidelijk dat beslissingen op governance- en technisch niveau elkaar kunnen beïnvloeden. Daarom is het cruciaal dat beide trajecten nauw op elkaar worden afgestemd en door de business track worden opgevolgd.

Tot slot blijven dezelfde algemene taken van kracht als in de vorige fase: het opvolgen van de EHDS en het voortdurend netwerken met andere initiatieven voor datadeling.

10.3.2.3 Pre-productie

De technische data space groeit samen met het hele **business-** en **governance-ecosysteem**. Het is nu tijd om de nieuwe **use cases** uit te werken. Vanaf dit punt wordt het een routine die zich steeds herhaalt. Nieuwe use cases moeten worden geïmplementeerd op zowel technisch als governance-niveau.

Het **technische luik** ondersteunt de data space-actor bij de integratie van de nieuwe technologie.
Het **business- en governance-luik** zorgt ervoor dat nieuwe actoren, die nog geen deel uitmaken van de data space, worden ingeleid en geïnformeerd over de werking van de data space.

Naast het uitwerken van nieuwe use cases moet ook de **data space zelf** op alle vlakken worden beheerd. Vanaf nu vindt er voortdurend iteratie plaats op de **business-, governance- en technische** aspecten van de data space om verbeterpunten te identificeren en processen aan te passen.

Tot slot blijven algemene taken zoals het opvolgen van de **EHDS** en andere **datadelingsinitiatieven** van kracht.

10.3.2.4 Post-productie

In dit deel wordt grotendeels hetzelfde verwacht als in de pre-productiefase, met enkele kleine aanpassingen. **Bestaande use cases** die in productie zijn, kunnen nu feedback genereren om verbeteringen aan te brengen in de data space en de werking van individuele use cases.

Daarnaast kan er steeds meer aandacht worden besteed aan **non-MVP-doelen**, zoals uitbreiding van de scope, uitbreiding naar andere regio's of **EHDS-compliance**.

Hoe meer de data space de EHDS-regulering en de bijhorende HDAB's kan ondersteunen, hoe meer waarde de data space kan bieden voor het health landschap binnen Vlaanderen, België en Europa.

10.4 ACTIEPLAN

Het actieplan schetst de acties die al ondernomen zijn en mogelijke stappen die in de toekomst kunnen volgen. De belangrijkste vereiste om opgenomen te worden in deze lijst van projecten is de impact op de Vlaamse Health Data Space (VHDS). Deze projecten kunnen op verschillende manieren bijdragen:

- **Rechtstreekse bijdrage aan de implementatie en realisatie van de VHDS**
  Bijvoorbeeld: implementatie of verder onderzoek specifiek gericht op de VHDS.
- **Onrechtstreekse bijdrage aan de implementatie en realisatie van de VHDS**
  Bijvoorbeeld: het oprichten van het ecosysteem met instanties waar de VHDS in de toekomst deel van kan uitmaken.
- **Het verduidelijken van de weg naar de implementatie van de VHDS**
  Bijvoorbeeld: Europese wetgeving die standaardisering uitwerkt, waardoor onderzoek naar technologische of datastandaarden niet meer nodig is.

Het is niet noodzakelijk dat een project wordt uitgevoerd vanuit hetzelfde perspectief als dit onderzoek. Zolang een project een concrete meerwaarde biedt voor de verdere oprichting en implementatie van de VHDS, is het waardevol om op te volgen en in dit hoofdstuk te vermelden.

10.4.1 Lopende projecten

10.4.1.1 Oprichting van de HDA

Dit betreft geen projectopvolging, maar eerder de opbouw van een volledige organisatie. De Health Data Authority (HDA) heeft zich gepositioneerd als de coördinerende HDAB voor België in relatie tot de Europese Health Data Space (EHDS). Dit betekent dat zij verantwoordelijk zullen zijn voor taken zoals het verstrekken van data permits. Dit impliceert echter niet dat de HDA al deze taken zelf zal uitvoeren. Er kunnen meerdere uitvoerende HDAB's ontstaan die specifieke taken op zich nemen.

De oprichting van de HDA is cruciaal voor de VHDS. Het biedt inzicht in de functionele en organisatorische vereisten waaraan de VHDS moet voldoen om de HDA optimaal te ondersteunen. Op dit moment is het nog niet helemaal duidelijk welke exacte taken de HDA zal opnemen. Het is dus zeer belangrijk dat de evolutie hiervan wordt opgevolgd zodat de positionering van de VHDS optimaal uitgewerkt kan worden.

10.4.1.2 SIMPL-project

SIMPL is een opensource, veilige middleware-oplossing die datatoegang en interoperabiliteit binnen Europese data-initiatieven ondersteunt. Dit project is een initiatief van de Europese Commissie en richt zich momenteel op de ontwikkeling van een Minimum Viable Product (MVP). Deze MVP zou de algemene behoeften van de meeste data spaces, inclusief health data spaces, moeten dekken.

Het SIMPL-project kan een aanzienlijke impact hebben op de implementatie van de VHDS. Indien er concrete bouwblokken worden uitgebracht op technisch en governance niveau, is de kans groot dat de VHDS deze bouwblokken zal overnemen. Dit zal bijdragen aan interoperabiliteit met de EHDS en andere Europese data space-initiatieven (zie ook 3.4.1.6 SIMPL-project).

10.4.1.3 TEHDAS2

Het TEHDAS2-project is een gezamenlijke actie van 29 landen om de bestaande Europese wetgeving voor het delen van gezondheidsdata te interpreteren. Het doel is om harmonisatie in regelgeving te creëren ter ondersteuning van de implementatie van de EHDS. Dit project biedt richtlijnen en informatie om organisaties zo efficiënt mogelijk om te laten gaan met de veranderingen die de EHDS met zich meebrengt.

Hoewel de VHDS niet alleen gericht is op de EHDS, speelt deze wel een belangrijke rol. De richtlijnen van TEHDAS2 kunnen ervoor zorgen dat bepaalde keuzes automatisch worden overgenomen bij de implementatie van de VHDS.

10.4.1.4 Impactanalyse EHDS VO/EWI/Digitaal Vlaanderen

De impactanalyse van Departemenet Zorg/Digitaal Vlaanderen/EWI richt zich op de EHDS-wetgeving, maar dan vanuit een Vlaams/Belgisch perspectief. Dit project ontrafelt de implicaties van de EHDS-verordening en behandelt vragen zoals:

> Wat moet er gebeuren in het Vlaamse health data-landschap om te voldoen aan de EHDS?
> Hoe groot is de kloof tussen de huidige situatie en de MVP die vereist is om aan de EHDS te voldoen?

Voor de VHDS is het essentieel om dit project te volgen. Het helpt bij het positioneren van de VHDS als een interoperabele en complementaire oplossing voor de Vlaamse/Belgische EHDS-opstelling.

10.4.2 Projecten in aanvraag

10.4.2.1 HDA Call for Innovation

De HDA Call for Innovation (Q4 2024) is een initiatief van de HDA om de ontwikkeling en het beheer van gezondheidsdata te vergemakkelijken. Dit wordt gezien als een kans om in co-creatie de verdere ontwikkeling van de VHDS voort te zetten. Verschillende voorstellen werden ingediend, met een focus op de technische implementatie van de VHDS bij diverse actoren binnen het Vlaamse health data-landschap. Dit kan dienen als springplank tussen het huidige onderzoeksproject en een toekomstig implementatieproject. Bij publicatie van dit eindrapport was er nog geen duidelijkheid over de resultaten van deze innovation call.

10.4.2.2 Voorbereiding en implementatie van de health data space

Na afronding van dit onderzoeksproject is een voorbereidings-/implementatieproject een logisch vervolg. Het onderzoek heeft aangetoond dat er een duidelijke lacune is die de VHDS kan vullen op het gebied van gezondheidsdata-uitwisseling. In combinatie met de EHDS-regulering en het ondersteunende doel van de VHDS, biedt dit voldoende aanleiding om een vervolgproject te starten. Dit nieuwe project zal zich richten op de effectieve implementatie van de VHDS. Een projectvoorstel werd voorgelegd aan de nieuwe regering. Bij publicatie van dit eindrapport was er nog geen nieuws over al dan niet toekenning van budgetten voor dit vervolgproject.

11 CONCLUSIE

Het Vlaamse Health Data Space R&D-project heeft als pionier binnen het huidige data space landschap de fundamenten gelegd voor de ontwikkeling van een Vlaamse health data space en de voorbereiding op de European Health Data Space (EHDS)-regulering. Het project, uitgevoerd tussen 2023 en 2024, heeft waardevolle inzichten opgeleverd over de business-, governance-, juridische en technische randvoorwaarden die essentieel zijn voor de realisatie van een dergelijke data space.

