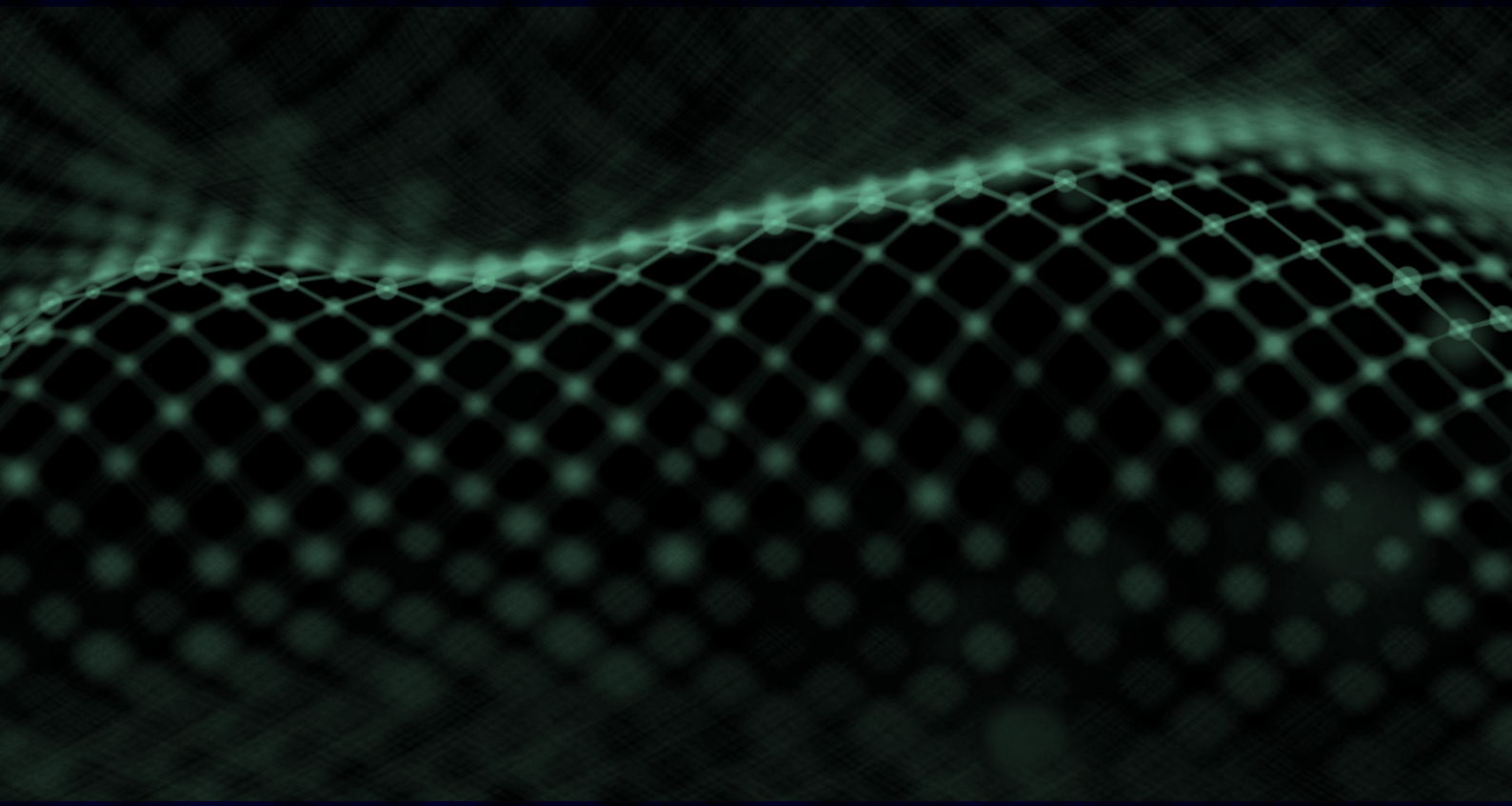
# Verantwoord datadelen voor AI



NL AI Coalitie

Maart 2020

# Voorwoord

De Nederlandse AI Coalitie (NL AIC) is springlevend. Bij schrijven van dit voorwoord (maart 2020) zijn driehonderd organisaties deelnemer van de coalitie geworden. Dat is een prachtig resultaat, maar dit is slechts een begin. Een goede coalitie heeft twee hoofddoelen: samenwerking én resultaat.

Dit rapport is een concreet resultaat van samenwerking in de Werkgroep Data Delen. Het is tot stand gekomen met medewerking van deelnemers van verschillende organisaties in de werkgroep. Dat is niet triviaal want pas wanneer je zaken gaat vastleggen in een rapport word je gedwongen heldere doelstellingen te formuleren, keuzes te maken die collectief worden ondersteund en komt verbinding tot stand tussen deelnemers.

Dit rapport is onderdeel van onze NL AIC propositie waarbij we verantwoord datadelen als basis voor AI-toepassingen gaan realiseren met en voor onze deelnemers. Een onderwerp van groot belang. Data is samen met slimme algoritmes de bouwstenen voor AI-applicaties die ook geacht worden goed en verantwoord te functioneren.

Behalve dit rapport bieden we trainingen en een handleiding hoe te komen tot een implementatie (proof of concept). Daarmee is een kennisbasis beschikbaar. Dit jaar gaan we aan de slag met de toepassing van deze kennis in praktische use cases, die worden aangedragen door de werkgroepen van de NL AIC in toepassingsgebieden. Hierbij vermijden we puntoplossingen maar streven we naar schaalbare oplossingen die breed ingezet kunnen worden.

Dit rapport is tot stand gekomen door samenwerking en met ondersteuning van het Ministerie van Economische Zaken en Klimaat, TNO, en door de actieve deelnemers van de Werkgroep Data Delen bestaande uit bedrijven (groot en klein), universiteiten, overheden en belangenorganisaties die meedenken, meelezen, meeschrijven en vooral meedoen!

**Kees van der Klauw**
*Coalitiemanager Nederlandse AI Coalitie*

**Harrie Bastiaansen**
*TNO*

**Frans van Ette**
*Voorzitter Werkgroep Data Delen*

# Inhoudsopgave

# 1. Introductie

## 1.1. Achtergrond

Deelnemers aan de Nederlandse AI Coalitie (NL AIC [1]) hebben aangegeven dat datadelen een belangrijke voorwaarde is voor het verbeteren van de positie van Nederland. Dat is een logische conclusie: Veel AI toepassingen hebben data nodig om de AI-algoritmes te trainen, te verbeteren en uit te voeren. Het spreekt dus vanzelf dat toegang tot data ogenblikkelijk op het netvlies komt.

Idealiter is data vrij toegankelijk, maar de realiteit is vaak anders. De data houdt zich vaak op bij verschillende organisaties die zelfstandig keuzes maken over wie de data mag gebruiken en waarvoor. Data heeft waarde, en mag daarom soms niet of beperkt gedeeld worden. Er kunnen kosten mee gemoeid zijn met het beschikbaar stellen van de data. Daarnaast zijn er regelgevingsbeperkingen rondom het delen van data, zoals de Algemene Verordening Gegevensbescherming (AVG).

Bezorgdheid over vertrouwen, veiligheid en gebrek aan controle over het gebruik van beschikbaar gestelde gegevens belemmeren momenteel het grootschalig delen van gegevens [2]. Daarmee vertraagt de ontwikkeling en de introductie van nieuwe AI toepassingen, ondanks de grote voordelen die ermee kunnen worden behaald wanneer grotere volumes en verschillende types data beschikbaar alom zouden zijn.

Het is dus zo makkelijk nog niet om AI applicaties te ontwikkelen wanneer daarvoor data uit een veelheid aan bronnen moet komen. Om het delen van data binnen en tussen economische sectoren en de maatschappij te ondersteunen, heeft het Nederlandse ministerie van Economische Zaken en Klimaat daarom onlangs verschillende beleidsrichtlijnen gepubliceerd [3] [4]. In dit beleid wordt de economische waarde van het delen van data geschetst. Tevens wordt het belang van een adequate omgeving voor het delen van data als een belangrijke factor benoemd. Deze beleidsrichtlijnen zijn niet specifiek op de toepassing voor AI gericht, maar desalniettemin daarvoor wel relevant. Ook in het beleid van de EU staan datadelen en AI volop in de belangstelling. Recentelijk heeft de Europese Commissie zowel communicaties over het belang van AI voor Europa [5], een gecoördineerd plan [6] als een white paper over AI voor Europa [7] uitgebracht, tezamen met een communicatie over de Europese data strategie [8].

Doel van de werkgroep 'datadelen' van de NL AIC is om de horde van datadelen ten behoeve van AI zo makkelijk mogelijk te nemen. Een belangrijk uitgangspunt is dat de eigenaren van data controle moeten houden. Het belangrijkste woord daarbij is 'datasoevereiniteit'. Dus geen goed vertrouwen dat het wel in orde komt, maar een verstandig gekozen oplossing die garandeert dat er op verantwoorde wijze met data omgegaan wordt. Tegen voorwaarden die de data eigenaar bepaalt. Daar komt veel bij kijken. Maar heel veel is al mogelijk. Soms moeten lastige keuzes gemaakt worden, maar gegeven de mogelijkheden die AI biedt, is het alleszins de moeite waard.

## 1.2. Bedrijf-strategische belang van datadelen voor AI

Sinds het begin van het digitale tijdperk verschuift de rol van data technologieën binnen organisaties van een functioneel- naar een strategisch niveau. Waar organisaties eerst een IT-afdeling hadden die diensten leverden aan de operationele afdelingen, wordt steeds vaker de algehele strategie bepaald door data en wat de organisatie ermee kan.

Organisaties creëren vooral waarde uit data wanneer die data uit de meest relevante bronnen komt. Dat betekent niet alleen eigen data, maar ook data van buiten de organisatie. Het gaat om data van leveranciers en klanten maar ook van andere partijen waarmee (voorheen) niet werd samengewerkt. Soms zijn dat zelfs concurrenten. Hierbij is het voor de meeste partijen in

de keten duidelijk dat data een kernasset is. Organisaties is er veel aan gelegen om hun eigen waardevolle data te beschermen, terwijl ze zoveel data als mogelijk van anderen trachten te ontsluiten.

De strategische relevantie van datadelen is gegroeid door een leertraject van digitale voorlopers. Vele techreuzen zijn groot geworden door hun vermogen om de meest inzichtrijke data te verzamelen. Ook zij zijn klein begonnen: Bedrijven zoals Amazon gingen eerst efficiëntieslagen maken in bestaande verdienmodellen, zoals het verkopen van boeken. Data-analyse liet toen duidelijk zien waar in de bedrijfsprocessen inefficiëntie optrad en hoe dat beter kon. Inmiddels is min of meer elke industriesector bezig met dit soort verfijning van de bestaande processen.

Deze voorlopers hebben ingezien dat vergaande vormen van data-analyse op basis van (gedeelde) data nieuwe verdienmodellen mogelijk maken. Dit vormde de basis voor innovatieve verdienmodellen, waarbij diensten soms zelfs gratis geleverd worden voor het leveren van relevante data.

Data heeft dus significante waarde en het is zaak om de juiste bronnen aan te boren.

Daarmee komen we tot datadelen tussen organisaties: Met ketenbrede data verbeteren AI-innovaties de nauwkeurigheid van prognoses en verbeteren ze de strategische analyse. Dit ondersteunt de besluitvorming en innovatiekracht om aan veranderende eisen van de eindklant te voldoen. Data gedeeld tussen organisaties, gekoppeld aan het inzetten van AI, stelt organisaties in staat een klantgericht, geïntegreerd bedrijfsmodel te creëren dat meer efficiëntie en flexibiliteit biedt en zichtbaarheid vergroot. Voor alle duidelijkheid, het bedrijfsmodel is hier te definiëren in de meest brede context, dus ook in overheidsdiensten, not for profit's. Het gaat dus om alle aspecten van onze economie en de wijze hoe we onze maatschappij inrichten.

Er is een snelgroeiend aantal voorbeelden van het gebruik van datadelen ten behoeve van AI voor allerlei toepassingen. Het toenemende belang van datadelen is daarbij te zien in hoe AI zich stapsgewijs doorontwikkelt en daarmee nieuwe verdienmodellen of diensten mogelijk maakt [9].

In appendix A word dit strategisch belang vanuit verschillende oogpunten verder beschreven.

In dit document stellen we ons verder niet de vraag wat we willen met AI. AI applicaties worden bedacht met een reden, daar kunnen we vanuit gaan en is daarmee geen onderdeel van dit rapport. Het startpunt is dat datadelen randvoorwaardelijk is om optimaal data bronnen te ontsluiten ten behoeve van de AI applicaties en daarmee de AI-applicaties zo goed mogelijk te laten functioneren.

### 1.3. Datadelen voor NL AIC: rol en context

NL AIC heeft vijf sector-overstijgende thema's geïdentificeerd om ontwikkeling en grootschalige adoptie van AI in Nederland te stimuleren. Deze thema's zijn 'over de sectoren' heen gedefinieerd en worden daarom ook aangeduid als 'horizontals' of bouwstenen. Het thema datadelen is één van deze bouwstenen [1].

Met het vormgeven van de werkgroep 'datadelen' binnen de NL AIC is een community-of-practice gestart die de uitdagingen in datadeel ecosystemen kan aangaan. Daarbij is een belangrijke rol weggelegd voor de werkgroep om een positief klimaat en een governance model vorm te geven om datadelen ten behoeve van AI over organisatiegrenzen heen te faciliteren, binnen Nederland en aansluitend bij internationale ontwikkelingen.

De context hierbij is AI en dat heeft zijn specifieke uitdagingen. Maar datadelen is in allerlei andere terreinen en toepassingen een belangrijk onderwerp. Denk aan het uitwisselen van data ten behoeve van procesoptimalisatie over bedrijfsketens of voor het volgen van producten in een leverings- of productieketen. Er zijn derhalve inmiddels diverse (inter) nationale initiatieven actief op het gebied van datadelen,

waar de werkgroep 'datadelen' van NL AIC bij dient aan te haken.

Een belangrijk initiatief in dat verband is de Nederlandse Data Sharing Coalition (DSC, [10]). Uitgangspunt van DSC is dat we uiteindelijk toe moeten naar cross-sectoraal datadelen. Dus niet alleen het regelen tussen een paar organisaties voor een specifieke toepassing, maar het zo inrichten dat datadelen generiek gemaakt wordt. Dat is een uitgangspunt waar ook NL AIC leden veel aan zullen hebben. Zodra de oplossingen die gebouwd worden in NL AIC verband makkelijker herbruikbaar zijn, dalen de kosten van bouw, implementatie en beheer. Samenwerking tussen NL AIC en DSC is dus voor beide initiatieven en de betrokken deelnemers van groot belang.

Een tweede belangrijke powerhouse van datadelen is het dataregister van de Nederlandse overheid [11]. Georganiseerd door het Ministerie van Binnenlandse Zaken is dit portal de basis van toegang tot data vanuit de overheid. Op het portal is veel informatie al beschikbaar. Er is een team beschikbaar dat helpt bij de mogelijkheden die er zijn en er wordt meegedacht in de problematiek om tot goede oplossingen te komen. Uiteindelijk kan dat leiden tot datadeals tussen betrokken partijen waar datadelen wordt gerealiseerd. Deze aanpak is een prachtig entree voor NL AIC leden in de beschikbaarheid van data uit overheidsdomeinen.

Dit zijn twee belangrijke voorbeelden, maar er gebeurt veel meer in Nederland, zeker ook op regionaal en sectoraal niveau. Dat is goed en tegelijkertijd is dit initiatief van NL AIC daarbij een mooie aanleiding om de verbinding te zoeken en samen te bouwen. Zo leren de verschillende initiatieven van elkaar en kunnen gezamenlijk werken samenhang en afstemming.

Naast Nederlandse initiatieven gebeurt er internationaal ook heel veel. Zo heeft Duitsland eind 2019 het GAIA-X initiatief gestart [12], waar een Europees antwoord wordt gegeven op de grote platformen uit de VS en wijze waarop Aziatische (vaak Chinese) IT systemen worden ontwikkeld en geëxploiteerd. Toegang tot data speelt daarbij een cruciale rol. Reden waarom in EU verband veel initiatieven worden ontplooid en wordt geïnvesteerd in oplossingen waar privacy-by-design en datasoevereiniteit als basis principes worden gehanteerd.

## 1.4. Gecontroleerd datadelen ten behoeve van AI

Organisaties zien steeds meer dat data een economisch bezit of een maatschappelijk belang vertegenwoordigt. Het delen van data met andere partijen brengt mogelijkheden voor innovaties, nieuwe vormen van samenwerking, veranderende businessmodellen en nieuwe manieren om de maatschappij in te richten. Daarmee is datadelen een groots (wellicht wat ongezien) gezamenlijk infrastructureel project geworden. Van groot belang voor het verdienvermogen van Nederland, voor maatschappelijke ontwikkelingen, voor hoe mensen en organisaties regie houden of juist weer krijgen.

Daarbij is in toenemende mate de behoefte ontstaan om grip te krijgen op (de voorwaarden voor) het gebruik van data wanneer het gedeeld wordt met andere partijen. We willen dus wel datadelen, maar misbruik van data dient te worden voorkomen om organisaties en personen het vertrouwen te geven hun gevoelige data te delen. Startpunt is 'daarom *gecontroleerd datadelen'*. Het gecontroleerd datadelen is uit te splitsen in drie aspecten:

- *Datasoevereiniteit ('data sovereignty')* is het vermogen van een natuurlijke persoon of organisatie om volledig zelfbepalend te zijn met betrekking tot zijn data, d.w.z. de mogelijkheid voor een rechtspersoon om exclusief te beslissen over het gebruik van zijn data als een economisch bezit. Het vereist dat mensen en organisaties controle hebben over de omstandigheden over hoe hun data wordt gedeeld en hoe deze door andere partijen mogen worden verwerkt.

- *Vertrouwen ('trust')* is de eigenschap zekerheid te krijgen dat de entiteiten (personen, organisaties of systemen) waarmee data wordt gedeeld, daadwerkelijk de entiteiten zijn die zij beweren te zijn en dat zij dienovereenkomstig zullen handelen. Vertrouwen kan worden gerealiseerd door middel van adequate identificatie, authenticatie- en certificeringsmethodes.
- *Veiligheid ('security')* is de eigenschap te kunnen garanderen dat het daadwerkelijk delen van data is beveiligd tegen ongeautoriseerd misbruik van deze data door beveiligingsinbreuken, zowel ten gevolge van kwaadwillige opzet of per ongeluk. Het omvat aspecten zoals gecodeerd datatransport en opslag en software certificering en attestatie.

Gecontroleerd datadelen is een multidisciplinair proces waarbij niet alleen technologie wordt ingeschakeld, maar ook zakelijke en juridische overwegingen en afspraken een rol spelen [13].

Het gecontroleerd delen van data ten behoeve van AI heeft grote gelijkenis met het delen van data ten behoeve van andere toepassingen, bijvoorbeeld het delen van transactie en operationele data om de effectiviteit en efficiëntie van supply chain-processen te verbeteren. Maar er is ook een aantal kenmerken dat maakt dat sommige aspecten van datadelen anders, belangrijker of complexer worden. Deze worden beschreven in het volgende hoofdstuk.

Voor management van en verantwoording over wetenschappelijke data zijn daarbij de FAIR principes [14] relevant. De FAIR principes zijn gericht op de vindbaarheid ('Findability), toegankelijkheid ('Accessibility'), interoperabiliteit (Ínteroperability) en hergebruik ('Reuse') van wetenschappelijke data.

## 1.5. Rapportage: doelgroep, doelen en structuur

Dit rapport is opgesteld door de werkgroep 'datadelen' ten behoeve van alle deelnemers aan de NL AIC die voor hun AI applicaties gezamenlijk data willen delen.

De doelen van dit rapport zijn:

1. Aangeven wat datadelen ten behoeve van AI-toepassing specifiek maakt in vergelijking met datadelen voor andere toepassingen en welke uitdagingen daarbij naar voren komen. Dit doel wordt geadresseerd in hoofdstuk 2.
2. De aanpak van datadelen ten behoeve van AI, voortbouwend op visies, raamwerken en technologieën die al in verschillende contexten zijn opgesteld. Dit doel wordt geadresseerd in hoofdstuk 3.
3. Het vervolgtraject vanuit de huidige 'IST' situatie naar de toekomstige 'SOLL' te beschrijven, als proces van first-time-engineering naar operationalisatie. Dit doel wordt geadresseerd in hoofdstuk 4.

In aanvulling hierop bevat dit rapport de volgende appendices waarin een aantal relevante aspecten (die in de hoofdrapportage alleen op hoofdlijn worden benoemd) in meer detail worden omschreven:

- Appendix A '*Business relevantie en digitale transformatie*' adresseert het belang en de business-mogelijkheden van datadelen ten behoeve van AI, samen met opties voor organisaties om deze in hun bedrijfsvoering in te passen.
- Appendix B: '*Samenwerkingsmodellen: data, algoritme en resultaat*' beschrijft de opties en afwegingen over in welk domein de AI-algoritmes worden uitgevoerd; gaat de data naar het AI-algoritme of vice versa. Dit karakteriseert het type van data dat tussen partijen wordt gedeeld en daarmee of en hoe deze moet worden beschermd.
- Appendix C: '*Juridisch kader*' beschouwt twee belangrijk aspecten van het juridisch kader (wettelijke regime) voor datadelen ten behoeve van AI: de wettelijke bepalingen voor het delen van persoonlijke data en de wettelijke eisen aan en onderdelen van de datadeel overeenkomsten waarin de juridische, commerciële en gebruiksvoorwaarden worden vastgelegd.

- Appendix D: *'Technieken voor datadelen'* geeft een overzicht van (technische) ontwikkelingen die relevant zijn voor het vormgeven van infrastructuren voor gecontroleerd datadelen. Dit omvat zowel overkoepelende architecturen voor datadelen als beveiligingstechnieken voor data integriteit.

# 2. Datadelen ten behoeve van AI

Een aantal kenmerken van (gecontroleerd) datadelen ten behoeve van AI is anders, belangrijker of complexer dan bij datadelen voor andere toepassingen. Bij andere toepassingen kan gedacht worden aan bijvoorbeeld het delen van transactie en operationele data ten behoeve van procesoptimalisatie over bedrijfsketens of voor het volgen van producten in een leverings- of productieketen. Dat specifieke voor AI moeten we verder definiëren om daar uiteindelijk in het vervolg en richting implementaties goed rekening mee te kunnen houden.

De AI-specifieke kenmerken van datadelen worden in de achtereenvolgende secties van dit hoofdstuk uitgewerkt: de typering van data voor AI-systemen en de eigenschappen van datadelen voor AI.

## 2.1. Typering data voor AI-systemen

Er zijn verschillende types van AI-systemen, elk met hun eigen behoefte aan data die gedeeld dient te worden. In deze sectie worden twee hoofdsoorten onderscheiden: datagestuurde en kennisgestuurde AI-systemen. Hun gemeenschappelijke component is dat intelligentie of kennis in het AI-systeem gebracht wordt om een complexe taak uit te kunnen voeren. Het verschil zit in de manier waarop die intelligentie of kennis verkregen wordt.

Datagestuurde AI-systemen vinden door middel van statistische en machine learning methoden automatisch kennis, bijvoorbeeld over de te nemen beslisstappen. Veelal gebeurt dat op basis van historische gegevens, die als trainingsdata de relatie tussen eigenschappen van datasubjecten en de daaruit volgende 'conclusie' in zich herbergen. In een eenvoudig geval vindt een machine learning methode de relatie tussen een beperkt aantal soorten gegevens, bijvoorbeeld op basis van eenvoudige lineaire correlaties. Geavanceerde machine learning methoden betrekken veel meer gegevens en staan complexere relaties toe. Het resultaat is een model, dat informatie uit de trainingsdata samenvat in een beperkt aantal parameters (modeldata).

Bij kennisgestuurde AI-systemen is de kennis verkregen door raadpleging van domeinexperts. Het verkrijgen van expertkennis heet kenniselicitatie, waarvoor vele methoden bestaan, zoals interviewen, case-study en rollenspel. De kennis kan op verschillende manieren verkregen en uitgedrukt worden: van 'als-dan' regels tot wiskundige functies. Om kennisgestuurde AI mogelijk te maken is het nodig dat de gedeelde data uitgedrukt is op een manier die aansluit bij de opgehaalde expertkennis. Bij het delen van data moeten daarom eisen omtrent betekenis van data goed beschreven en vastgelegd worden in taxonomieën en ontologieën: de vooraf overeengekomen woordenboeken van begrippen en de mogelijke relaties daartussen.

Bij de realisatie van de datagestuurde en kennisgestuurde AI-systemen spelen verschillende typen data een rol, zowel in de ontwikkelfase als in de operationele fase van het AI-systeem:

- *Trainingsdata:* Datagestuurde AI-systemen maken gebruik van historische data om goed ingeregeld te worden: dat proces wordt 'trainen' of 'leren' genoemd en de gebruikte data zijn de trainingsdata.
- *Modeldata:* Het trainen of inregelen van een AI-systeem op basis van trainingsdata resulteert in een model met een aantal geleerde parameters. Dit tezamen zijn de modeldata.
- *Kennisdata:* In het geval van een kennisgestuurd AI-systeem is de verzamelde kennis ook als data op te vatten.
- *Productiedata:* Productiedata zijn de data die actueel verwerkt worden door het AI-systeem, en waar een analyse op gedaan wordt ten behoeve van een beslissing of voorspelling. Zowel kennis- als

datagestuurde systemen verwerken productiedata.

## 2.2. Eigenschappen datadelen voor AI

Zoals eerder benoemd heeft datadelen ten behoeve van AI-toepassingen een aantal specifieke aspecten, welke in de achtereenvolgende paragrafen van deze sectie worden benoemd.

### *2.2.1. Domein van verwerking: samenwerkingsmodellen*

Door hun vermogen om complexe verbanden af te kunnen leiden zijn AI-systemen bij uitstek geschikt om veel verschillende databronnen tegelijk te analyseren. Ook hebben sommige AI-systemen het kenmerk dat ze met heel grote hoeveelheden data het beste werken, bijvoorbeeld bij deep learning.

De verschillende databronnen voor AI-systemen kunnen niet altijd eenvoudigweg samengebracht worden. Enerzijds kan het zijn dat de hoeveelheden data daarvoor te groot zijn, anderzijds kunnen er redenen van vertrouwelijkheid zijn die het nodig maken dat de data bij de eigenaar of beheerder moeten blijven en dus niet overgedragen mogen worden. Denk daarbij aan privacy beperkingen volgend uit de AVG of wegens bedrijfsvertrouwelijkheid.

Kortom, om verschillende redenen kan het wenselijk zijn dat AI-systemen gedistribueerd zijn: de data staat in het domein van verschillende organisaties en op verschillende plaatsen en het AI-systeem moet in staat gesteld worden om daaruit het model te trainen.

De uitdaging hierbij is dat vrijwel alle bestaande datagestuurde AI-algoritmen momenteel vereisen dat de data in één database of dataset beschikbaar zijn. Desalniettemin komen de technieken beschikbaar om gedistribueerde AI-systemen te ontwerpen waarbij de ontwerpkeuze ontstaat om de databronnen niet bij elkaar te brengen. Een voorbeeld van typen algoritmen die in staat zijn om uit verdeelde databases te leren zijn federated learning algoritmen. Daarnaast biedt ook (secure) Multi-Party Computation mogelijkheden voor het realiseren van gedistribueerde AI-systemen. We noemen het hier kort; verderop in dit rapport volgt meer uitleg.

Voor het domein van verwerking in de *trainingsfase* zijn er drie basisopties (de 'samenwerkingsmodellen'):

- *Analysis-to-Data:* Het AI-systeem wordt naar de databron gestuurd en wordt daar uitgevoerd. In veel gevallen volgen een aantal iteraties, waarin het algoritme deel oplossingen uitwisselt en uiteindelijk convergeert naar een eindoplossing van het model.
- *Data-to-Analysis*: De data wordt naar het AI-systeem gestuurd en daar verwerkt, samen met data van andere bronnen. In deze vorm kan een centrale dataset gevormd worden, waardoor vele standaard AI-algoritmen toepasbaar zijn.
- *Data-and-Analysis-to-Lake*: Alle data wordt centraal bij een vertrouwde derde partij (Trusted Third Party: TTP) verzameld (een 'data lake'). Ook het AI-systeem wordt naar die derde partij gestuurd. Het trainen vindt vervolgens dáár plaats, en het systeem communiceert de modeleigenschappen terug. Ook in dit samenwerkingsmodel zijn de standaard AI-algoritmen toepasbaar.