Hoewel het ambitieniveau aanvankelijk zeer hoog lag, bleek tijdens de looptijd van het project dat de complexiteit van het stakeholderlandschap en de onduidelijkheden rond juridische en technische vereisten zorgden voor bijstellingen van de doelen. Ondanks deze uitdagingen heeft het project een minimaal maar waardevol kader ontwikkeld dat als startpunt kan dienen voor verdere implementatie en uitwerking van de Vlaamse health data space.

Een belangrijke vaststelling is dat, ondanks de moeizame betrokkenheid van sommige stakeholders, de vraag naar decentrale manieren van datadeling in de gezondheidszorg groeit. Dit toont het belang aan van een aanpak die rekening houdt met de verwachtingen en onzekerheden van actoren binnen het gezondheidszorglandschap. Daarnaast biedt het rapport een belangrijke bijdrage door openstaande vragen en kritische aandachtspunten rond de EHDS-regulering te verhelderen, zoals secure processing environments en rolverdelingen.

Met dit onderzoeksproject heeft Vlaanderen een voortrekkersrol ingenomen en aantoonbare vooruitgang geboekt in vergelijking met andere EU-lidstaten. Hoewel veel aspecten in de toekomst herbekeken zullen moeten worden naarmate de EHDS-regulering concreter wordt, biedt dit rapport een solide basis voor verdere stappen en een visie voor datadeling binnen de Vlaamse gezondheidszorg.

Kortom, het project heeft de Vlaamse positie in het Europese data space landschap versterkt en waardevolle bouwstenen geleverd om de implementatie van de EHDS-regulering te ondersteunen.

12 ONDERZOEKSDOELSTELLINGEN

Als onderdeel van dit onderzoeksproject werd een antwoord gevraagd op een aantal onderzoeksdoelstellingen zoals beschreven in het Besluit van de Vlaamse Regering (BVR). De beschrijving van deze activiteiten en hoe bovenvermelde hoofdstukken hierop een antwoord geven komt aan bod in dit hoofdstuk.

12.1 DOELSTELLING 1

12.1.1 Omschrijving

Noden van de overheid inzake datagedreven beleid, population health & care management, health data space en een digital health & care twin in kaart brengen.

12.1.2 Resultaten

Deze noden of behoeften werden in kaart gebracht in hoofdstuk 4 Behoefteanalyse Vlaamse Health Data Space (business context). Hierbij werd stapsgewijs te werk gegaan.

Eerst werden de te bevragen stakeholders in kaart gebracht (4.1.1 Stakeholder identificatie) waarna voor elk van die stakeholders een behoefteanalyse werd gemaakt (4.1.2 Behoeften bevragen). Vervolgens werd gekeken naar de huidige en toekomstige situatie (4.2 Huidige en ideale (toekomstige) situatie) om daarna de behoeftes te formuleren van een health data space (4.3 Behoeftes Health Data S).

In een laatste fase werd gekeken naar de behoeftes van de Vlaamse overheid (4.4 Noden van de Vlaamse overheid).

12.2 DOELSTELLING 2

12.2.1 Omschrijving

Deze noden mappen ten opzichte van nationale en internationale technologische enablers: gaia-x, IDSA, VSDS (niet limitatieve lijst)

12.2.2 Resultaten

In eerste instantie werd een overzicht gegeven van deze verschillende technologische enablers op Vlaams, Belgisch en internationaal niveau. Ook werd aandacht besteed aan data spaces in het domein van de gezondheidszorg:

> 3.4.1 Internationale speelveld
> 3.4.2 Belgische speelveld
> 3.4.3 Vlaamse speelveld
> 3.4.4 Data spaces in het domein van de gezondheidszorg

In een tweede fase werd een analyse gemaakt van de actuele data space componenten van deze enablers (zie hoofdstuk 8.1 Analyse actuele data space componenten). Finaal werd op basis van de noden vanuit doelstelling 1 een conceptuele architectuur gedefinieerd (zie hoofdstuk 8.2 Conceptuele architectuur) en werd deze gemapt ten opzichte van de actuele componenten om zo het design van een Health Data Space te bepalen (zie hoofdstuk 8.3 Design componenten).

12.3 DOELSTELLING 3

12.3.1 Omschrijving

Via een use-case gedreven aanpak valideren: aan de hand van technische en inhoudelijke use-cases.

12.3.2 Resultaten

In hoofdstuk 5 Use cases werd een overzicht gegeven van het plan van aanpak en de potentiële use cases binnen dit project. In de daaropvolgende hoofdstukken wordt uitleg gegeven over de juridische, governance, en technische aspecten om vervolgens in hoofdstuk 9 Uitwerking Data4PHM use case, meer detail te geven over hoe dit werd toegepast op de uiteindelijke gekozen use case binnen dit project.

12.4 DOELSTELLING 4

12.4.1 Omschrijving

Inzichten en expertise aanleveren en overdragen aan de administratie, opdat een roadmap kan uitgebouwd worden voor verdere uitrol op grote schaal.

12.4.2 Resultaten

Gedurende dit project werden verschillende workshops opgezet met het doel inzichten en expertise te verzamelen en aan te leveren aan de administratie van Departement Zorg. Deze inzichten werden verwerkt in de verschillende hoofdstukken in dit rapport en vormen de basis voor hoofdstuk 10 Go-to-marketstrategie - Roadmap - Actieplan.

12.5 DOELSTELLING 5

Antwoorden en methodologieën en procedures aanreiken voor onderstaande onderzoeksvragen.

12.5.1 Onderzoeksvraag 1

12.5.1.1 Omschrijving

Hoe kunnen we bestaande initiatieven en architecturale concepten rond data spaces (vb. gaia-x, IDSA, VSDS) gebruiken in functie van dit project rond population health management en digitale health & care twin?

12.5.1.2 Resultaten

In eerste instantie werd een overzicht gegeven van de bestaande initiatieven en architecturale concepten. Dit zowel op Vlaams, Belgisch als op internationaal niveau. Ook werd aandacht besteed aan data spaces in het domein van de gezondheidszorg:

> 3.4.1 Internationale speelveld
> 3.4.2 Belgische speelveld
> 3.4.3 Vlaamse speelveld
> 3.4.4 Data spaces in het domein van de gezondheidszorg

In een tweede fase werd op basis van deze initiatieven en concepten een overzicht gegeven van de bestaande data space componenten (zie hoofdstuk 8.1 Analyse actuele data space componenten) en in een laatste fase werd nagegaan hoe deze kunnen gebruikt worden in functie van dit project rond population health management (zie hoofdstuk 8.3 Design componenten en hoofdstuk 8.4 User journey).

12.5.2 Onderzoeksvraag 2

12.5.2.1 Omschrijving

Hoe ziet de architectuur van een data space voor population health management binnen het Zorgatlas-platform eruit?

12.5.2.2 Resultaten

Bij deze onderzoeksvraag is op te merken dat initieel van een verkeerde premisse vetrokken werd, namelijk dat de data space deel zou uitmaken van het bestaande ZorgAtlas Data Platform van het Departement Zorg. Gezien een data space echter een decentraal karakter heeft en het Departement Zorg hierin als prosumer zou optreden, werd hier dan ook van afgestapt. De voorgestelde architectuur (zie 8.8 Zorgatlas) baseert zich op een aantal componenten zoals een data space connector of data catalog die potentieel binnen de infrastructuur van het Departement Zorg zouden gedeployed kunnen worden.

12.5.3 Onderzoeksvraag 3

12.5.3.1 Omschrijving

Hoe kan de health data space gekoppeld worden aan andere data spaces (-infrastructuur) (lokaal, nationaal, internationaal)?

12.5.3.2 Resultaten

Het data space landschap was tijdens de looptijd van het project nog onvoldoende geëvolueerd om reeds doorgedreven inzichten te genereren rond de koppeling van de health data space aan andere data spaces. Aangezien koppeling uitdagingen meebrengt op zowel technisch als governance vlak, dient deze onderzoeks-vraag verder uitgediept te worden in een vervolgproject (zie sectie 4.3.3 Het koppelen van data spaces).

12.5.4 Onderzoeksvraag 4

12.5.4.1 Omschrijving

Hoe kan een Health-data space een meerwaarde creëren voor de betrokken interne en externe stakeholders?

12.5.4.2 Resultaten

Eerst en vooral werden de te bevragen stakeholders in kaart gebracht (4.1.1 Stakeholder identificatie) waarna vervolgens de behoeften werden bevraagd (4.1.2 Behoeften bevragen). Vervolgens werd gekeken naar de huidige en ideale (toekomstige situatie) (4.2 Huidige en ideale (toekomstige) situatie) om daarna de behoeftes te formuleren van een health data space (4.3 Behoeftes Health Data S).

12.5.5 Onderzoeksvraag 5

12.5.5.1 Omschrijving

Hoe kunnen we de Health Data Space operationaliseren, rekening houdend met de randvoorwaarden op ethisch, legaal en gegevensveiligheidsvlak?

12.5.5.2 Resultaten

In hoofdstuk 6 Juridische en ethische principes worden de randvoorwaarden op ethisch, legaal en gegevensveiligheidsvlak overlopen en in hoofdstuk 10 Go-to-marketstrategie - Roadmap - Actieplan wordt besproken hoe een health data space kan geoperationaliseerd worden.