In appendix B worden deze basis samenwerkings-modellen verder beschreven.

Er wordt opgemerkt dat de informatie in het AI-model in meer of mindere mate sporen van de trainingsdata kan bevatten. Als die trainingsdata vertrouwelijk zijn, is dat mogelijk een probleem. Daarom is het distribueren van het AI-systeem op te vatten als het delen van data, waarvoor methodes voor het gecontroleerd datadelen relevant zijn.

De *productiefase* stelt minder hoge eisen aan de locatie van de gegevens. In deze fase worden databronnen in principe individueel benaderd. Het ligt dan voor de hand om het samenwerkingsmodel 'Analysis-to-Data' toe te passen, waarbij de resultaten vervolgens

teruggevoerd worden naar het AI systeem. Verder is van belang dat in deze fase ook modeldata en/of kennisdata gedeeld worden. Deze data kan nog steeds gevoelig zijn, hetgeen het toepassen van een maatregel voor gecontroleerd datadelen nodig maakt.

Het bepalen van het domein van verwerking door middel van een geschikt samenwerkingsmodel heeft gevolg voor de te nemen maatregelen om data te beschermen. Het samenwerkingsmodel definieert de rollen van de betrokken partijen: wie levert data aan, wie verwerkt die data middels het AI-systeem, wie gebruikt die data, waar en wanneer wordt data tussen organisaties overgedragen? Voor elk van de organisatieovergangen dienen adequate maatregelen voor het beschermen van de gedeelde data te worden ingericht

### *2.2.2. Datasoevereiniteit: consent management en autorisaties*

Voor organisaties is datasoevereiniteit een belangrijk uitgangspunt voor het delen van hun gevoelige data. Datasoevereiniteit houdt in dat de rechthebbende zelf bepaalt met wie en voor wat voor doeleinden de data gedeeld wordt. Dit wordt vormgegeven in een autorisatiearchitectuur. Deze bepaalt wie toegang tot welke data toegang krijgt met wat voor doel, i.e. 'consent management'.

De autorisatiearchitectuur voor AI-toepassingen dient aan een aantal AI-specifieke datadeel kenmerken tegemoet te komen:

- In veel gevallen zal de data van de data aanbieder als bron voor de AI-systemen niet op de locatie en in de systemen van de data aanbieder zelf beschikbaar zijn. Bijvoorbeeld thermostaat data wordt verzonden naar de energieleverancier en wordt daar in de systemen opgeslagen. Dit vereist dat de autorisatiearchitectuur het mogelijk moet maken om gedelegeerde machtigingen en autorisaties in te richten.
- Met verwerking door een AI-systeem wordt uit de brondata nieuwe informatie gegenereerd, welke vervolgens weer met een andere partijen kan worden gedeeld. Daarbij ontstaat de vraag of de oorspronkelijke data aanbieder ook op deze nieuwe data grip dient te willen of moet uitoefenen, waarmee de autorisatiearchitectuur de vereiste machtigingen dient te prolifereren in de verwerkingsketen.
- Bij het toepassen van de verschillende basis samenwerkingsmodellen, zoals beschreven in de vorige paragraaf, worden verschillende types data op verschillende plaatsen in de keten gedeeld tussen onafhankelijke organisaties. De autorisatiearchitectuur moet op adequate wijze met deze verschillende samenwerkingsmodellen om kunnen gaan.

In het 'Analysis-to-Data' samenwerkingsmodel wordt het AI-systeem uitgevoerd in het domein van de data aanbieder. In dit geval bepaalt de data aanbieder zelf of het AI-systeem toestemming krijgt om met zijn data te werken en op welke manier. Dat soevereiniteit heeft dan betrekking op het AI-systeem. Er moet vastgesteld kunnen worden of het AI-systeem daadwerkelijk is wie het zegt dat het is (vertrouwen) én de data aanbieder moet kunnen zien wat het systeem met zijn data gaat doen (veiligheid). Deze aanpak is onder andere in de 'Personal Health Train' [15] uitgewerkt waarbij het AI-systeem getraind wordt op medische gegevens van patiënten. Het algoritme 'reist' daarbij langs de verschillende ziekenhuizen, die niet willen dat hun data hun organisatie verlaat.

### *2.2.3. Vertrouwen in het AI-systeem en dataverwerking*

Naast datasoevereiniteit is vertrouwen in het AI-systeem van groot belang voor de bereidheid van organisaties om er data mee te willen delen. Ook dit kent een aantal verschillende aspecten:

- *Transparantie:* Soms is het voldoende om te laten zien hoe het AI-systeem werkt (welke stappen en berekeningen er gedaan worden: het algoritme),

maar transparantie en inzicht in de werking is pas compleet als ook de instellingen (de manier waarop de machine learning op de trainingsdata ingeregeld is: het model) bekend zijn. Ook als de trainingsdata van een systeem niet beschikbaar zijn, kan dat het vertrouwen in het AI-systeem ondermijnen.

- *Bias, discriminatie en proxies:* Om datagestuurde AI mogelijk te maken is het nodig trainingsdata beschikbaar te hebben die zo volledig mogelijk de benodigde informatie en kennis afdekt. Of, in andere woorden, de trainingsdata moet representatief zijn voor alle datasubjecten waar het AI systeem uitspraken over zal moeten doen. Dit lijkt misschien eenvoudig, maar is een van de grote uitdagingen, zeker als het over data van mensen of groepen van mensen gaat. Zo kunnen historische, maatschappelijke processen tot gevolg hebben dat etnische groepen onterecht onder- of oververtegenwoordigd zijn in de trainingsdata, zoals van autocontroles op openbare wegen. We spreken dan van bias en discriminatie. In het voorbeeld van een AI systeem voor de klimaatregeling van gebouwen zal dat wellicht wat vergezocht zijn (alhoewel de verschillende temperatuurgevoeligheid van mannen en vrouwen nog een interessante discussie kan opleveren), maar voorbeelden uit de strafrechtketen zijn inmiddels berucht [16].

  Om discriminatie en bias te voorkomen of in ieder geval te beperken schrijft de AVG voor dat bepaalde persoonsgegevens niet gebruikt mogen worden zonder geldig doel. Denk bijvoorbeeld aan het geslacht voor werving- en selectietoepassingen. Bij het datadelen moet hier rekening mee gehouden worden. Door de kracht van AI-algoritmes is het echter niet genoeg om deze attributen uit de database niet te delen. AI-algoritmes zijn in staat uit andere gegevens, zoals gewenste aantal werkuren, alsnog informatie over het geslacht van de sollicitant te achterhalen. De mogelijkheid om methodieken te ontwikkelen voor deze specifieke randvoorwaarden vergt extra aandacht.

- *Datakwaliteit:* Kwaliteitsbewaking voor data in AI-systemen is extra belangrijk onder meer omdat AI data uit verschillende bronnen verwerkt wordt waarvan de kwaliteit verschillend kan zijn. Een andere reden is dat de output van AI-systemen vaak door weer andere systemen verwerkt wordt waardoor sneeuwbaleffecten kunnen ontstaan. Ook is er het risico dat de mens de output van (ketens van) AI-systemen zonder veel kritische reflectie overneemt. Grip op datakwaliteit kan worden verkregen door monitoren vanuit het gezichtspunt van zelfbescherming (het voorkomen dat de data aanbieder zelf echt slechte data gaat opleveren), of vanuit het gezichtspunt van contract bewaking (het voorkomen dat de kwaliteit van de resulterende data buiten de gemaakte afspraken met de afnemer komt te liggen). Het monitoren van datakwaliteit kan zowel op de input als op de output van het AI-systeem. Extra aandachtspunt is dat de output van AI-systemen meestal onzekerheden in zich dragen. Hoe die onzekerheden een plaats te geven in de opvolgende verwerkingen is geen uitgemaakte zaak.

### *2.2.4. Conformiteit en compliance*

Bij het delen van data met AI-systemen, kunnen door data aanbieders voorwaarden over toegang en gebruik van de data afgesproken en opgelegd worden. Door het AI-systeem dient daarbij verantwoording afgelegd te worden aan de data aanbieders dat men zich bij de verwerking van de data geconformeerd heeft aan deze afspraken. Indien voor het datadelen door de aanbieder is gekozen om gebruik te maken van generieke van derde partijen afgenomen diensten voor het registreren en afdwingen van autorisaties (consent management), dan dient aangesloten te worden bij de koppelvlakken en informatiemodellen die hiervoor beschikbaar gesteld worden. Speciale aandacht gaat daarbij ook naar de potentiele vertrouwelijkheid van de data die in de ondersteunende processen gegenereerd wordt (de 'metadata'), waarover de data aanbieder controle wenst te houden en waarover de verwerker verantwoording

dient af te leggen [17].

Het is daarbij essentieel om te kunnen reageren op vragen en klachten over de geleverde AI-diensten en producten. Hiervoor moet je precies kunnen achterhalen hoe het geleverde tot stand is gekomen en op basis van welke data (i.e. 'traceerbaarheid'). Dit kan gaan van transparantie informatie welke high level inzicht geeft, via een detail beschrijving van alle data, AI modellen en configuraties, tot aan het (automatisch) kunnen reproduceren van het geleverde resultaat. Traceerbaarheid is belangrijk voor de accountability van een systeem (ben je in staat om vast te stellen welke delen van het systeem wat gedaan hebben en wie eventueel verantwoordelijk is) en heeft dus vooral met vertrouwen te maken.

Naast kenmerken van datadelen ten behoeve van AI zelf, zijn er ook wettelijke redenen waarom toepassing van AI in de context van datadelen speciaal is. Zo wordt in de AVG ingegaan op geautomatiseerde besluitvorming. In zulke gevallen is transparantie vereist. Vaak zal die besluitvorming een vorm van AI gebruiken. Daarom is transparantie een aspect van datadelen dat voor AI extra belangrijk is.

De AVG stelt ook eisen aan het verwerken en delen van persoonsgegevens, wat met name impact heeft op het werken met (centrale) trainingsdata. En vanzelfsprekend is discriminatie ethisch en wettelijk zelden toegestaan, zoals aangegeven onder het aspect '*Bias, discriminatie en proxies*' in de vorige paragraaf: Nogmaals, voor AI-systemen is het niet voldoende de discriminatoire gegevens niet te delen, wegens de vaak aanwezige proxies voor die gegevens.

Ook is het uitgangspunt van 'doelbinding' van toepassing. Dit omhelst het principe dat de verwerkende organisatie en het AI-algoritme alleen de data mag vragen, gebruiken en de (resultaten ervan) delen ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, waarvoor toestemming door de data aanbieder is verleend.

Daarnaast dient de privacy afdwingbaar te zijn. Bij het geven van consent en in de autorisatiearchitectuur dient het voor de data aanbieder mogelijk te zijn aan te geven voor welk doel zijn gegevens ter beschikking worden gesteld en of anonimiteit bij de verdere verwerking en verspreiding van zijn gegevens gegarandeerd zijn.

# 3. Aanpak: voortbouwen op visies en raamwerken

Zoals aangegeven in sectie 1.3, staat het onderwerp datadelen vanuit verschillende oogpunten momenteel volop in de aandacht. Dat betekent ook dat er inmiddels visies en raamwerken zijn opgesteld over de manier waarop het onderwerp datadelen kan worden aangepakt. Hierop kan (en moet) de NL AIC werkgroep datadelen voortbouwen.

De secties in dit hoofdstuk beschrijven een aantal van deze visies en raamwerken waarop wordt voortgebouwd. Deze vormen input van het ontwikkeltraject zoals in het volgende hoofdstuk wordt uitgewerkt.

## 3.1. Uitdagingen aan datadelen ten behoeve van AI

De Big Data Value Association (BDVA) is een vereniging van onderzoeksinstellingen gericht op data-onderzoek en ontwikkeling in Europa. Datadelen is vanzelfsprekend een belangrijk onderwerp voor deze groep. In reactie op de mededeling van de Europese Commissie [18] heeft de BDVA een position paper uitgebracht [19] waarin vanuit het perspectief van de gebruikers de belangrijkste technische uitdagingen rondom datadelen benoemd worden. Deze uitdagingen komen voort uit de ambitie "*to realise a cross-border, cross-sectoral sharing data space and enable platforms to process 'mixed' proprietary, personal and open public data introduces new technical challenges*". De uitdagingen gaan niet alleen over de data zelf, maar ook over de metadata, de modellen en algoritmen die erop werken. Alhoewel deze uitdagingen niet specifiek voor AI zijn geformuleerd, zijn ze wel allemaal in meer of mindere mate van belang voor AI. De uitdagingen zijn, naar AI doorvertaald, weergegeven in Tabel 1.