12.5.6 Onderzoeksvraag 6

12.5.6.1 Omschrijving

Hoe krijgen we onze databases en datastromen FAIR en wat met standaarden zoals OSLO, openEHR (niet limitatieve opsomming)?

12.5.6.2 Resultaten

Om deze vraag te beantwoorden werd onderzoek gedaan enerzijds algemeen binnen het gebied van datastandaarden (zie 8.5 Datastandaarden) maar anderzijds ook specifiek binnen de uitwerking van de use case (zie 9.3 Fair data en metadata).

13 LEXICON

Het lexicon definieert de meest gangbare termen zoals gebruikt binnen dit project.

Accession Agreement (*toetredingsvoorwaarden*)
Een schriftelijke verklaring die de toelating van een rechtspersoon of natuurlijk persoon tot de data space regelt. Vanaf het moment van ondertekening, verbindt deze entiteit zich tot het naleven van de algemene voorwaarden van de data space. Doorgaans bevat de toetredingsovereenkomst elementen zoals:

- Algemene voorwaarden
- Toegangs- en gebruiksbeleid op data space-niveau
- Governance structuur (inclusief omschrijving van de rollen en verantwoordelijkheden)
- High-level procedures (bijvoorbeeld on-/offboardingprocedure, conflictresolutie …)
- Code of conduct (gedragscode)

Men kan verschillende versies van de toetredingsovereenkomst hanteren, afhankelijk van de rol(len) die de ondertekenende entiteit zal invullen binnen een data space.

Attestation (*attestatie*)
Het validatieproces dat controleert of aan bepaalde eisen werd voldaan in het kader van het authenticatieproces. Er zijn drie soorten attestaties.

- Identity attestation (identiteitsattestatie): toont aan dat een entiteit binnen een bepaalde context gekoppeld is aan specifieke rollen, rechten of verantwoordelijkheden.
- Participation attestation (deelname-attestatie): toont aan dat iemand deelneemt aan een specifieke data space en zich aan de regels houdt.
- Compliance attestation (nalevingsattestatie): toont aan dat een entiteit voldoet aan nationale of sectorspecifieke regels.

Attestatie wordt gevalideerd door een trust anchor. Indien de attestatie vergezeld wordt van een cryptografisch bewijs, kan men van een verifiable credential spreken.

Authenticatie en autorisatie
Het authenticatieproces is gericht op het bevestigen van een identiteit, terwijl autorisatie bepaalt welke toegangsniveaus en -rechten een entiteit zal krijgen.

Broker
Zie **Metadata Broker**

Clearing house
Een *data intermediary* die diensten verleent met betrekking tot de afhandeling en verrekening van financiële en datatransacties binnen de data space. De clearing house heeft vier primaire functies.
(1) Verzoening en afwikkeling van datatransacties. (2) Naleving van de voorwaarden die zijn vastgesteld door dataleveranciers. (3) Toekenning van de overeengekomen vergoeding voor (de uitwisseling van) data. (4) Registratie van data- en/of financiële transacties. Daarnaast kan de clearing house een rol spelen in de authenticatie- en autorisatieprocedures van de data space.

Code of conduct (*gedragscode*)
Een reglement dat de zachte regels rond “goed gedrag” binnen de data space afdekt. Het omschrijft onderwerpen als normen, principes en verwachtingen naar correct of ethisch gedrag. In de meeste gevallen zal het navolgen van deze regels eerder afhangen van goodwill dan van handhaving.

Connector
De data space component die ontworpen is om de gegevensuitwisseling te faciliteren door op een veilige, gecontroleerde en interoperabele manier te communiceren met alle andere componenten binnen de data space. Het is de toegangspoort naar de data space. Een connector kan uitgerust zijn met ingebouwde functies voor autorisatie, versleuteling en het handhaven van datadelingsafspraken.

Control plane
De Control Plane is het geheel aan componenten binnen het data space ecosysteem die verantwoordelijk zijn voor het afhandelen van overeenkomsten voor het delen van data en is verantwoordelijk voor het orkestreren van de data transfer door het delegeren aan de Data Plane. Control planes beheren o.a. de state (start, stop, pending, in progress ...) van een data transfer en kunnen inzichten bieden (aan de hand van transaction logs).

Cryptographic proof (*cryptografisch bewijs*)
Een wiskundig en technisch bewijs dat aantoont dat een bepaalde attestatie valabel is, en er niet mee geknoeid is. Dit bewijs wordt uitgegeven door een Trust Anchor.

Data asset
Een waardevolle bron van data die werd verzameld, opgeslagen en geoptimaliseerd voor gebruik in een bepaald product, dienst of proces. Het kan verschillende vormen aannemen, zoals een database, dataset, of een andere vorm van georganiseerde gegevensverzameling.

(Data)catalogus
Een georganiseerde verzameling van metadata die een overzicht biedt van de beschikbare datasets binnen een data space. Het fungeert als een soort zoekmachine, waarbinnen gebruikers gegevensbronnen kunnen vinden en er toegang toe kunnen vragen.

Data consumer
Een data space participant (rechtspersoon of natuurlijk persoon) die betrokken is bij het ontvangen en gebruiken van data die verstrekt wordt door een data provider. Een data consumer gebruikt de data zoals ze wordt aangeleverd voor doeleinden zoals rapportage of beleidsbeslissingen. Een data consumer die de data ook bewerkt, wordt veelal eerder als data user beschouwd.

Data governance
Het raamwerk van regels, processen en beleidsprocedures die bepalen hoe data binnen een organisatie wordt beheerd, beschermd en benut. Het omvat verantwoordelijkheden met betrekking tot het ontwerp, de eigendom, de toegang en het gebruik van data, en zorgt ervoor dat gegevens op een consistente, veilige en verantwoorde manier worden behandeld, met aandacht voor compliance, privacy en kwaliteit.

Data holder (gegevensverstrekker)
Een rechtspersoon of natuurlijke persoon die verantwoordelijk is voor het bewaren, beheren en beschermen van gegevens in overeenstemming met toepasselijke wet- en regelgeving en rekening houdende met eventuele toepasselijke intellectuele eigendomsrechten. De data holder heeft het recht om toegang te verlenen tot, of controle uit te oefenen over de gegevens.

Data intermediary
Een partij of entiteit binnen de data space die een essentiële technische of niet-technische dienst levert om betrouwbare datatransacties tussen participanten mogelijk te maken of te vergemakkelijken.
Data intermediairs leveren diensten aan zoals dataverzameling, databeheer, identiteitsmanagement, autorisatie, toestemmingsbeheer of gegevensverificatie. Ze kunnen daarbij wel of niet betrokken zijn bij de eigenlijke gegevensuitwisseling.

Indien een data intermediary ook erkend wil zijn door de DGA als data intermediation service provider (DISP), dan moet deze entiteit voldoen aan de vereisten opgesteld in Hoofdstuk III van de DGA (meer bepaald de artikels 10 en 12 in het bijzonder).

Data plane
De Data Plane is verantwoordelijk voor de uiteindelijke data transfer van een data provider naar een data consumer. Verschillende Data Planes ondersteunen de verschillende data transfer protocollen (zoals HTTPS, S3, files transfer ...).

Data product
Een data product is een verzameling van data assets, zoals datasets en dataservices, die gebundeld zijn in een bruikbare vorm en die zakelijke waarde leveren in een specifieke use case of data space toepassing.

Data (product) contract
Het contract dat de afspraken, voorwaarden en regels voor het gebruik, delen en beheren van een specifiek data product binnen een data space vastlegt, zodat het data product op een veilige manier wordt gebruikt. Het contract definieert onder andere de toegangs- en gebruiksvoorwaarden, de datakwaliteit en -beschikbaarheid, de beveiliging- en privacyregels, de verantwoordelijkheden en rechten, en de regels rond monitoring en naleving.

Data product owner
De partij verantwoordelijk voor het beheer en de waardecreatie van een data product binnen de data space. Deze zorgt ervoor dat het data product aansluit bij de behoeften van gebruikers en de strategische doelen, en beheert aspecten zoals de ontwikkeling en kwaliteit van het dataproduct, onder andere door het onderhouden van de metadata in de datacatalogus.

Data prosumer
Een deelnemer aan een data space die zowel data deelt (data provider) als gebruikt (data consumer).

Data provider (gegevenshouder)
Een deelnemer aan een data space die gegevens ter beschikking stelt aan andere deelnemers binnen die data space. De data provider kan bij het toegang verlenen tot deze gegevens zijn eigen voorwaarden opleggen aan eventuele gebruikers (data consumers) via gebruiks- en toegangsrechten, maar is potentieel zelf gebonden aan de voorwaarden die vastgesteld zijn door de gegevensverstrekker (data holder).

Data recipient
Een deelnemer aan de data space die - binnen een specifieke datatransactie - gegevens (technisch) ontvangt van een data provider. Het is mogelijk dat de data recipient deze gegevens daarbij niet verwerkt of gebruikt, en ze uitsluitend doorgeeft aan een andere partij. Vindt er wel een verwerking of consumptie plaats, dan is de data recipient ook een data user of een data consumer.

Data space catalog
Een lijst van alle aangeboden data producten en hun usage policies in een data space.

Data space governance
Het geheel van regels, beleidsmaatregelen, processen en structuren die het beheer en de organisatie van een data space reguleren. Een goed beheerde data space creëert vertrouwen en laat deelnemers toe aan data-uitwisseling te doen met respect voor de juridische, ethische, zakelijke en technische vereisten.

Data space participant (d*ata space deelnemer*)
Een partij die deelneemt aan een data space en zich ertoe verbonden heeft de regels en het regelgevend kader van die data space na te leven. Een data space participant kan zowel een natuurlijk persoon als een rechtspersoonlijkheid zijn (bijvoorbeeld een bedrijf of een overheidsdienst).

Data space registery
Een officieel register of een lijst van deelnemers aan een data space (data providers, data consumers en andere relevante partijen). Het register bevat informatie over de identiteit van de deelnemers en hun rechten, verantwoordelijkheden en rollen binnen de data space.

Data space use case
Een specifieke toepassing waarin de gegevens binnen een data space worden gebruikt om een bepaald probleem op te lossen, een dienst te leveren of waarde te creëren voor de deelnemers.

Data subject
Een natuurlijk persoon wiens persoonsgegevens worden verzameld, verwerkt of gedeeld binnen een data space. Dit individu is geïdentificeerd of identificeerbaar, hetzij direct (bijvoorbeeld door een naam of identificatienummer) hetzij indirect (via andere kenmerken zoals locatie, online identificatie, of specifieke fysieke, genetische, psychologische, economische of sociale kenmerken).

Data transactie
Het proces waarbij gegevens worden uitgewisseld tussen partijen binnen een data space. Dit proces heeft zowel een technische als een zakelijke dimensie en omvat verschillende fasen ([start] → onderhandeling → acceptatie → uitvoering → gebruik → [einde]). Tijdens iedere fase in het proces kan een conflictsituatie optreden die tot escalatie en (eventueel) het heronderhandelen van de transactie kan leiden.

Data transfer
De concrete transfer van gegevens van een data provider naar een data consumer. Een data transfer kan plaatsvinden via verschillende data transfer protocollen (zoals HTTPS, S3, files transfer ...).

Data user (*gegevensgebruiker*)
Een partij die gebruik maakt van data binnen een data space, ongeacht of deze data wordt geconsumeerd, geanalyseerd, verwerkt of hergebruikt. De data kan voor verschillende doeleinden worden gebruikt, zoals analyse, rapportage, machine learning, of het creëren van nieuwe producten en diensten. Data users bewerken of transformeren gegevens voor verdere toepassingen, in tegenstelling tot data consumers, die gegevens per definitie gebruiken zoals ze worden aangeleverd.

Digitaal contract
Het digitaal contract legt de voorwaarden, policies en afspraken vast die twee (of meer) participanten maken op het niveau van een data asset of dataproduct. Deze afspraken komen boven op de algemene afspraken die in de accession agreement vastgelegd zijn op data space niveau.

Federated catalog
Geeft een overzicht van de individuele catalogs beschikbaar op elke connector in een data space.
De beschrijving van zo'n catalog komt sterk overeen met de beschrijving van een individuele catalog waar de federated catalog een groepering is van een aantal catalogs. Een metadata broker maakt gebruik van de federated catalog om nog extra features zoals zoeken en vinden toe te voegen.

Identifier
Een unieke aanduiding of code die wordt gebruikt om een specifiek object, entiteit of item te identificeren binnen een systeem of netwerk. Het zorgt ervoor dat het object op een eenduidige manier kan worden herkend en onderscheiden van andere objecten.

Identity provider
Een entiteit die diensten aanbiedt voor het creëren, onderhouden, beheren en verifiëren van identiteitsinformatie van deelnemers aan een data space, zodat toegang tot systemen en gegevens op een gecontroleerde manier kan worden verleend.

Interoperabiliteit
Het vermogen van verschillende systemen, software of technologieën om effectief en naadloos met elkaar te communiceren en samen te werken, ondanks verschillen in onderliggende structuren of standaarden.

Governance authority
Het geheel aan governance bodies (of governance-organen) binnen een data space die verantwoordelijk zijn voor het opstellen, onderhouden en operationaliseren van het governance framework. De governance authority omvat (minstens) een bestuurlijke en een uitvoerende functie. Afhankelijk van de grootte en de juridische structuur van de data space kan de governance authority ook andere functies uitvoeren, en uit één of meerdere organen bestaan.

Governance body (*governance-orgaan*)
Een structuur binnen een data space die toegewezen is aan (een) specifieke functie(s) of taak met betrekking tot het operationaliseren en onderhouden van het governance framework.

Governance framework
Het geheel aan interne regels, beleidsmaatregelen, afspraken, processen en procedures die betrekking hebben op de organisatie en de dagelijkse werking van de data space, en die zorgen voor effectief en verantwoordelijk leiderschap, controle en toezicht.

Governance structuur
Het geheel aan governance-organen, inclusief de bijhorende rollen, verantwoordelijkheden, en verhoudingen, zowel tot andere interne governance-organen, als tot relevante externe actoren.
In tegenstelling tot de governance authority omschrijft de governance structuur dus ook de relaties en samenwerkingen met entiteiten buiten de data space.

Metadata
Gegevens die informatie beschrijven over de data. Het biedt de nodige context om data te kunnen beheren, registreren en interpreteren. Het bevat details over de inhoud, het formaat, de oorsprong, de bewerkingen en de toegang van de gegevens.

Metadata broker
De metadata broker is de verzamelplaats van alle metadata en ondersteunt het doorzoeken van aangeboden datasets. Het is een applicatie die het bijvoorbeeld toelaat voor een gebruiker om op zoek te gaan naar datasets waarin bepaalde gegevens zitten die nodig zijn voor zijn onderzoek. De metadata broker zal daarbij ook aangeven waar en hoe de gebruiker de gewenste gegevens kan bekomen.

NiFi
Apache NiFi is een softwareproject van de Apache Software Foundation dat is ontworpen om de gegevensstroom tussen softwaresystemen te automatiseren. Het maakt gebruik van het concept van extraheren, transformeren, laden (ETL) en is gebaseerd op de "NiagaraFiles"-software die eerder is ontwikkeld door de Amerikaanse National Security Agency (NSA), die ook de bron is van een deel van zijn huidige naam - NiFi.

Onboarding
Het proces voor toetreding tot een data space. Het wordt veelal opgenomen in de accession agreement en omschrijft de verschillende stappen die een deelnemer zal doorlopen om een volwaardig lid te worden van de data space. Het proces kan verschillend zijn voor verschillende types deelnemers.

Offboarding
Het proces voor uittreding uit een data space. Net zoals de onboarding procedure wordt dit proces doorgaans opgenomen in de accession agreement, waar de voorwaarden tot uittreding, de looptijd van de overgangsperiode en de afspraken rond dataretentie duidelijk omschreven zijn. Indien de data space een gedwongen offboarding procedure wil voorzien (bijvoorbeeld als deel van haar handhavingsmechanismes), dan worden de voorwaarden voor een onvrijwillige exit hier duidelijk in gestipuleerd.

Rules (regels) en policies (beleidslijnen)
Rules of regels zijn specifieke en gedetailleerde richtlijnen die voorschrijven wat wel of niet mag in een bepaalde situatie. Ze zijn vaak rigide en operationeel, en gericht op het afdwingen van concreet gedrag. Policies of beleidslijnen zijn bredere principes of richtlijnen die een algemeen kader schetsen voor besluitvorming en gedrag. Ze bieden meer flexibiliteit en richten zich op de langetermijnstrategie.

Provenance (herkomst van de data)
Informatie over de datatransactie, opgeslagen als bijkomende data. Het beschrijft de geschiedenis van de gegevens vanaf het moment van creatie tot het moment van consultatie en omvat details over de herkomst van de gegevens, de erop uitgevoerde processen en de partijen die betrokken waren bij de verzameling, bewerking of analyse. Deze provenance-data kunnen door een data consumer of data user geconsulteerd worden.

SIMPL
Open source middleware platform dat technische bouwblokken aanbiedt voor het bouwen van (Europese) data spaces. De bouwblokken ondersteunen o.a. data toegang en interoperabiliteit ondersteunt tussen internationale data spaces. Wordt gesteund door de Europese commissie en is op moment van schrijven in volle ontwikkeling.

Traceability (traceerbaarheid)
Informatie over de datatransactie, opgeslagen als bijkomende data. Waar provenance een data consumer toelaat terug te keren naar de herkomst van de data, maakt traceability het latere gebruik van de gegevens transparant voor een data provider. Traceability-gegevens loggen de uitgevoerde bewerkingen en transformaties, en houden bij wie toegang heeft gehad tot of gebruik heeft gemaakt van de gegevens.