De Strategic Research Innovation & Deployment Agenda (SRIDA, [20]) die door de BDVA en euRobotics is opgesteld identificeert de belangrijkste uitdagingen die in EU-verband moeten worden opgepakt. De bijbehorende voorgestelde acties zijn, vrij vertaald:

- Creëer de condities voor de ontwikkeling van vertrouwde Europese datadeel raamwerken, waarbij op bestaande initiatieven voortgebouwd moet worden (data platformen, i-spaces, big data innovation hubs). Het gaat om veschillende types data: persoonlijke, niet-persoonlijke, open, gesloten en proprietary data.
- Bevorder het gebruik van open datasets en open benchmarks voor AI-algoritmes, met name voor validatie van kwaliteit vanuit software engineering en functioneel gezichtspunt.
- Bepaal specifieke maatregelen om het delen van gegevens op te nemen in de kern van de data life cycle management voor betere toegang tot gegevens, waardoor samenwerking tussen actoren van de dataketen in beide richtingen langs de keten en in verschillende sectoren wordt aangemoedigd.
- Zorg voor ondersteunende maatregelen voor Europese bedrijven om veilig nieuwe technologieën, werkwijzen en beleidsmaatregelen te implementeren.
- Coördineer en harmoniseer de inspanningen van de lidstaten en realiseer het potentieel van Europese digitale AI-diensten in het licht van wereldwijde concurrentie.
- Leid en beïnvloed standaarden met betrekking tot tools voor het delen van gegevens, behoud van privacy, kwaliteitscontrole, samenwerking en interactie.
- Bevorder standaardisatie op Europees niveau, maar blijf samenwerken met internationale initiatieven voor AI die wereldwijd worden gemaakt.

| *Uitdaging* | *Relevantie voor AI* |
|---|---|
| **Betrouwbaarheid van data en kwaliteit van AI** | Omdat AI 'dieper' in besluitvorming wordt toegepast is betrouwbaarheid nog belangrijker dan bij 'gewoon' datadelen. Validatie van (herkomst van) data is belangrijk. Ook bias, met name in trainings-datasets, hoort hierbij. |
| **Bescherming van gevoelige data, privacy** | Omdat AI meer informatie uit data kan halen (ook impliciete gevoelige informatie) is het goed omgaan met gevoeligheid en privacy nog belangrijker. |
| **Soevereiniteit, eigenaarschap van data** | Zowel bedrijven als individuen 'leveren' data en gezien de grotere mogelijkheden die AI levert om hier waarde uit te halen, wordt het belang van soevereiniteit onder AI alleen maar groter. Veilige toegangscontrole is van groot belang, zeker bij gedecentraliseerde verwerking. Daarnaast zal AI data uit verschillende bronnen (kunnen) verwerken. |
| **Data life-cycle management** | Deze is niet ontworpen voor delen. Daarom is het extra belangrijk om aandacht te geven aan de volwassenheid van datadiensten (cleaning, aggregatie).<br><br>Het onderscheid in 'training' en 'productie' is daarbij voor data life-cycle management van groot belang. Voor de kwaliteit van AI-systemen is het van groot belang dat deze niet getraind zijn op data die inmiddels verouderd is. |
| **Open data** | Open data levert voor AI kansen omdat veel AI-algoritmen taken moeten vervullen waarvoor veel data nodig is (denk aan imagenet voor het trainen van beeldherkenning) maar is ook een mogelijke bedreiging omdat het re-identificeren van geanonimiseerde datasets ermee mogelijk wordt. |
| **Verificatie en provenance** | De betrouwbaarheid van de data zelf en het kennen van de oorsprong ervan is belangrijk voor betrouwbare uitkomsten, maar heeft ook een aansprakelijkheids-component. |
| **Gedecentraliseerde verwerking, toegang tot data** | Architecturen om AI te leren op gedistribueerde data, waarbij toegang tot data nog belangrijker is vanwege de 'datahonger' van veel AI-algoritmen. Privacy, bandbreedte en omvang van data spelen een rol bij de afweging rondom gedecentraliseerde verwerking. Dit aspect wordt verder geadresseerd in appendix B. |
| **Datadeel raamwerken, Europese en internationale afstemming** | Afsprakenstelsels die ook onderling en in gezamenlijkheid de juiste doelen nastreven zijn extra belangrijk voor AI, nu er nadrukkelijk wordt gesproken over een 'Europese' versie van AI die verschilt van 'kapitalistische' AI (VS) of 'totalitaire' AI (China). |
| **Interoperabiliteit** | Omdat AI niet alleen maar datagestuurd is, maar ook kennisgestuurd, is de semantiek van data belangrijker dan bij 'gewone' dataverwerking; interoperabiliteit is de basis voor goede semantiek. |

Tabel 1: Uitdagingen aan datadelen voor AI

## 3.2. Van een (gesloten) hub-model naar een (open) netwerk-model

Het denken over datadelen heeft zich ontwikkeld. Concepten als datasoevereiniteit krijgen meer aandacht. Dit leidt er toe dat het model waarbinnen data gedeeld wordt veranderd is.

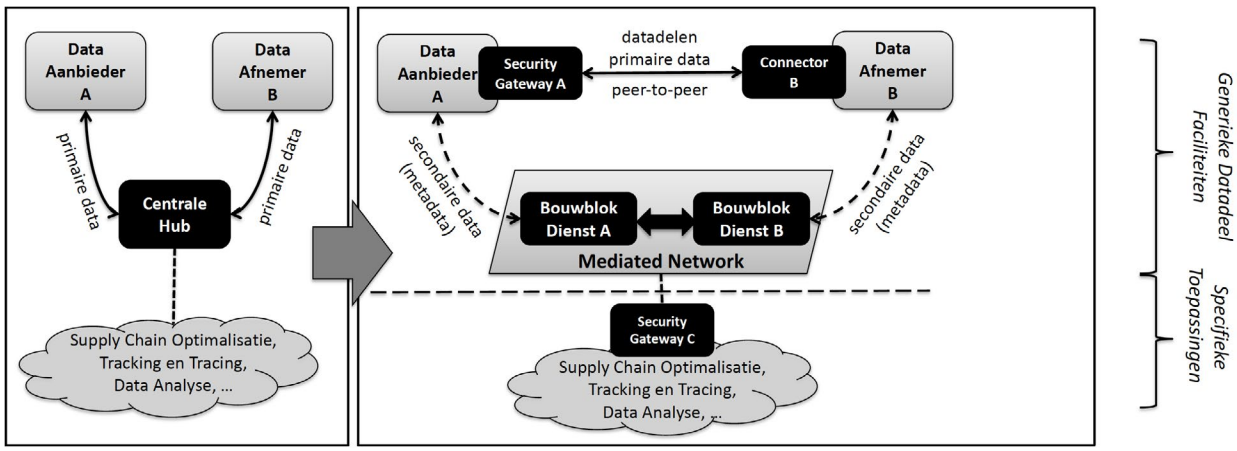
Datasoevereiniteit is een essentiële voorwaarde voor data aanbieders (eigenaren) om hun potentieel gevoelige data te delen. Vanuit het perspectief van de aanbieders is het delen van zijn data van toepassing op een mogelijk groot aantal data ontvangers waarmee hij zijn gegevens zou willen delen. Dit geeft hen echter een grote uitdaging, aangezien de concepten voor betrouwbaar datadelen momenteel voornamelijk worden aangeboden vanuit specifieke datadeel omgevingen met hun eigen specifieke oplossingen. Dit wordt aangeduid als het hub-model (Figuur 1) [21]: een diversiteit aan datadeel omgevingen met hun eigen specifieke oplossingen om data aanbieders te voorzien van mogelijkheden voor het onderhouden van datasoevereiniteit. Het hub-model wordt vaak gebruikt voor sectorspecifieke, gesloten, gemeenschappen.

Voor de data aanbieders leidt dit tot een dreiging van lock-in met grote diversiteit en daarmee ook integratie-inspanningen tot gevolg voor het definiëren en handhaven van de diverse datasoevereiniteit aanpakken.

Een enkel toegangspunt voor de data aanbieder met gemeenschappelijke en overeengekomen protocollen voor het definiëren en afdwingen van datasoevereiniteit zal de gegevensaanbieders duidelijke operationele voordelen bieden met betrekking tot de efficiëntie en effectiviteit van het beheer van zijn gegevensuitwisselingsverbindingen.

Als alternatief krijgt de netwerk-model benadering momenteel veel aandacht. Het biedt generieke infrastructurele bouwblokken (zie sectie 3.3) voor het gecontroleerd delen van data, waarmee de data aanbieder één toegangspunt heeft tot gemeenschappelijke en overeengekomen protocollen voor het definiëren en handhaven van de voorwaarden voor het delen van data. Met succes wordt een netwerk-model benadering toegepast voor infrastructurele dienstverlening in de bank- en telecommunicatiesector.

Figuur 2 illustreert de overgang van een oplossing specifieke hub-model benadering naar een open, generieke netwerk-model benadering met infrastructurele bouwblokken voor data soevereiniteit.




Figuur 1: De hub-model aanpak (l) en open netwerk-model aanpak (r) voor datadelen [21].

Betrouwbaar datadelen op basis van een open netwerk-model benadering voor het realiseren van datasoevereiniteit wint aan belangstelling. De technologische concepten en componenten om een dergelijk netwerk-model mogelijk te maken, worden momenteel volwassen en komen beschikbaar.

De iSHARE en IDS initiatieven zoals verder in sectie 3.5 en appendix D van dit rapport toegelicht zijn voorbeelden netwerk-model benaderingen voor datadelen die momenteel veel aandacht krijgen.

## 3.3. Gecontroleerd en betrouwbaar datadelen: de basis bouwblokken

Een set van essentiële bouwstenen voor het mogelijk maken van het gecontroleerd, en betrouwbaar delen van data is daarbij geïdentificeerd en beschreven [3], zoals weergegeven in Figuur 2.

De essentie van deze bouwstenen voor het delen van data als basis voor de opkomende data economie is dat organisaties de potentiële waarde van hun gegevens kunnen benutten en er hun voordeel mee kunnen doen.

| Bouwstenen | Toelichting |
|---|---|
| 1. Bericht- en datastandaarden | • Het bepalen van bericht- en datastandaarden voor datadelen zorgt ervoor dat machines eenvoudig data kunnen verwerken zonder menselijke tussenkomst. Succesvolle datadeelinitiatieven bouwen op basis van een (minimale) set datastandaarden en sluiten daarbij aan bij technisch veel geaccepteerde berichtstandaarden |
| 2. Operationele afspraken | • Operationele afspraken bepalen de kaders voor de deelnemende partijen met betrekking tot de operationele processen rondom datadelen (bijv. serviceprocessen). Dit zorgt ervoor dat processen waarbij bepaalde data wordt gebruikt op een uniforme manier worden afgehandeld |
| 3. Juridische afspraken | • Juridische afspraken zorgen ervoor dat de regels rondom beheer en organisatie, regels voor gebruik van data, financiën, operationele aspecten, arbitrage en technische aspecten van een datadeelinitiatief juridisch zijn vastgelegd. Juridische afspraken waarborgen een kader waarbinnen de deelnemers aan een datadeelinitiatief opereren |
| 4. Verdien-/ bekostigingsmodel | • Het verdienmodel zorgt dat de kosten van de initiatie en exploitatie van een datadeelinitiatief gedekt worden en moet dus bij ontwerp van initiatief worden meegenomen |
| 5. Connectiviteit | • Connectiviteit is de manier waarop verschillende partijen de data met elkaar of via een tussenpersoon / platform uitwisselen. Connectiviteit tussen bedrijven bij datadelen wordt tegenwoordig bijvoorbeeld vaak gerealiseerd door gestandaardiseerde APIs |
| 6. Governance | • Goede governance is essentieel om vertrouwen van deelnemers in een datadeelinitiatief te borgen. Initiatieven worden vaak beheerd vanuit een (consortium van) marktpartij(en) en/of een brancheverenigingen afhankelijk van het doel van het initiatief |
| 7. Metadata | • Metadata beschrijft een dataset. Afspraken over metadata zorgen ervoor dat het voor machines eenvoudig wordt om te navigeren door datasets en informatie over de inhoud, locatie, toegangsrechten, etc. uit te lezen. Dit zorgt ervoor dat (externe) partijen data kunnen vinden en dit borgt interoperabiliteit van datasets en systemen |
| 8. Consent | • Het is belangrijk dat de data-eigenaar controle heeft over zijn eigen data. Consent betreft het krijgen en geven van datatoegangsrechten. Consent management zorgt ervoor dat de data-eigenaar eenvoudig kan specificeren wie tot welke data en onder welke juridische condities toegang krijgt, voor hoe lang, etc. |
| 9. Identificatie en authenticatie | • Identificatie en authenticatie is het proces waar iets of iemand een identiteit claimt o.b.v. bepaalde karakteristieken. Het is belangrijk dat een identiteit gevalideerd kan worden met een bepaalde mate van zekerheid, zodat de deelnemende partijen elkaar kunnen vertrouwen |

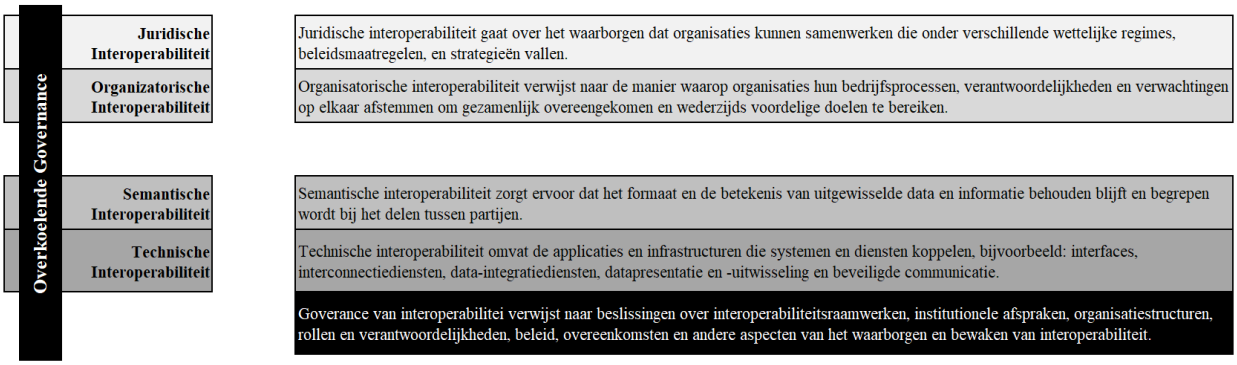
Figuur 2: Essentiële bouwblokken voor gecontroleerd en betrouwbaar datadelen [3].

### 3.4. Interoperabiliteit: governance, juridisch, organisatorisch, semantisch en technisch

Betrouwbaar datadelen geeft een multidisciplinaire uitdaging. Het delen van data ten behoeve van AI over toepassingen, organisaties en sectoren kan worden gekenmerkt als een federatieve omgeving (of 'systeem-van-systemen'), waarin een veelheid aan specifieke platformen hun mogelijkheden bundelen om gecontroleerd datadelen met behoud van datasoevereiniteit mogelijk te maken. Interoperabiliteit is daarbij essentieel voor brede adoptie en gemakkelijke integratie.