Trust anchor
Een betrouwbare (neutrale) entiteit, organisatie of technisch middel dat kan worden ingezet om bijvoorbeeld een identiteit of (digitale) certificaat te valideren en uit te geven.

Trust framework
Het geheel aan (technologische) middelen en mechanismen die het mogelijk maken het governance framework uit te voeren. Het trust framework laat toe deelnemers en diensten af te wegen tegen de gemaakte regels en afspraken en maakt handhaving mogelijk. Op die manier zorgt het trust framework voor transparantie, veiligheid, vertrouwen en controle binnen de data space.

Usage policy (gebruiksbeleid)
De term usage policy kan in twee contexten gebruik worden:

- Het betreft de voorwaarden en regels die van toepassing zijn op data space participanten en/of data intermediaries die diensten verlenen in het kader van de health data space. Dit omvat het geheel van interne en governance regels, specifiek bepaald door de health data space zelf, zoals gedragsregels, alsook externe wetgeving die van toepassing is en geconcretiseerd kan zijn.
  Er wordt naar deze regels verwezen in de accession agreement.
- Het betreft de voorwaarden en regels die van toepassing zijn op de data assets bepaald door de data provider en/de holder. Het zijn de voorwaarden onder dewelke een data kan gedeeld worden met een data consumer.

Value-added services
Verzamelnaam voor alle bijkomende diensten die een data space wil aanbieden aan haar deelnemers, extra bij de eigenlijke datatransacties. Deze diensten creëren op een of andere manier waarde voor het ecosysteem, bijvoorbeeld omdat ze nieuwe functionaliteiten aanbieden of bestaande functionaliteiten gebruiksvriendelijker maken. Voorbeelden van value-added services zijn data transformaties, AI-modellen, pseudonimisatie, data gateway services …

Verifiable credentials
Een type identiteitsverificatie waarbij een attestatie bevestigd kan worden via een cryptografisch bewijs, doorgaans uitgegeven door een trust anchor.

Vocabulary of Vocabularia
Een gestandaardiseerde set van termen, definities en concepten die worden gebruikt om data te beschrijven en te structureren. Het biedt een gemeenschappelijke taal voor deelnemers in een data space.

Vocabulary provider
Een deelnemer aan een data space die verantwoordelijk is voor het creëren, beheren en onderhouden van vocabularia (gestandaardiseerde termen en definities) die binnen de data space worden gebruikt.
Ze zorgen ervoor dat de data space vocabularia in lijn liggen met internationaal gedefinieerde standaarden en staan in nauw overleg met het gehele ecosysteem.

Vocabulary hub
Gecentraliseerde opslagplaats of platform voor het opslaan en raadplegen van overeengekomen vocabularia. Het dient als bron voor toegang tot en integratie van vocabularia in datamodellering. Devocabulary hub bevordert de vindbaarheid van termen en concepten binnen een data space en kan ook informatie bevatten over herkomst en traceerbaarheid.

14 AFKORTINGENLIJST

ADD	Attention Deficit Disorder
AH	Aansprakelijkheid
AIA	AI Act (AI-verordening)
API	Application Programming Interface
AV	Algemene vergadering
AVA	Algemene vergadering van aandeelhouders
AVG	Algemene Verordening Gegevensbescherming
BID	Beleidsinformatie en Data
BMI	Body Mass Index
BV	Besloten vennootschap
BVR	Besluit van de Vlaamse Regering
CRUD	Create, Read, Update, Delete
DAC	Data access committee
DAO	Organisatie voor data-altruïsme of data altruism organisation
DGA	Datagovernanceverordening of data governance act
DID	Decentralized Identifier
DISP	Databemiddelingsdienst of data intermediary service provider
DMZ	Demilitarized Zone
DPIA	Data protection impact assessment
DPO	Functionaris voor gegevensbescherming of data protection officer
DSA	Data Sharing Agreement
DSBA	Data Spaces Business Alliance
DSSC	Data Space Support Centre
DS4H	Dataspace4health
DZORG	Departement Zorg
EU	Europese Unie
EDPB	European Data Protection Board
EESV	Europees economisch samenwerkingsverband
EHDS	European Health Data Space
EPD	Elektronisch Patiënten Dossier
FAIR	Findable Accessible Interoperable Reusable
FFDP	Verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie of Free flow of non-personal data regulation
FHIN	Federated Health Innovation Network
GBA	Gegevensbeschermingsautoriteit
GDA	Gezondheidsdata Agentschap
GEB	Gegevensbeschermingseffectenbeoordeling
GFD	Gedeeld Farmaceutisch Dossier
HDA	Health data agency
HDS	Health data space
HPV	Humaan papillomavirus
HTML	HyperText Markup Language
IAM	Identity en Access Management
IDS	International Data Spaces
IDSA	International Data Space Association
IE	Intellectuele Eigendom
IMA	Intermutualistisch Agentschap

IVC	Informatie Veiligheidscomité
IVZW	Internationale vereniging zonder winstoogmerk
KSZ	Kruispuntbank van de Sociale Zekerheid
MOU	Memorandum of Understanding
MVP	Minimum Viable Product
MZG	Minimale Ziekenhuis Gegevens
NIST	National Institute of Standards and Technology
NV	Naamloze vennootschap
ODRL	Open Digital Rights Language
OMOP	Observational Medical Outcomes Partnership
OSLO	Open Standards for Linked Organizations
PHM	Population Health Management
PoC	Proof of Concept
PSI	Richtlijn hergebruik overheidsinformatie
RPH	Rechtspersoonlijkheid
RvB	Raad van Bestuur
SCE	Europese coöperatieve vennootschap
SE	Europese naamloze vennootschap
SFTP	Server File Transfer Protocol
SOLID	Social Linked Data
SPE	Secure Processing Environment
SSDF	Secure Software Development Framework
SZ	Sociale zekerheid
TTP	Trusted Third Party
VC	Verifiable Credential
VHDS	Vlaamse Health Data Space
VIKZ	Vlaams Instituut voor Kwaliteit van Zorg
VSDS	Vlaamse Smart Data Space
VWDS	Vlaamse Water Data Space
VZN	Vlaams Ziekenhuis Netwerk
VZW	Vereniging zonder winstoogmerk
WER	Wetboek Economisch Recht
WVP	Wet Verwerking Persoonsgegevens
WVV	Wetboek Vennootschappen en Verenigingen

15 REFERENTIELIJST

15.1 WETGEVING

15.1.1 Europees

- Verordening (EU) 2024/… van het Europees Parlement en de Raad van … *on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847*. (Finale versie nog niet gepubliceerd)
- Verordening (EU) 2024/1689 van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie). *Publicatieblad van de Europese Unie,* 12 juli 2024.
- Verordening (EU) 2023/2864 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data en tot wijziging van Verordening (EU) 2017/3294 en Richtlijn (EU) 2020/1828. *Publicatieblad van de Europese Unie*, 22 december 2023, p. 2854.
- Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 20 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724. *Publicatieblad van de Europese Unie* 152, 3 juni 2022, p. 1.
- Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie. *Publicatieblad van de Europese Unie* 303, 28 november 2018, p. 59-68.
- Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad. *Publicatieblad van de Europese Unie* 117, 5 mei 2017, p. 1-175.
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming). *Publicatieblad van de Europese Unie (L119)*, 27 april 2016, 1-88.
- Verordening (EU) 2016/426 van het Europees Parlement en de Raad van 9 maart 2016 betreffende persoonlijke beschermingsmiddelen en tot intrekking van Richtlijn 89/686/EEG van de Raad. *Publicatieblad van de Europese Unie L* 81, 31 maart 2016, p. 51.
- Verordening (EU) 536/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende klinische proeven met geneesmiddelen voor menselijk gebruik en tot intrekking van Richtlijn 2001/20/EG. *Publicatieblad van de Europese Unie* L 158, 27 mei 2014, p. 1-76.
- Verordening (EU) 726/2004 van 31 maart 2004 tot vaststelling van communautaire procedures voor het verlenen van vergunningen en het toezicht op geneesmiddelen voor menselijk en dierengeneeskundig gebruik en tot oprichting van een Europees Geneesmiddelenbureau. *Publicatieblad van de Europese Unie* 136, 30 april 2004, p. 1.
- Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG. *Publicatieblad van de Europese Unie L* 96, 22 mei 2014, p. 62.
- Richtlijn 2004/23/EG van 31 maart 2004 tot vaststelling van kwaliteits- en veiligheidsnormen voor het doneren, verkrijgen, testen, bewerken, bewaren en distribueren van menselijke weefsels en cellen. *Publicatieblad van de Europese Unie* 102, 7 april 2004, p. 48.
- Richtlijn (EU) 2019/1024 van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (PSI). *Publicatieblad van de Europese Unie*, 26 juni 2019, p. 56.

- Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan. *Publicatieblad van de Europese Unie* 157, 15 juni 2016, p. 1-18.
- Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken. *Publicatieblad van de Europese Unie* 77, 27 maart 1996, p. 20-28.
- Richtlijn 2001/83/EG van het Europees Parlement en de Raad van 6 november 2001 tot vaststelling van een communautair wetboek betreffende geneesmiddelen voor menselijk gebruik. *Publicatieblad van de Europese Unie*, 28 november 2001, p. 67.

15.1.2 Belgisch

- Gecoördineerde Grondwet. *Belgisch Staatsblad*, 17 februari 1994.
- Wetboek van Economisch Recht. *Belgisch Staatsblad,* 29 maart 2013, p. 19 975.
- Wetboek van Vennootschappen en Verenigingen (WVV). *Belgisch Staatsblad*, 4 april 2019.
- Wet van 15 mei 2024 tot uitvoering van Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724. *Belgisch Staatsblad*, 7 juni 2024, p. 70 980.
- Wet van 22 december 2020 betreffende medische hulpmiddelen. *Belgisch Staatsblad*, 18 januari 2021, p. 2 193.
- Wet van 22 april 2019 inzake de kwaliteitsvolle praktijkvoering in de gezondheidszorg. *Belgisch Staatsblad*, 14 mei 2019, p. 46 372.
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. *Belgisch Staatsblad*, 5 september 2018, p. 68 616.
- Wet van 7 mei 2017 betreffende klinische proeven met geneesmiddelen voor menselijk gebruik. *Belgisch Staatsblad*, 22 mei 2017, p. 58 619.
- Wet van 4 mei 2016 inzake het hergebruik van overheidsinformatie. *Belgisch Staatsblad,* 3 juni 2016, p. 34 148.
- Wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen. *Belgisch Staatsblad*, 13 oktober 2008, p. 54 454.
- Wet van 19 december 2008 inzake het verkrijgen en het gebruik van menselijk lichaamsmateriaal met het oog op de geneeskundige toepassing op de mens of het wetenschappelijk onderzoek. *Belgisch Staatsblad*, 30 december 2008, p. 68 774.
- Wet van 13 december 2006 houdende diverse bepalingen betreffende gezondheid. *Belgisch Staatsblad,* 22 december 2006, p. 73 782.
- Wet van 7 mei 2004 inzake experimenten op de menselijke persoon. *Belgisch Staatsblad*, 18 mei 2004, p. 39 516.
- Wet van 22 augustus 2002 betreffende de rechten van de patiënt. *Belgisch Staatsblad*, 26 september 2002, p. 43 719.
- Bijzondere Wet van 8 augustus 1980 tot Hervorming der Instellingen. *Belgisch Staatsblad*, 15 augustus 1980, p. 23 779.
- KB van 18 mei 2021 betreffende klinische onderzoeken. *Belgisch Staatsblad*, 25 mei 2021, p. 53 283.
- KB van 29 april 2019 tot uitvoering van het Wetboek van vennootschappen en verenigingen. *Belgisch Staatsblad*, 30 april 2019, p. 42 246.
- KB van 29 april 2008 betreffende de samenstelling en werkwijze van de Commissie voor de toegang tot en het hergebruik van bestuursdocumenten. *Belgisch Staatsblad,* 8 mei 2008, p. 24 362.
- KB van 29 oktober 2007 tot bepaling van de behandelingsprocedure en -termijnen voor een aanvraag voor hergebruik van overheidsinformatie alsook het toezicht op de verplichting om bestuursdocumenten beschikbaar te stellen. *Belgisch Staatsblad,* 6 november 2007, p. 56 338.
- KB van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. *Belgisch Staatsblad*, 13 maart 2001, p. 7 839.

- Beroepsinstantie inzake openbaarheid van bestuur en hergebruik van overheidsinformatie. Afdeling hergebruik van overheidsinformatie van 8 oktober 2007. *Belgisch Staatsblad*, 5 november 2007, p. 56 282.

15.1.3 Vlaams

- Decreet van 8 juli 2022 tot oprichting van het platform Vitalink. *Belgisch Staatsblad*, 16 september 2022, p. 67 512.
- Decreet van 26 april 2019 betreffende de organisatie van de eerstelijnszorg, de regionale zorgplatformen en de ondersteuning van de eerstelijnszorgaanbieders. *Belgisch Staatsblad*, 24 mei 2019, p. 50 234.
- Decreet van 13 februari 2019 betreffende de woonzorg. *Belgisch Staatsblad,* 3 mei 2019, p. 43 078.
- Decreet van 18 mei 2018 houdende de Vlaamse sociale bescherming. *Belgisch Staatsblad,* 17 augustus 2018, p. 65 011.
- Decreet van 18 mei 1999 betreffende de centra voor geestelijke gezondheidszorg. *Belgisch Staatsblad*, 17 juni 1999.
- Bestuursdecreet van 7 december 2018. *Belgisch Staatsblad*, 19 december 2018, p. 100 723.
- Besluit van de Vlaamse Regering van 19 juli 2007 betreffende het hergebruik van overheidsinformatie bij de diverse departementen binnen de Vlaamse ministeries en bij de intern verzelfstandigde agentschappen zonder rechtspersoonlijkheid. *Belgisch Staatsblad,* 5 november 2007, p. 56 256.
- Besluit van de Vlaamse Regering van 19 juli 2007 tot oprichting van de beroepsinstantie inzake openbaarheid van bestuur en het hergebruik van overheidsinformatie, *Belgisch Staatsblad,* 5 november 2007, p. 56 257.
- Ministerieel besluit met betrekking tot vastlegging van de modellicentie inzake hergebruik van overheidsinformatie van 8 oktober 2007. *Belgisch Staatsblad,* 5 november 2007, p. 56 277.

15.2 RECHTSPRAAK

15.2.1 Hof van Justitie

- Hof van Justitie van de Europese Unie. (9 november 2024). *Fixtures Marketing Zaak* (C-46/02, ECLI:EU:C:2004:694).
- Hof van Justitie van de Europese Unie. (26 april 2023). *Gemeenschappelijke Afwikkelingsraad (GAR). Europese Toezichthouder voor Gegevensbescherming (EDPS)* (T-557/20, ECLI:EU:T:2023:219).
- Hof van Justitie van de Europese Unie. (4 juli 2023). *Meta/Bunderkartellamt* (C-252/21, ECLI:EU:C:2023:537).
- Hof van Justitie van de Europese Unie. (26 april 2023). *SRB/EDPS* (Zaak T-557/20, ECLI:EU:T:2023:219).
- Hof van Justitie van de Europese Unie. (19 oktober 2016). *Patrick Breyer/Bundesrepublik Deutschland* (Zaak C-582/14, ECLI:EU:C:2016:779).
- Hof van Justitie van de Europese Unie. (9 november 2004). *British Horseracing Board Ltd. V. William Hill Organization Ltd.* (Zaak C-203/02, ECLI:EU:C:2004:695).

15.2.2 Belgisch

- Grondwettelijk Hof nr. 127/2013. van 26 september 2013. *Belgisch Staatsblad*, 21 november 2013, p. 86 503.

15.3 SOFT LAW

- Commissie voor de bescherming van de persoonlijke levenssfeer. (16 januari 2019). *Aanname van de lijst met verwerkingen waarvoor een Gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd conform artikel 35.4 van de Algemene Verordening Gegevensbescherming*. https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&caller=summary&pub_date=19-03-22&numac=2019011184.