Verschillende kaders zijn ontwikkeld voor het realiseren van interoperabiliteit voor dergelijke federatieve omgevingen. Een aanpak die veel wordt gehanteerd is het (nieuwe) Europese interoperabiliteitskader zoals ontwikkeld door de Europese Commissie [22]. Zoals weergegeven in Figuur 3 onderscheidt het vier interoperabiliteitsniveaus die moeten worden geïmplementeerd onder een overkoepelende governance-aanpak: juridische, organisatorische, semantische en technische interoperabiliteit.

De niveaus van interoperabiliteit zoals beschreven in de figuur dienen te worden geadresseerd in een overkoepelende aanpak voor gecontroleerd en betrouwbaar datadelen voor die gevallen waarbij interoperabiliteit tussen datadelen van sectoren, toepassingen, landen of jurisdicties wordt nagestreefd. Deze komen in dit rapport aan de orde.




Figuur 3: Interoperabiliteitmodel zoals gedefinieerd in het 'new European Interoperability Framework' [22].

## 3.5. Datadeel technologieën: overzicht en relevantie voor AI

Voor het technisch vormgeven van infrastructuren om gecontroleerd en betrouwbaar data te kunnen delen voor AI toepassingen, is er een aantal interessante technologieën. Daarbij wordt onderscheid gemaakt tussen 4 categorieën:

- Datadeel architecturen die datadelen met generieke bouwblokken volgens het netwerk-model mogelijk maken.
- Beveiligingstechnieken om data te beschermen tijdens het delen ervan.
- Beveiligingstechnieken om de data te beschermen vóór of na het uitvoeren van de AI applicatie.
- Aanpalende technieken die bruikbaar zijn, maar niet direct de vertrouwelijkheid van gegevens beschermen.

In Tabel 2 is voor elk van deze categorieën een aantal voorbeelden van technologieën weergegeven. In appendix C worden deze uitgebreider beschreven.

| *Datadeel architecturen* | *Aanpalende technieken* |
|---|---|
| *International Data Spaces (IDS)*<br><br>Een Europees initiatief om op gestandaardiseerde wijze en op basis van een referentie-architectuur het (gecontroleerd) delen van gegevens mogelijk te maken. | *Distributed ledger*<br><br>Een decentrale manier om grote hoeveelheden transacties (contracten, documenten, etc.) op te slaan, en die garandeert dat de opgeslagen informatie niet meer veranderd kan worden. Een voorbeeld hiervan is blockchain technologie. |
| *iSHARE*<br><br>Een Nederlands initiatief voor de logistieke sector, dat een uniforme reeks afspraken voor identificatie, authenticatie en autorisatie realiseert. | *Ontology Based Access Control (OBAC)*<br><br>Dit is een hulpmiddel om structuur te krijgen in grote verzamelingen data met hoge diversiteit, en biedt mogelijkheden om toegang tot die data te reguleren. |
| *Beveiligingstechnieken tijdens delen* | *Beveiligingstechnieken vóór/na AI* |
| *Secure Multi-Party Computation (MPC)*<br><br>Een verzameling van innovatieve cryptografische technologieën die het mogelijk maakt dat meerdere partijen gezamenlijk rekenen met data, alsof ze een grote database hebben met al hun data, maar zonder dat ze elkaars data kunnen zien. | *Differential privacy*<br><br>Een manier om te voorkomen dat de uitkomsten van statistische analyses te herleiden zijn tot personen, door ruis toe te voegen aan persoonlijke data, en kan in combinatie met federated learning of MPC gebruikt worden om de output van AI-algoritmen te beschermen. |
| *Federated learning*<br><br>Een vorm van machine learning met gedistribueerde data, waarbij het algoritme zo wordt opgezet dat de data die tussen partijen wordt uitgewisseld minder gevoelig is. | *Anonimiseren en pseudonimiseren*<br><br>Technieken om te voorkomen dat data valt terug te leiden naar personen, door identificeerbare informatie uit gegevens te verwijderen of te verhaspelen. |

Tabel 2: Overzicht datadeel technologieën

# 4. Ontwikkeltraject: van 'IST' naar 'SOLL'

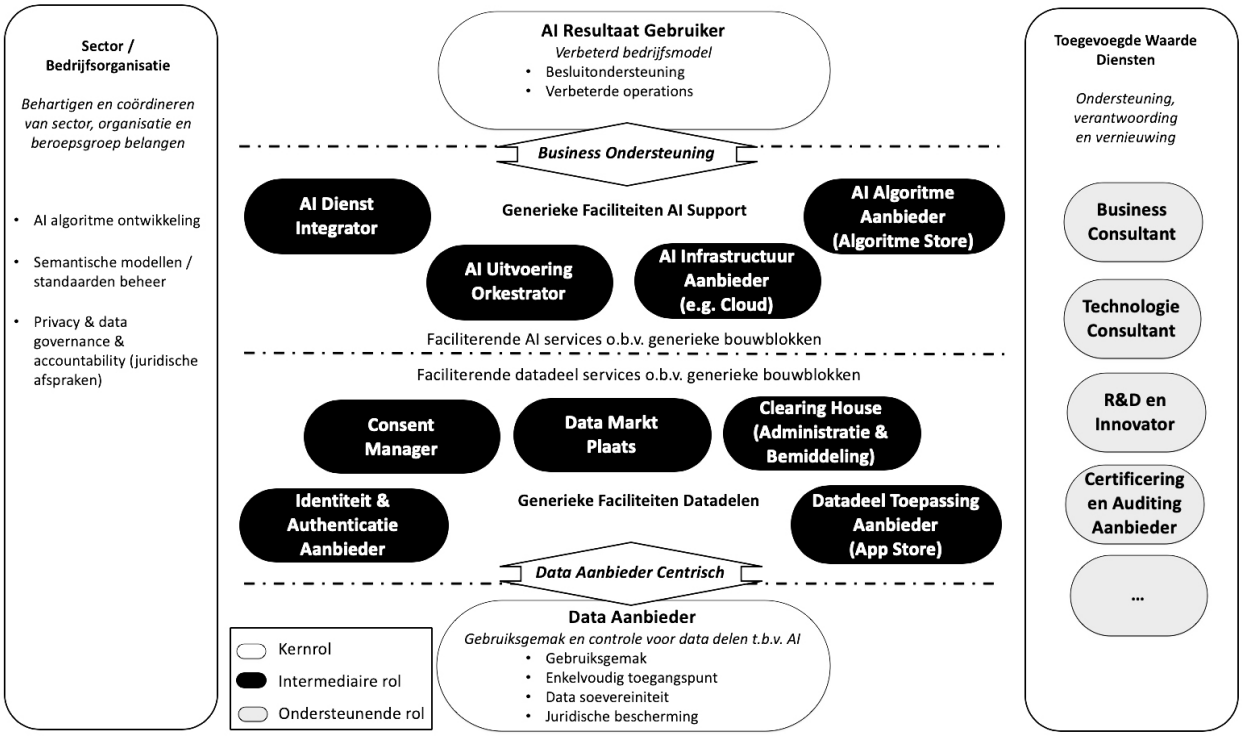
Datadeel architecturen bevinden zich nog in een opkomende fase. Voor veel organisaties geldt dat begeleiding nodig is om hiervan gebruik te maken, zeker met de nieuwere technologieën die er beschikbaar komen. In het kader van de NL AIC bestaat de mogelijkheid de ideeën, architecturen en concepten rondom datadelen voor AI verder te ontwikkelen en te realiseren.

In dit hoofdstuk wordt het ontwikkeltraject vanuit de huidige 'IST' situatie naar de toekomstige 'SOLL' situatie beschreven. Daartoe beschrijven de achtereenvolgende secties de rollenmodel / ecosysteem aanpak voor de inrichting van de generieke datadeel infrastructuur, het proces van first-time-engineering naar operationalisatie en het initiële, representatieve, toepassing scenario en proof-of-concept (PoC) als eerste stap in het vervolgtraject van de NL AIC werkgroep datadelen.

## 4.1. Ecosysteem voor datadelen: bouwblokken en rollen

Er bestaat geen 'one-size-fits-all' aanpak voor het inrichten van datadelen ten behoeve van AI. Verschillende doelstellingen, belangen en perspectieven zullen maken dat er verschillende datadeel aanpakken zullen worden gevolgd. Het is daarbij wel van belang dat de verschillende aanpakken zo goed mogelijk kunnen worden ondersteund door een diversiteit aan datadeel functies. Door deze als generieke en herbruikbare bouwblokken in een (open) netwerk-model ter beschikking te stellen, wordt afhankelijkheid vermeden van (gesloten) platforms die organisaties en mensen in de greep hebben, zie sectie 3.2.

Om de diversiteit aan aanpakken voor datadelen ten behoeve van AI en oplossingen beter inzichtelijk en hanteerbaar te maken, wordt een ecosysteem van rollen gedefinieerd, die gezamenlijk de benodigde bouwblokken kunnen leveren, zie Figuur 4. De rollen worden in samenhang ontwikkeld en gevalideerd.




Figuur 4: Het rollenmodel (ecosysteem) voor datadelen t.b.v. AI.

Zoals de figuur aangeeft maakt het ecosysteem voor datadelen t.b.v. AI onderscheid in 'kernrollen', 'intermediaire rollen' en 'ondersteunende rollen':

- *Kernrollen*. De kernrollen zijn de direct belanghebbenden voor het delen van data. Dit zijn de partijen waartussen primaire data gedeeld wordt, i.e. de data aanbieders en de AI resultaat gebruikers.
- *Intermediaire rollen voor generieke faciliteiten*. De intermediaire rollen leveren de ondersteunende functies als herbruikbare bouwblokken die het datadelen tussen de kernrollen faciliteren. Zoals de figuur laat zien, onderscheiden we daarbij intermediaire rollen voor datadelen en intermediaire rollen voor AI-support. Deze rollen zullen geen toegang mogen hebben tot de primaire data. Mogelijk verwerken ze wel de secondair data vereist en gegenereerd door de ondersteuningsprocessen, ook wel 'metadata' genoemd. De intermediaire rollen zijn over het algemeen door vertrouwde derde partijen vormgegeven, i.e. zogenaamde 'Trusted Third Parties' (TTP's).
- *Ondersteunende rollen*. Deze rollen vervullen geen activiteit in het daadwerkelijke proces van datadelen, maar kunnen wel nodig zijn om het systeem te laten functioneren.

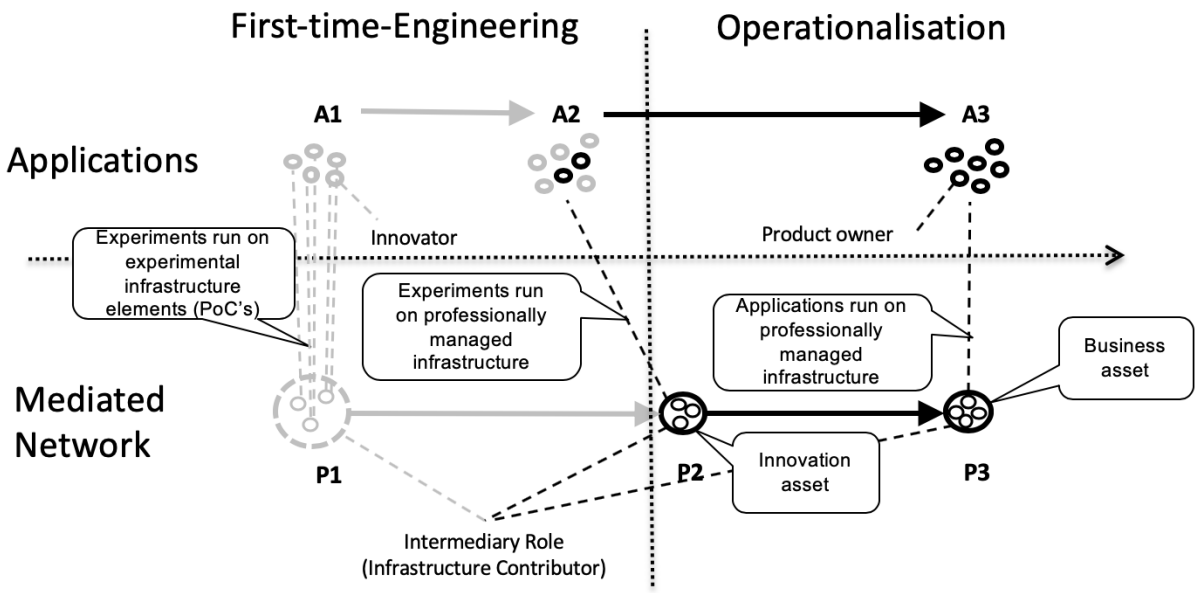
Op dit punt is het goed te verwijzen naar een aantal internationale initiatieven die momenteel raken aan de aanpak zoals beschreven in deze sectie. Google biedt hun AI-platform aan [23]. Deze levert functies en bouwblokken voor AI-support. Deutsche Telekom levert het concept van de 'Data Intelligence Hub' [24] met functies en bouwblokken voor zowel AI-support als datadelen. Daarnaast krijgt het GAIA-x initiatief [12] momenteel veel aandacht. Dit initiatief is eind 2019 vanuit Duitsland gestart om een Europees cloud infrastructuur te ontwikkelen als alternatief voor de grote platformen uit de VS en Azië.

## 4.2. Van first-time-engineering naar operationalisatie

Om de kracht van het NL AI-landschap te versterken is het van belang aan een gezamenlijke infrastructuur voor het delen van data ten behoeve van AI te werken, om toepassingsmogelijkheden te vergroten en vendor lock-in te voorkomen. Het doel is om voor Nederland een sterke AI-infrastructuur te maken, waarin organisaties door samenwerking impactvolle toepassingen op de markt kunnen brengen. Daartoe beschrijft deze sectie op hoofdlijnen het proces hoe bedrijven het delen van data ten behoeve van AI, eerst via 'first-time-engineering' naar uiteindelijk de dagelijkse praktijk ('operationalisatie') kunnen brengen. Een gedetailleerdere uitwerking hiervan is opgenomen in een aparte rapportage van de werkgroep datadelen van NL AIC [25].