- European Data Protection Board (EDPB). (26 november 2024). *Richtsnoeren 1/2024 on processing of personal data based on Article 6(1)(f) GDPR.* https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en.
- European Data Protection Board. (7 juli 2021). *Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*.
- European Data Protection Board (EDPB). (21 april 2020). *Richtsnoeren 3/2020 inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak.* https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_nl.pdf.
- European Data Protection Board. (4 mei 2020). *Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679*. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf.
- European Data Protection Board (EDPB). (23 januari 2019). *Opinion 3/2019 concerning Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art. 70.1.b)).* https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_hu.
- European Union Agency for Cybersecurity (ENISA). (Juni 2023). *Cybersecurity and privacy in AI - Medical imaging diagnosis*, p. 19. https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity%20and%20privacy%20in%20AI%20-%20Medical%20imaging%20diagnosis.pdf.
- Europese Commissie. (24 september 2024). *Implementing the Data Governance Act – guidance document*.
- Europese Commissie. (23 februari 2022). *Commission Staff Working Document on Common European Data Spaces*. https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces.
- Europese Commissie. (29 mei 2019). *Mededeling van de Commissie aan het Europees Parlement en de Raad. Richtsnoeren over de verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie,* COM(2019) 250 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN.
- Europese Commissie. (19 september 2017). *Digital Single Market. Free Flow of non-personal data*. https://digital-strategy.ec.europa.eu/en/library/free-flow-non-personal-data.
- Europese Commissie. (12 december 2012). *Implementation of the PSI Directive in Belgium.* https://digital-strategy.ec.europa.eu/en/news/implementation-psi-directive-belgium.
- Gegevensbeschermingsautoriteit (GBA). (2 oktober 2023). *Advies 133/2018*.
- Gegevensbeschermingsautoriteit (GBA). (25 mei 2020). *Advies nr. 42/2020 betreffende een wetsvoorstel tot oprichting van een databank bij Sciensano in het kader van de strijd tegen de verspreiding van het coronavirus COVID-19*.
- Gegevensbeschermingsautoriteit (GBA). (2019). *Nota over de verwerking van gegevens uit patiëntendossiers*, DOS-2019-04611. https://www.gegevensbeschermingsautoriteit.be/publications/nota-over-de-verwerking-van-gegevens-uit-patientiendossier.pdf.
- Groep Gegevensbescherming Artikel 29 (WP 29). (22 augustus 2018) *Guidelines on Transparency under Regulation 2016/679*.
- Groep Gegevensbescherming Artikel 29 (WP 29). (13 oktober 2017). *Guidelines on Data Protection Impact Assessment (DPIA)*. https://ec.europa.eu/newsroom/article29/items/611236/en.
- Groep Gegevensbescherming Artikel 29 (WP 29). (10 april 2014). *Opinion 05/2014 on Anonymisation Techniques*.
- Groep Gegevensbescherming Artikel 29 (WP 29). (2 april 2013). *Opinion 03/2013 on purpose limitation.*
- Groep Gegevensbescherming Artikel 29 (WP 29). (20 juni 2007). *Advies 4/2007 over het begrip persoonsgegevens*.
- Raad van de Europese Unie. (18 maart 2024). *Proposal for a Regulation on the European Health Data Space – Analysis of the final compromise text with a view to agreement,* 2022/0140(COD). https://www.consilium.europa.eu/en/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/.

- Raadgevend Comité voor Bio-ethiek. (17 november 2003). *Advies 25: Betreffende de bewaartijd van de bloedkaartjes en het vertrouwelijk karakter van de gegevens voor het opsporen van aangeboren metabolische afwijkingen*.
- Sectoraal Comité voor de Sociale Zekerheid en van de Gezondheid, Afdeling "Gezondheid". (17 maart 2015). *Beraadslaging nr. 15/014 betreffende de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen in het kader van de oprichting van een register over cardiale incidenten en het gebruik van de gegevens voor wetenschappelijke doeleinden.*
- Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid, Afdeling "Gezondheid". (15 juli 2014). *Beraadslaging nr. 14/059 met betrekking tot de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen in het kader van het Thales project.*
- World Health Organization (WHO). (28 juni 2021). *Ethics and governance of artificial intelligence for health – WHO Guidance*. https://iris.who.int/bitstream/handle/10665/341996/9789240029200-eng.pdf?sequence=1.
- World Health Association (WMA). (4 juni 2020). *Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks*. https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases- and-biobanks/.
- World Health Association (WMA). (Oktober 2013). *Declaration of Helsinki – Medical research involving human participants*. https://www.wma.net/what-we-do/medical-ethics/declaration-of-helsinki/.

15.4 WEBSITES

- Athumi. (2023). *Het Oprichtingsdecreet*. Opgehaald van Athumi: https://athumi.eu/over-ons/decreet
- Catena-X. https://catena-x.net/en/ [Laatst geraadpleegd op 26/11/2024]
- Data Spaces Radar. https://www.dataspaces-radar.org/radar/ [Laatst geraadpleegd op 26/11/2024]
- Dataspace4health project. https://www.dataspace4health.lu/ [Laatst geraadpleegd op 26/11/2024]
- Data Spaces Support Centre. https://dssc.eu/ [Laatst geraadpleegd op 26/11/2024]
  - DSSC. (2023, September 29). *Core Concepts*. Opgehaald van Data Space Support Centre: https://dssc.eu/space/Glossary/176554052/2.+Core+Concepts.
  - DSSC. (2024, March 19). *Access & Usage Policies Enforcement*. Opgehaald van Data Spaces Support Center: https://dssc.eu/space/BVE/357075567/Access+%26+Usage+Policies+Enforcement.
  - DSSC. (2024, March 11). *Data Spaces Blueprint 1.0*. Opgehaald van Data Spaces Support Center: https://dssc.eu/space/BVE/357073006/Data+Spaces+Blueprint+v1.0
  - DSSC. (2024, March 11). *Organisational and Business Building Blocks*. Opgehaald van Data Space Support Center: https://dssc.eu/space/BBE/178421909/Organisational+and+Business+building+blocks.
  - DSSC. (2024, March 11). *Organisational Form and Governance Authority*. Opgehaald van Data Spaces Support Center: https://dssc.eu/space/BVE/357074549/Organisational+Form+and+Governance+Authority.
  - DSSC. (2024, March 11). *Trust Framework*. Opgehaald van Data Spaces Support Centre: https://dssc.eu/space/BVE/357075461/Trust+Framework.
  - DSSC. (2024, October 11). *Use Case Development*. Opgehaald van Data Spaces Support Center. https://dssc.eu/space/BBE/178422021/Use+Case+Development.
- De Vlaamse Smart Data Space. https://www.vlaanderen.be/digitaal-vlaanderen/onze-oplossingen/vlaamse-smart-data-space [Laatst geraadpleegd op 26/11/2024]
- Digitaal Vlaanderen. (2024). *Afsprakenkader Vlaamse Smart Data Space.* Vlaamse overheid. Opgehaald van Vlaanderen. https://assets.vlaanderen.be/image/upload/v1718364725/Finale_Versie_Ontwerp_Afsprakenkader__VSDS_ckfmfd.pdf [Laatst geraadpleegd op 18/11/2024]
- eHealth. (sd). *Regeling*. Opgehaald van eHealth: https://www.ehealth.fgov.be/ehealthplatform/nl/regeling [Laatst geraadpleegd op 18/11/2024]
- Europese Commissie. https://commission.europa.eu/index_nl [Laatst geraadpleegd 12/12/2024]

  - *Een Europese datastrategie*. https://digital-strategy.ec.europa.eu/nl/policies/strategy-data [Laatst geraadpleegd op 12/12/2024]
  - *Europese datastrategie*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_nl [Laatst geraadpleegd op 12/12/2024]
  - *Common European Data Spaces*. https://digital-strategy.ec.europa.eu/en/policies/data-spaces [Laatst geraadpleegd op 12/12/2024]
  - (24 april 2024). *Questions and Answers on the European Health Data Space*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_2251 [Laatst geraadpleegd op 16/12/2024]
- Europees Parlement. *Legislative Train Schedule – proposal for a regulation on the European Health Data Space*. https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-european-health-data-space.
- European Data Protection Supervisor. *Necessity & Proportionality*.https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en#:~:text=In%20the%20context%20of%20fundamental,disadvantages%20to%20exercise%20the%20right [Laatst geraadpleegd 13/12/2024]
- FOD Economie. (24 maart 2022). *Bescherming van Databanken door Het Auteursrecht*. https://economie.fgov.be/nl/themas/intellectuele-eigendom/intellectuele-eigendomsrechten/auteursrecht-en-naburige/rechtsbescherming-van/bescherming-van-databanken/bescherming-van-databanken#:~:text=Een%20databank%20is%20slechts%20auteursrechtelijk,schepping%2C%20eigen%20aan%20de%20maker [Laatst geraadpleegd 16/12/2024]
- FOD Justitie. *VZW*. https://justitie.belgium.be/nl/themas_en_dossiers/vennootschappen_verenigingen_en_stichtingen/verenigingen/vzw#:~:text=Een%20vereniging%20zonder%20winstoogmerk%20(vzw)%20is%20een%20groep [Laatst geraadpleegd 16/12/2024]
- Gaia-x. https://gaia-x.eu/ [Laatst geraadpleegd op 26/11/2024]
- Go4Fair. https://www.go-fair.org/fair-principles/ [Laatst geraadpleegd op 16/12/2024]
- Health Data Agency. https://www.hda.belgium.be/nl [Laatst geraadpleegd op 26/11/2024]
  - *Onze visie*. https://www.hda.belgium.be/nl/about_us [Laatste geraadpleegd op 13/12/2024]
- HDA data cataloog. https://catalog.hda.belgium.be/ [Laatst geraadpleegd op 26/11/2024]
- HDA financieringsaanvraag. https://www.hda.belgium.be/nl/diensten/financiering-van-innovatieprojecten [Laatst geraadpleegd op 26/11/2024]
- HDA gegevens aanvraag. https://www.hda.belgium.be/nl/data_request [Laatst geraadpleegd op 26/11/2024]
- Health-X project. https://www.health-x.org/home [Laatst geraadpleegd op 26/11/2024]
- Health-X project milestones. https://www.health-x.org/meilensteine [Laatst geraadpleegd op 26/11/2024]
- Health-X project werkpakketten. https://www.health-x.org/arbeitspakete [Laatst geraadpleegd op 26/11/2024]
- Het Vlaams datanutsbedrijf Athumi. https://athumi.be/ [Laatst geraadpleegd op 26/11/2024]
- Innovatrix https://www.imec.be/nl/open-innovatrix-overzicht.
- International Data Space Association. https://internationaldataspaces.org/ [Laatst geraadpleegd op 26/11/2024]
- 26/6/2024: Network of the national library of medicine. https://www.nichd.nih.gov/ [Laatst geraadpleegd op 10/12/2024]
- Qlik Data Sience vs Data Analytics https://www.qlik.com/us/data-analytics/data-science-vs-data-analytics [Laatst geraadpleegd op 16/12/2024]
- SIMPL program. https://simpl-programme.ec.europa.eu/ [Laatst geraadpleegd op 26/11/2024]
- SIMPL programme development dashboard. https://simpl-programme.ec.europa.eu/dashboard/development [Laatst geraadpleegd op 26/11/2024]
- https://doi.org/10.5281/zenodo.12699573.
- 05/09/2024: Statistiek Vlaanderen. https://www.vlaanderen.be/statistiek-vlaanderen [Laatst geraadpleegd op 10/12/2024]

- Van Damme, S. (2023) *Governance models for Solid platform ecosystems* & (2024) *Landscape of Governance for Health Data Sharing.* http://hdl.handle.net/1854/LU-01JE69GX1C47WRMVK06GHK3EN6 & http://hdl.handle.net/1854/LU-01JE69816N8NYMAHFX76T05ZZF.
- Vlaanderen (Vlaamse overheid). *Vitalink, het digitaal platform voor het delen van gezondheidsgegevens*. Vitalink, het digitaal platform voor het delen van gezondheidsgegevens | Vlaanderen.be [Laatst geraadpleegd op 18/12/2024]
- 18 april 2024: Vloca Kennishub (2024) *Geaggregeerde data*. https://vloca-kennishub.vlaanderen.be/Geaggregeerde_data#:~:text=Data%20aggregatie%20is%20een%20proces,beroep%20of%20inkomen%2C%20te%20verkrijgen [Laatst geraadpleegd op 12/12/2024]
- We Are-project. https://we-are-health.be/nl [Laatst geraadpleegd op 26/11/2024]

15.5 BOEKEN

- *Beauchamp, T.L., &Childress, J.F., (2013) Principles of Biomedical Ethics, 7th Edition.*
- *De Bot, D. (2020). De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit. Mechelen, Wolters Kluwer Belgium, 438 e.v.*
- *Decourriere, A. (2020).* Les bases de données*. In* Droits intellectuels : contentieux de la validité et de la contrefaçon *(83e ed., Ser. Pratique du droit, pp. 545-553). Wolters Kluwer Belgium.*
- *Meijers, E.M. (1948). Algemene begrippen van het burgerlijk recht. Leiden: Universitaire Pers.*
- *Van Gerven, D. (2022).* Verenigingen, vennootschappen en stichtingen*. Mechelen: Wolters Kluwer Belgium.*

15.6 ARTIKELS

- Asswad, J., & Marx Gómez, J. (2021). *Data Ownership: A Survey. Information, 12(11), 465*. *https://doi.org/10.3390/info12110465*.
- Baartmans, C., & Steenbruggen, W. (2023). Een Europese Unie voor zorgdata: so close yet so far, *Computerrecht* (NL), 2023(3).
- Biasin, E. (19 mei 2022). The Data Act will concern eHealth apps and Medical Devices. *CiTiP Blog*. https://www.law.kuleuven.be/citip/blog/the-data-act-will-concern-ehealth-apps-and-medical-devices/][Laatst geraadpleegd 9 december 2024]
- Centre for IT & IP. (2 oktober 2023). *White Paper on the Definition of Data Intermediation Services*. https://www.law.kuleuven.be/citip/en/docs/books/citip-white-paper-on-the-definition-of-data.pdf/@@download/file/CiTiP%20White%20Paper%20on%20the%20Definition%20of%20Data%20Intermediation%20Services_2023.pdf.
- Cools, L., (26 november 2024). *Is consent taking priority over legitimate interest under the GDPR?*, https://www.law.kuleuven.be/citip/blog/is-consent-taking-priority-over-legitimate-interest-under-the-gdpr/.
- Ducuing, C., *Data as a Contested Commodity* (15 maart 2024). Available at SSRN: https://ssrn.com/abstract=4767599 or http://dx.doi.org/10.2139/ssrn.4767599.
- Fritzenkötter, J., Hohoff, L., Pierri, P., Verhulst, S. G., Young, A., & Zacharzewski, A. (2022). *Governing the environment-related data space*. https://files.thegovlab.org/erdgovernance.pdf.
- Groos, D., & van Veen, E., (2020). Anonymised Data and the Rule of Law. *European Data Protection Law Review (EDPL),* 4.
- Hallinan, D. (2020). Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sciences, Society and Policy.*
- Hoeyer, K. (2019). Data as promise: Reconfiguring Danish public health through personalized medicine. *Social Studies of Science*, 49(4).
- *Hummel, P., Braun, M., & Dabrock, P. (2020). Own Data? Ethical Reflections on Data Ownership. Philosophy & Technology, (34), 545-572.* https://doi.org/https://doi.org/10.1007/s13347-020-00404-9.

- Lähteenoja, V., Himanen, J., Turpeinen, M., & Signorelli, S. *The landscape of consent management tools - a data altruism perspective*, Publications Office of the European Union, Luxembourg, 2024, doi:10.2760/0852673, JRC137572. https://publications.jrc.ec.europa.eu/repository/handle/JRC137572.
- Tanner, A. (2017). *Our bodies, our data. How companies make billions selling our medical records*. Beacon Press.
- Van Damme, S., Mechant, P., de Mildt, M., Dewaele, S., & Vandercruysse, L. (2024). *Personal Data Stores and Data Cooperatives: a Two-pronged, Sociotechnical Approach for Data Activism. V-Data Final Conference, Abstracts*. Presented at the V-Data Final Conference, Pavia, Italy.
- Vanhooreweder, R. (2024, February 28). *Facilitating Solid Technology: Athumi's Vision and Approach for Data Sharing.* Opgehaald van Solid Community: https://solidcommunity.be/wp-content/uploads/2024/03/20240228-Plenary-Sessions-Rob-Vanhooreweder.pdf.
- Verhenneman, G., & Vedder, A. (30 juni 2015). 'WITDOM "Empowering privacy and security in non-trusted environments", D6.1 - Legal and Ethical framework and privacy and security principles'.

15.7 RAPPORTEN/ADVIEZEN

- Mancini, G.F. (25 oktober 1984). *Conclusie zaak 234/83*, *Gesamthochschule Duisburg v. Hauptzollamt München,* ECLI:EU:C:1984:332.
- *Rapport: De Vlaming leeft gezonder in 2025. Tussentijdse evaluatie van het strategisch plan 'De Vlaming leeft gezonder in 2025'*. https://www.zorg-en-gezondheid.be/sites/default/files/2022-11/Tussentijdsrapport_Gezonderlevenin2025_definitief.pdf [laatst geraadpleegd op 2/12/2024]

15.8 NICE TOT READ

- Bartolomucci, F., & Leoni, F. (2024). Designing an Effective Governance Model for Data Collaboratives. *Research-Technology Management*, *67*(4), 49-61. https://doi.org/10.1080/08956308.2024.2351331
- Gangneux, J. (2023). Deliverable D2.2 Multi-Stakeholder Governance Scheme. https://static1.squarespace.com/static/63718ba2d90d0263d7fc1857/t/6557179174ea0873bd612813/1700206503021/DS4SSCC_D2.2+Mulkti+stakeholder+governance+scheme_FINAL.pdf.
- Huber, T & Kude, T & Dibbern, J. (2017). Governance Practices in Platform Ecosystems: Navigating Tensions Between Cocreated Value and Governance Costs. Information Systems Research. forthcoming. 10.1287/isre.2017.0701.
- Green climate fund (policies and strategies) https://www.greenclimate.fund/about/policies.
- Otto, B., ten Hompel, M., & Wrobel, S. (2022). *Designing data spaces: The ecosystem approach to competitive advantage*. Springer.
- Vermeulen, I. (2024). Symposium report "Big Data for Health & Care: the Arisal of Data Spaces". Zenodo. https://doi.org/10.5281/zenodo.12699218.
- Vermeulen, I. (2024). Workshop report "How to set-up a health data sharing initiative?". Zenodo.
- Verstraete, M/, Verbrugge, S., Colle, D. Solid: Enables of decentralized, digital platforms ecosystems. https://hdl.handle.net/10419/265673.
- Why are we talking about Data Spaces? https://rise.articulate.com/share/gpChBULr0HCHBSJCKcXELOQax7tn9KHs#/lessons/f77WCXxwgzkIu47AvH9OPuL9xZS5axj6.