Voor het proces van first-time-engineering naar operationalisatie wordt uitgegaan van het ontwikkelproces dat wordt aangeduid als het 'strategic options model'. Deze is weergegeven in Figuur 5. Het beschrijft de ontwikkeling voor digitale diensten van de experimentele ('first-time-engineering', met grijs aangegeven in de figuur) naar operationele fase ('operationalisation', met zwart aangegeven in de figuur). Hierin maken we onderscheid tussen de generieke technische infrastructuur (het 'mediated network') die benodigd is voor het ondersteunen van (datadelen ten behoeve van) AI en de applicaties van de nieuwe technologie zelf. Daarbij bevat de generieke technische infrastructuur zowel de dadadeel als AI-faciliterende laag zoals aangegeven in Figuur 4, welke herbruikbare bouwblokken bevatten die benodigd zijn voor het veilig en verantwoord delen van data met verschillende partijen en het ondersteunen van AI-toepassingen. Deze infrastructuur kan zowel fysieke (bijv. hardware) als ook abstracte elementen, zoals een afsprakenstelsel of software, bevatten.

Voor sommige partijen kan het extra waardevol zijn om kennis en ervaring op te doen met het ontwikkelen, runnen en faciliteren van de faciliterende infrastructuur, terwijl anderen juist op zoek zijn naar ervaring met het ontwikkelen van nieuwe AI applicaties die hiervan




Figuur 5: Strategic Options Model. De infrastructuur laag bevat de datadeel en faciliterende AI-functies voor die gezamelijk AI toepassingen mogelijk maken.

gebruik kunnen maken.

De rol van 'infrastructure contributor' is voor partijen weggelegd die bouwblokken als dienst beschikbaar stellen en daarmee samen de infrastructuur tot een functioneel geheel maken. Denk daarbij aan zowel bouwblokken in de datadeel laag als bouwblokken in de AI-faciliterende laag, zoals aangegeven in Figuur 4.Deze rol kan door een veelheid aan partijen naast elkaar ingenomen worden.

In het proces naar operationalisatie, kunnen partijen starten met het ontwikkelen van fase "I1": één experimenteel onderling gedeelde infrastructuur voor het runnen van meerdere experimentele applicaties. Deze kan op basis van meerdere initiële gebruikers use cases vormgegeven worden als een samenwerking van een aantal partijen ('voorlopers') met als doel een of meerdere AI applicaties te realiseren met specifieke technische use cases en de technische infrastructuur in gedachten.

Voor de snelheid en kwaliteit van de gezamenlijke AI-ontwikkeling in Nederland is het daarbij van belang dat de initiële gebruikers use cases er niet alleen zijn om van elkaar te leren, maar ook als aanzet om voort te kunnen bouwen op weg naar operationalisatie. Dus een use case levert zowel inzicht in de toepassing als een initiële (referentie) architectuur en implementatie voor herbruikbare bouwblokken.

Zoals weergegeven in Figuur 5 worden als onderdeel van het proces drie fases onderscheiden voor de infrastructuur en AI-toepassingen. Deze zijn beschreven in Tabel 3.

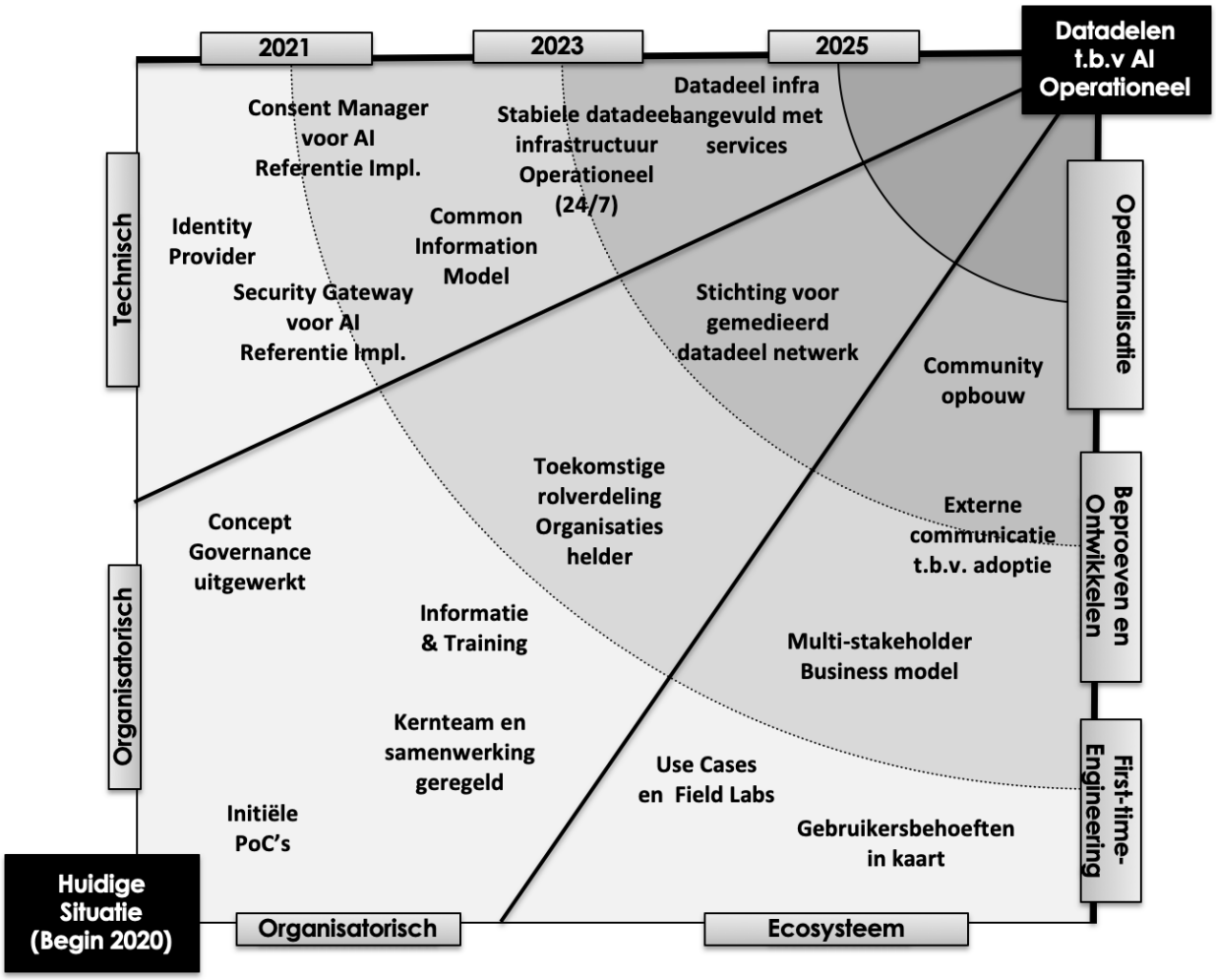
| *Infrastructuur ('I')* | *AI-toepassingen ('A')* |
|---|---|
| I1: Een experimentele infrastructuur voor het delen van data, gebaseerd op generieke bouwblokken van de PoC's, om te leren hoe men een dergelijke infrastructuur opzet en onderhoudt. Hieronder valt ook het deployment en management van AI-applicaties op basis van deze data. Ontwikkelaars van AI applicaties moeten er rekening mee houden dat deze infrastructuur nog niet aan al hun eisen, zoals beschikbaarheid, stabiliteit, veiligheid, zal voldoen. | A1: Experimentele AI-toepassingen, voornamelijk bedoeld om vaardigheden op te ontwikkelen met het delen van data. |
| I2: Een datadeel infrastructuur die voldoende professionaliteit heeft zodat deze als dienst aan gebruikers kan worden aangeboden die willen experimenteren met het ontwikkelen en draaien van AI-applicaties. Deze AI applicaties stellen nieuwe eisen aan het datadelen zoals toegang, controle, veiligheid en feedback. Het is een innovatie asset die innovatieve AI-applicaties op basis van gedeelde data mogelijk maakt. | A2: Experimentele AI-toepassingen, voornamelijk bedoeld om ervaring op te doen met het ontwikkelen van AI-applicaties ter voorbereiding op productie. |
| I3: Dit is een operationele, generieke, infrastructuur voor het delen van data ten behoeve van exploiteerbare AI-toepassingen. Het is een business asset, die aan andere eisen moet voldoen dan I2, omdat er exploiteerbare applicaties van afhankelijk zijn. Ook zullen andere bedrijfsrisico's en overeenkomsten van toepassing zijn dan bij I2. | A3: Exploiteerbare AI-toepassingen die voldoende betrouwbaar en stabiel zijn om aan eindgebruikers beschikbaar te stellen in ruil voor iets van monetaire waarde. |

Tabel 3: Fases voor de generieke Infrastructuur ('I') en AI-toepassingen ('A') in het proces van first-time-engineering naar operationalisatie

In het proces nemen de partners van NL AIC actief deel aan de gezamenlijke taak om een roadmap op te stellen voor het doorlopen van deze fases voor infrastructuur en AI-toepassing. In de roadmap wordt daarbij de driedeling gehanteerd:

- *Technologie:* Het vormgeven van de architectuur benodigd voor het delen van data, het definiëren van interfaces en informatiemodellen en het demonstreren en realiseren van use cases.
- *Organisatie (governance):* Deze is gericht op de (door)ontwikkeling van de voorgestelde aanpak, architecturen, interfaces en standaarden. Dit bevat zowel de procesinrichting hiervoor door middel van een aansturende organisatie en de inrichting van een change (advisory) board als de technische roadmap.
- *Ecosysteem:* Deze is gericht op de adoptie door organisaties en marktpartijen. Aangezien we hier te maken hebben met een implementatie door meerdere partijen, spreken we over een ecosysteem. Het is van belang dit ecosysteem zo goed mogelijk te faciliteren ter voorbereiding en realisatie van groei. Door de opschaling van zowel partijen die verantwoord data met elkaar delen als van AI-toepassingen zelf word de positieve impact voor de eindgebruikers in steeds grotere mate gerealiseerd.

In Figuur 6 is een concept roadmap voor het ontwikkelproces van first-time-engineering naar operationalisatie weergegeven. De individuele activiteiten zijn verder beschreven in [25].




Figuur 6: Concept roadmap voor het ontwikkelproces van first-time-engineering naar operationalisatie.

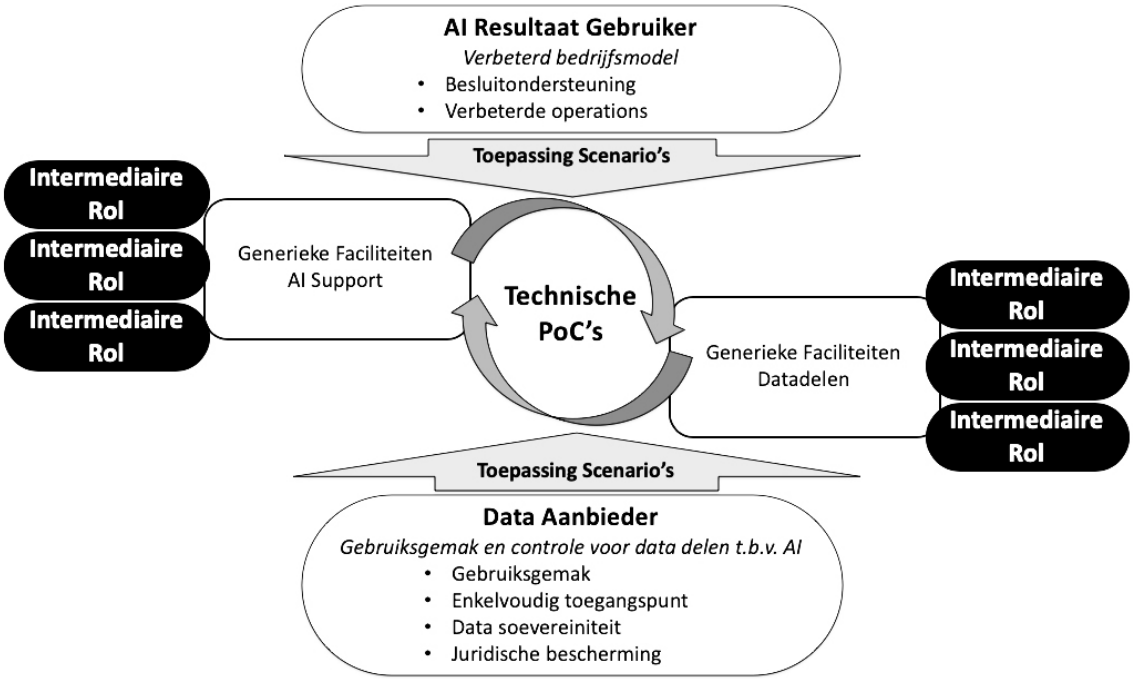
### 4.3. Toepassing scenario's en proofs-of-concept

In het traject naar operationalisatie zullen de ideeën, architecturen en concepten rondom datadelen voor AI door middel van een selectie van toepassing scenario's en technische Proofs-of-Concept (PoC's) worden vormgegeven. De toepassing scenario's en de PoC's zijn gericht op demonstratie en validatie van een gemeenschappelijke datadeel infrastructuur. De doelen van de PoC's zijn om:

- De aanpak van datadelen volgens het rollenmodel / ecosysteem zoals weergegeven in Figuur 4, met generieke rollen (bouwblokken) voor zowel 'Generieke Faciliteiten Datadelen' als voor 'Generieke Faciliteiten AI-Support' in samenhang verder te ontwikkelen en technisch te valideren. Bij voorkeur wordt dit onafhankelijk van sector of toepassing gedaan, waardoor de datadeel infrastructuur cross-sectoraal aangeboden kan worden.
- Vast te stellen of deze aanpak van datadeel bijdraagt aan de bereidheid van organisaties om tot een manier van samenwerken te komen en daarbij (gevoelige) data te delen ten behoeve van AI-toepassingen.

Samen met de sectorvertegenwoordigers in de NL AIC worden één of meerdere AI toepassing scenario's gekozen waarvoor de concepten van datadelen ten behoeve van AI als PoC's worden ontwikkeld. Daarbij worden AI toepassing scenario's met significante impact gekozen. De organisaties uit de sector zullen worden betrokken bij de voorbereiding en realisatie van de AI toepassing scenario's en PoC's. De resultaten worden gedeeld met de leden van de coalitie.

Er is niet een 'one-size-fits-all' aanpak voor het inrichten van datadelen ten behoeve van AI. Het is daarom niet de bedoeling en mogelijk om één toepassing scenario te definiëren die het gehele speelveld van (gecontroleerd) datadelen voor AI afdekt. Daarom wordt gekozen voor een aanpak op basis van een aantal illustratieve en representatieve toepassing scenario's en bijbehorende technische PoC's waarbij de PoC's de verschillende perspectieven op het rollenmodel zoals weergegeven in Figuur 4 en haar uitdagingen technisch demonstreren. Deze aanpak is geïllustreerd in Figuur 7.




Figuur 7: Concept roadmap voor het ontwikkelproces van first-time-engineering naar operationalisatie.

## 4.4. Initiële toepassing scenario en PoC

Als eerste stap van de NL AIC werkgroep datadelen in het vervolgtraject van first-time-engineering naar operationalisatie wordt een initiële, representatieve toepassing scenario (klimaatmanagement in gebouwen) uitgewerkt in een PoC. Dit initiële toepassing scenario en de PoC worden beschreven in de volgende paragrafen.

### *4.4.1. Representatief toepassing scenario: klimaatmanagement in gebouwen*

Vanuit de energiesector werken een aantal consortia aan de ontwikkeling van algoritmes voor klimaatinstallaties in kantoorgebouwen. Zij gebruiken hiervoor klimaatdata, aansturingsdata van de installaties zelf en data over de aanwezigheid en het welbevinden van gebruikers in de gebouwen. ECN heeft daarbij berekend dat door klimaatinstallaties slim aan te sturen 20-30 PetaJoule energie valt te besparen. Dat komt omdat meer dan 70% van de klimaatinstallaties in gebouwen niet goed afgestemd is, wat leidt tot gemiddeld 30% energieverspilling. Het oplossen hiervan kan potentieel een verlaging van het energieverbruik gerealiseerd worden dat gelijk staat aan het gebruik van circa 400.000 huishoudens.

Een logische stap, maar in de praktijk blijkt dit een lastige opgave: Steeds starten nieuwe consortia weer van nul af aan met het verzamelen van data om vanuit een nieuw consortium een algoritme te ontwikkelen of een aanpassing te doen. En vaak willen of durven relevante partijen geen data te delen waarmee het initiatief strandt of maar beperkt tot resultaten haalt.

Vanuit de NL AIC datadeel werkgroep is daarom deze use case in het energiedomein voorgesteld.

De uitwerking van deze initiële toepassing scenario en PoC kan de aanzet vormen voor één experimenteel onderling gedeelde infrastructuur voor het runnen van meerdere experimentele AI applicaties, bijv. het automatisch managen van gebouw-utiliteiten voor o.a. de regeling van klimaat en licht waardoor significante energiebesparing mogelijk gemaakt wordt. Doel is daarbij deze experimentele infrastructuur ook voor andere toepassing scenario's (in andere sectoren) te gebruiken.

### *4.4.2. PoC: datadelen t.b.v. het 'data-to-analysis' samenwerkingsmodel*

De PoC voor de initiële, representatieve toepassing scenario (klimaatmanagement in gebouwen) beschouwt initieel de datadeel infrastructuur gericht op het samenwerkingsmodel 'data-to-analysis'. De rollen en bouwblokken voor de generieke datadeel infrastructuur (zoals weergegeven in Figuur 4) worden zodanig gedefinieerd en vormgegeven dat een data-eigenaren hun brondata aan verschillende data analyse partijen beschikbaar kunnen stellen. De databronnen worden 'centraal' verwerkt, i.e. in het domein van de organisatie met het AI-systeem.

De rollen voor het leveren van generieke bouwblokken voor datadelen die hierbij zullen worden gedemonstreerd zijn:

- *Data marktplaats*, in een vereenvoudigde uitvoering van de rol als '*data broker*', waarbij de databronnen door de data-aanbieder geregistreerd en geadverteerd kunnen worden.

  Een data analyse partij kan bij de data broker zien welke data, tegen welke voorwaarden, beschikbaar is en zich hierop 'abonneren'. Daarbij wordt er van uitgegaan dat de brondata onder een overkoepelende voorgedefinieerde datadeel afspraak zal worden gedeeld met het AI-systeem, zonder financiële afhandeling.

- *Consent manager*, waarin de data-aanbieder verschillende types van autorisaties voor zijn brondata kan registreren, beheren en laten uitvoeren.

  Niet alle data van de data aanbieder zal op de locatie en in de systemen van de data aanbieder zelf beschikbaar zijn. Bijvoorbeeld thermostaat data

wordt verzonden naar de energieleverancier en wordt daar in de systemen opgeslagen. Dit vergt dat de autorisatiearchitectuur waarbinnen de consent manager opereert het mogelijk moet maken om gedistribueerde machtigingen en autorisaties in te richten.

Daarnaast zullen ook op de resultaten van het uitgevoerde AI-algoritme autorisaties vanuit de aanbieder van de brondata van toepassing kunnen zijn. Ook voor het registreren, beheren en uitvoering hiervan worden functies in de consent manager ingericht.

- *Identificatie en authenticatie manager*, die de functie, proces en technologie vormgeeft om zekerheid te geven dat een actor (mens, machine, softwarecomponent …) echt is wie hij / zij / het zegt te zijn.

  In de initiële PoC zal de identificatie van drie typen van actors worden uitgewerkt: die van organisaties / deelnemende partijen, van individuele personen en van security gateways binnen organisaties, i.e. de software modules die het delen van data met specifieke systemen kunnen beheren en beheersen. Bij deze PoC zal gebruik gemaakt worden van IDS connectors [27].

De rollen voor het leveren generieke bouwblokken voor AI-support die zullen worden gedemonstreerd zijn:

- *AI uitvoering orkestrator* die het uitvoeren van het AI-algoritme aanstuurt en monitort en daarbij de drie basis samenwerkingsmodellen uit appendix B faciliteert.

  In de initiële PoC is de functionaliteit van deze rol beperkt tot het faciliteren van het 'data-to-analysis samenwerkingsmodel.

- *AI infrastructuur aanbieder*, die de infrastructuur functies biedt om de AI-algoritmes uit te voeren.

  In de initiële PoC met het 'data-to-analysis samenwerkingsmodel biedt deze een beveiligde, virtueel privé omgeving, in de (cloud) infrastructuur om het het AI-algoritme uit te voeren en de databronnen daarheen te vervoeren. Op deze wijze wordt de brondata niet in het domein van de data-eigenaar zelf verwerkt, zonder daarbij concessies te doen aan de data soevereiniteit en beveiliging.

- *AI algoritme aanbieder*, die een bibliotheek van herbruikbare AI-algoritmes beheert en deze aan derde partijen aanbiedt.

Als uitbreiding op deze initiële PoC, kunnen als vervolg ook de functionele uitbreiding van de bovenbeschreven generieke rollen (bouwblokken) worden beschouwd die het mogelijk maken om ook de samenwerkingsmodellen 'analysis-to-data' en vervolgens 'data-and-analysis-to-lake' uit te voeren.

Bij het samenwerkingsmodel 'analysis-to-data' bijvoorbeeld, wordt de data 'lokaal' (i.e. in het domein van de databron) verwerkt. De functies van de rol 'consent manager' zal daarbij moeten worden uitgebreid, door aanvullende autorisaties op te nemen om de uitwisseling van AI-algoritmen, tussenresultaten en resultaten te borgen. Ook de functies van de rol 'AI uitvoering orkestrator' moet worden uitgebreid om de distributie van de AI-systemen over de verschillende data aanbieders te orkestreren en monitoren. De rol 'AI infrastructuur aanbieder' zal hiervoor adequate ondersteunende (cloud) diensten moeten aanbieden.

## Referenties


1. Nederlandse AI Coalitie (NL AIC). URL: https://nlaic.com/.
2. PricewaterhouseCoopers (PWC), IDSA (2018). "Data exchange as a first step towards data economy". URL: https://www.pwc.de/en/digitale-transformation/data-exchange-as-a-first-step-towards-data-economy.pdf.
3. Ministerie van Economische Zaken en Klimaat (2018). "Generiek afsprakenstelsel voor datadeelinitiatieven als basis van de digitale economie". URL: https://www.rijksoverheid.nl/documenten/rapporten/2018/ 12/30/generiek-afsprakenstelsel-voor-datadeelinitiatieven-als-basis-van-de-digitale-economie.
4. Ministerie van Economische Zaken en Klimaat (2019). "Nederland Digitaal - De Nederlandse visie op datadeling tussen bedrijven". URL: https://www.rijksoverheid.nl/documenten/publicaties/2019/02/20/nederland-digitaal---de-nederlandse-visie-op-datadeling-tussen-bedrijven.
5. Europese Commissie (2018). "Artificial Intelligence for Europe". EC Communications 237. URL: https://ec.europa.eu/transparency/regdoc/rep/1/2018/en/com-2018-237-f1-en-main-part-1.pdf.
6. Europese Commissie (2018). "Coordinated Plan on AI". EC Communications 795. URL: https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence.
7. Europese Commissie (2020). "On Artificial Intelligence - A European approach to excellence and trust". EC Communications 65. URL: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.
8. Europese Commissie (2020). "A European strategy for data". EC Communications 66. URL: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.
9. Langley, D., van Doorn, J., Ng, I., Stieglitz, S., Lazovik, A., & Boonstra, A. (2020). "The Internet of Everything: Smart things and their impact on business models". Journal of Business Research. URL: https://www.sciencedirect.com/science/article/pii/S014829631930801X.
10. Data Sharing Coalition. URL: https://datasharingcoalition.eu/about/.
11. Dataregister van de Nederlandse overheid. URL: https://data.overheid.nl/.
12. Federal German Ministry of Education and Research (2020). "Project GAIA-X". URL: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6.
13. Infocomm Media Development Authority of Singapore (IMDA) and Personal Data Protection Commission (PDPC) (2019). "Trusted Data Sharing Framework". URL: https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf.
14. Go-Fair. "FAIR Prinicples". URL: https://www.go-fair.org/fair-principles/.
15. Dutch Techcentre for Life Sciences. "Personal Health Train". URL: https://www.dtls.nl/fair-data/personal-health-train/.
16. Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2016). "How We Analyzed the COMPAS Recidivism Algorithm". URL: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.
17. Bastiaansen, H., Dalmolen, S., Kollenstart, M., & Punter, M. (2019). "Infrastructural Sovereignty over Agreement and Transaction Data ('Metadata') in an Open Network-model for Multilateral Sharing of Sensitive Data". ICIS2019 Conference, Munich, Germany, 15th – 18th December 2019. URL: https://aisel.aisnet.org/icis2019/economics_is/economics_is/23/.
18. Europese Commissie (2018). "Towards a common European data space". URL: https://ec.europa.eu/digital-single-market/en/news/communication-towards-common-european-data-space.
19. Big Data Value Association (2019). "Towards a European data sharing space". URL: https://www.eoscsecretariat.eu/towards-european-data-sharing-space.
20. Big Data Value Association & euRobotics (2019). "Strategic Research, Innovation and Deployment Agenda (SRIDA) for a European AI, Data and Robotics PPP". URL: http://www.bdva.eu/node/1359.
21. Liezenberg, C., Lycklama, D., & Nijland, S. (2018). "Everything transaction". LannooCampus.

22. Europese Commissie (2017). "New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations". European Union: Brussels. URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

23. Google. "AI Platform". URL: https://cloud.google.com/ai-platform.

24. Deutsche Telekom. "Data Intelligence Hub". URL: https://dih.telekom.net/en/.

25. Nederlandse AI Coalitie Werkgroep Datadelen (2020). 'Van First-time-Engineering naar Operationalisatie".

26. Drnevich, P., & Croson, D. (2013). "Information technology and business-level strategy: toward an integrated theoretical perspective". MIS Quarterly, pp. 483-509.

27. International Data Space Association - IDSA (2019). "International Data Spaces: Reference Architecture Model Version 3". URL: www.internationaldataspaces.org.

28. Royal Society Working Group (2017). "Machine learning: the power and promise of computers that learn by example. Technical report". URL: https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf.

29. NYC Analytics. "Mayor's Office of Data Analytics". URL: https://www1.nyc.gov/site/analytics/index.page.

30. Wirtz, B., & Müller, W. (2019). "An integrated artificial intelligence framework for public management". Public Management Review, 21(7), pp. 1076-1100.

31. Deephouse, D., Bundy, J., Tost, L., & Suchman, M. (2017). "Organizational legitimacy: Six key questions". The SAGE handbook of organizational institutionalism, 4(2), pp. 27-54.

32. Davis, J. (2016). "The group dynamics of interorganizational relationships: Collaborating with multiple partners in innovation ecosystems". Administrative Science Quarterly, 61(4), pp. 621-661.

33. Hinings, B., Gegenhuber, T., & Greenwood, R. (2018). "Digital innovation and transformation: An institutional perspective". Information and Organization, 28(1), pp. 52-61.

34. Felin, T., Foss, N., & Ployhart, R. (2015). "The microfoundations movement in strategy and organization theory". The Academy of Management Annals, 9(1), pp. 575-632.

35. Webb, A. (2019). "The big nine: How the tech titans and their thinking machines could warp humanity". Hachette UK.

36. Zhang, L. Cushing, R., Gommans, L., de Laat, C., & Grosso, P. (2019). "Modeling of Collaboration Archetypes in Digital Market Places". IEEE Access, Volume 7, pp. 102689 - 102700. URL: https://ieeexplore.ieee.org/document/8779607.

37. Van der Waaij, B., Lazovik, E., Albers, T., & Vonder, M. (2020). "CO-ARCH: Methodology for Collaborative ARCHitectures for cross-organizational data analysis". International Journal of Modeling and Optimization (IJMO). URL: http://www.ijmo.org/index.php?m=content&c=index&a=show&catid=100&id=931.

38. Europese Commissie - Article 29 Data Protection Working Party. "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", WI251rev0.1, pp. 19. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

39. Selbst, A., & Powles, J. (2017). 'Meaningful information and the right to explanation'. International Data Privacy Law', Vol. 7, No. 4, pp. 233 – 242.

40. Zuiderveen Borgesius, F., (2019). "Discrimination, artificial intelligence and algorithmic decision making". URL: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

41. Den Breeijen, S., & Bomhof, F. (2020). "Data sharing technologies", TNO.

42. Dutch Neutral Logistics Information Platform. "iSHARE Data Sharing Initiative". URL: https://www.iSHAREworks.org/en/.

43. Amsterdam Economic Board, 'Amsterdam Data Exchange', 2019. Available at: https://www.amsterdameconomicboard.com/initiatief/amdex.

44. Goldreich, O., Micali, S. & Wigderson, A. (1987). "How to play any mental game or a completeness theorem for protocols with honest majority". Proceedings of the 19th Annual ACM Symposium on Theory of Computing, New York, New York, USA, pp. 218-229.

**45.** Konecny, J., McMahan, B., & Ramage D. (2015). "Federated optimization: distributed optimization beyond the datacenter". URL: https://arxiv.org/abs/1511.03575.

**46.** DataShield. URL: http://www.datashield.aD.uk/.

**47.** Dwork, C. (2008). "Differential privacy: a survey of results". M. Agrawal, D. Du, Z. Duan, & A. Li (Eds.). Springer Berlin Heidelberg, pp. 1–19.

**48.** Kroon, U. (2013). "Ma3tch: Privacy and knowledge: Dynamic networked collective intelligence". 2013 IEEE International Conference on Big Data. URL: https://ieeexplore.ieee.org/document/6691683.

**49.** I2P Foundation Wiki. "Self-Sovereign Identity'. URL: https://wiki.p2pfoundation.net/Self-Sovereign_Identity.

**50.** Wikipedia. "Distributed Ledger". URL: https://en.wikipedia.org/wiki/Distributed_ledger.

**51.** Brewster, C., Nouwt, B., Raaijmakers, S., & Verhoosel, J. (2019). "Ontology-Based Access Control for FAIR Data". Data Intelligence Journal, Vol 2 (1), pp. 1–1966-77. URL: http://www.data-intelligence-journal.org/p/36/.

# APPENDIX A: Business relevantie en digitale transformatie

Sinds het begin van het digitale tijdperk verschuift de rol van data technologieën binnen bedrijven van een functioneel naar een strategisch niveau. Waar bedrijven eerst een IT-afdeling had die diensten leverden aan de operationele afdelingen, wordt steeds vaker de algehele strategie van het bedrijf bepaald door de data en wat het bedrijf ermee kan. Een plantenkas zit tegenwoordig vol high-tech om licht, lucht, water, temperatuur en nog veel meer op de plant af te stemmen. Binnen ziekenhuizen vergaren artsen steeds vaker data uit verschillende bronnen om behandelplannen te maken die rekening houden met de bredere levenskwaliteit van de patiënt. De bestuurders van elke organisatie beseffen dat hun toekomst afhangt van hun vermogen om data optimaal te vergaren en benutten.

Deze appendix beschrijft de business relevantie van datadelen voor het toepassen van AI technologie, de mogelijkheden die het schept en de wijze waarop organisatie deze in hun bedrijfsvoering kunnen inpassen.

## A.1. De bedrijf-strategische relevantie van datadelen ten behoeve van AI

Bedrijven creëren vooral waarde uit data wanneer die data uit de meest relevante bronnen komt. Dat betekent niet alleen eigen data gebruiken voor de nieuwste AI toepassingen, maar ook data van buiten de organisatie. Zoals van leveranciers en klanten maar ook van concurrenten of andere partijen waarmee, normaal gesproken, niet wordt samen gewerkt. In dit ketenbreed datadelen is het voor alle partijen duidelijk dat data de kernasset is, en bedrijven doen er alles aan om hun eigen waardevolle data veilig te stellen terwijl ze zoveel data als mogelijk van anderen trachten te ontsluiten. Vele tech-reuzen zijn groot geworden vooral door hun vermogen om de meest inzichtrijke data te verzamelen.

De bedrijf-strategische relevantie van datadelen is gegroeid door een leertraject van digitale voorlopers. Bedrijven zoals Amazon gingen eerst efficiëntieslagen maken in bestaande verdienmodellen, zoals het verkopen van boeken. Data-analyse liet duidelijk zien waar in de bedrijfsprocessen inefficiëntie optrad en hoe dat beter kon. Inmiddels is min of meer elke industriesector bezig met dit soort verfijning van de bestaande processen. Maar de voorlopers hebben gezien dat vergaande vormen van data-analyse volkomen nieuwe verdienmodellen mogelijk maken. Door onontgonnen datacombinaties te maken, en hierdoor nieuwe inzichten te genereren door AI-analyses, ontstaan nieuwe manieren om waarde te creëren; de basis voor nieuwe verdienmodellen.

Het delen van data tussen organisaties, gekoppeld aan het inzetten van AI, stelt bedrijven in staat om zichtbaarheid te vergroten en een klantgericht, geïntegreerd bedrijfsmodel te creëren dat meer efficiëntie en flexibiliteit biedt. Door gebruik te maken van gegevens uit de gehele keten, verbeteren AI-innovaties op nauwkeurige wijze de prognoses, vergroten ze de besluitvorming en verbeteren ze de strategische analyse en innovatie om aan de veranderende eisen van de eindklant te voldoen.

## A.2. Verschillende bedrijfsperspectieven op datadelen ten behoeve van AI

De strijd is losgebarsten om data- en AI-innovaties te creëren die nieuwe verdienmodellen mogelijk maken. Deze strijd betekent enerzijds dat bedrijven creativiteit en een positieve houding tot datadelen belangrijk vinden, maar anderzijds ook angstig zijn voor het verliezen van de strijd en vastberaden zijn om de eigen data-assets te verdedigen. Hierbij zijn meerdere bedrijfsperspectieven tegelijkertijd aanwezig en elk perspectief kan inzicht verschaffen in hoe datadelen ten behoeve van AI kan worden gestimuleerd. Een viertal perspectieven kan daarbij worden onderscheiden [26]:

- Ten eerste, vanuit een machtsperspectief, zullen bedrijven met buitengewoon goede toegang tot data vaak die positie gebruiken om zelf te profiteren, ten koste van andere partijen. Dit is het duidelijkst te zien bij platformbedrijven zoals Google, Apple, Amazon, Netflix die zelf erg veel data verzamelen en (analyses op) die data tegen hoge tarieven verkopen.
- Ten tweede, een perspectief gericht op kennis- en competentieontwikkeling laat zien dat de bedrijven die zelf de beste kennis over datadelen en AI opdoen of inkopen een groot voordeel zullen hebben. Hierbij zijn drie stappen van belang: het identificeren en vinden van de nodige kennis en competenties, het opnemen van die kennis en competenties in de eigen organisatie, en het integreren van die kennis en competenties in de bestaande producten, diensten en processen om tot kansrijke vernieuwingen te komen.
- Ten derde, een governance perspectief gaat in op het gelijkrichten van de prikkels om data te delen door een waardeketen. Er is een trend om steeds meer stakeholders te betrekken en data uit vele verschillende bronnen te zoeken, waardoor er veel meer complexiteit ontstaat in het regelen en besturen van samenwerkingen. Wanneer datadeel systemen volledig open en interoperabel worden zijn volledig nieuwe governance modellen nodig, zoals bijvoorbeeld beoogd wordt door de International Data Spaces Association (IDSA) [27].
- Als laatste van deze vier bedrijfsperspectieven op het delen van data in relatie tot AI, biedt flexibilisering belangrijke nieuwe kansen. De technische infrastructuur waarin bedrijven investeren om AI te implementeren is bij uitstek geschikt om, zonder extra investeringen, voortdurend aangepast te worden. Dit maakt het mogelijk voor bedrijven om op zeer korte termijn hun processen en diensten te veranderen. Tegelijkertijd bieden datadelen en AI actuele en nauwkeurige informatie om bedrijfsbeslissingen op te baseren. Deze verfijnde beslissingsondersteuning gekoppeld aan de flexibele processen betekenen samen dat het te verwachten is dat bedrijven steeds beter zullen worden in het snel benutten van nieuwe marktkansen en het snel vermijden van risico's.

## A.3. Strategische relevantie van datadelen ten behoeve van AI in de praktijk

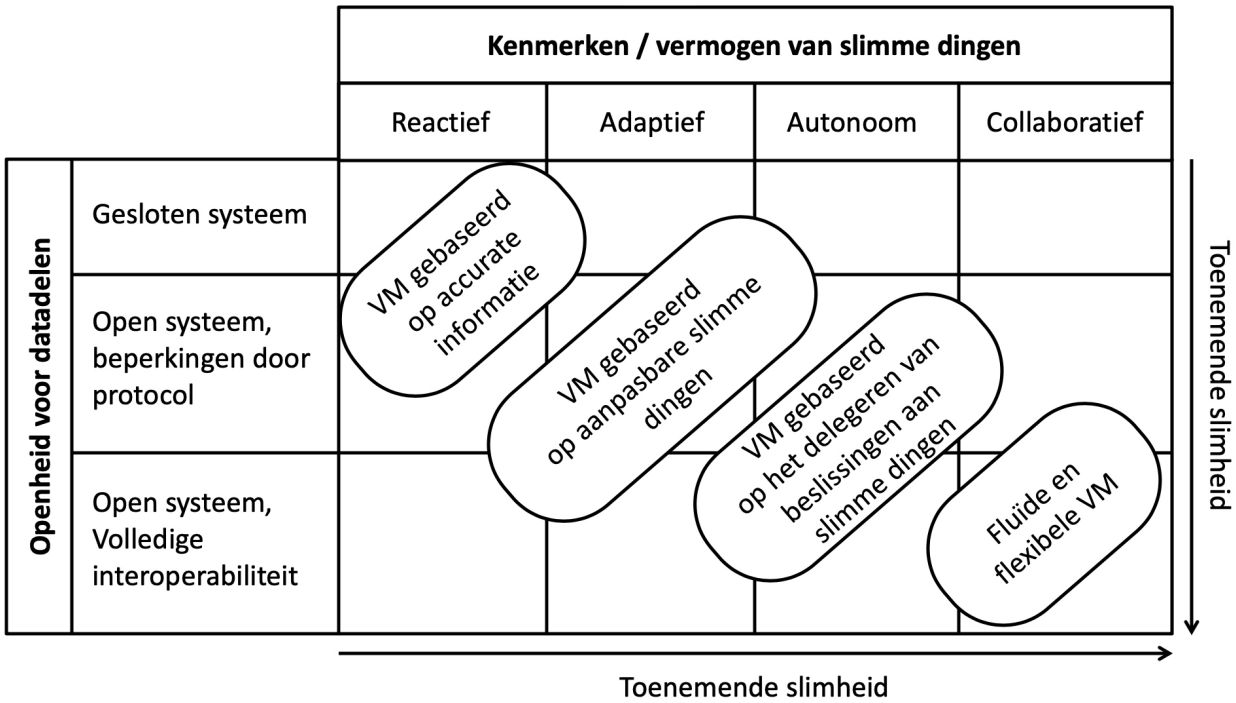
### *A.3.1. Datadelen voor AI in de private sector*

Er is een snelgroeiend aantal voorbeelden van bedrijfsimplementaties van datadelen ten behoeve van AI. Deze omvatten bijvoorbeeld analyses van gedrag op sociale media, beeldanalyse in medische radiologie en diagnostiek, en analyses ten behoeve van gepersonaliseerd beleggingsadvies (fintech).

In Europa zijn meerdere trans-sectorale samenwerkingen ontstaan voor het ontwikkelen van datadelen innovaties in relatie tot AI, waaronder het Zwitserse Dalle Molle Instituut voor Artificial Intelligence (IDSIA), het Duitse Onderzoekscentrum voor Artificial Intelligence (DFKI), het Institute for Analytics and Data Science (IADS) in de VK, en het Insight Centre for Data Analytics in Ierland. Hierbij is er een steeds duidelijker verschil op te merken in de manier waarop data wordt gedeeld afhankelijk van de heersende regelgeving.

Een terminologie voor het beschrijven van de invloed van datadelen met AI op de verdienmodellen van bedrijven is gegeven in [9]. Hierin is een onderscheid te maken tussen de kenmerken of het vermogen van slimme dingen die ontstaan door steeds meer gebruik van AI te maken, zodat de handelingsmogelijkheden van die slimme dingen steeds complexer worden:

- *Reactieve slimme dingen* kunnen snel inspelen op een veranderende omgeving.
- *Adaptieve slimme dingen* kunnen omgaan met veranderingen op de langere termijn door hun gedrag aan te passen, zoals leren van historische gegevens of gebruikspatronen.
- *Autonome slimme dingen* kunnen onafhankelijk handelen, zonder directe tussenkomst van menselijke agenten.
- *Collaboratieve slimme dingen* kunnen communiceren met andere slimme, AI-gebaseerde dingen om samen te werken aan een gezamenlijk doel.




Figuur 8: Niveaus van de slimheid van dingen, voor datadelen en AI, en hun impact op verdienmodellen (VM) [9].

Figuur 8 laat zien hoe bedrijven andere verdienmodellen kunnen ontwikkelen wanneer ze meer datadelen en hogere AI-handelingsmogelijkheden toepassen met toenemende niveaus van de slimheid van dingen:

- In een gesloten datasysteem met reactieve slimme dingen zijn er nieuwe mogelijkheden te vinden door de nauwkeurigheid van de informatie waarmee diensten en processen werken, zoals informatie over de locatie of conditie van dingen.
- Wanneer datadelen opener wordt en slimme dingen adaptief worden, kunnen de diensten of processen steeds aangepast worden op veranderende (gedrags)patronen.
- Met nog een stap richting open datasystemen en autonome dingen, zullen verdienmodellen ontstaan doordat slimme dingen zelf beslissingen uit handen van mensen kunnen nemen; dit is al te zien op kleinere schaal door bots te programmeren voor beleggingen.
- Op het hoogste niveaus van slimme dingen, met volledige open en interoperabele datasystemen en met collaboratieve AI-gedreven dingen, gaan verdienmodellen steeds sneller veranderen om in te spelen op wat op een specifiek moment voor specifieke belanghebbenden gewenst is.

De meeste bedrijven in Nederland bevinden zich nog aan het begin en zullen in de komende jaren steeds meer kennismaken met wat datadelen en AI voor hun verdienmodellen kunnen betekenen. Ze zullen hierbij zelf slim te werk moeten gaan, bijvoorbeeld door krachten te bundelen, willen ze een gezonde concurrentiepositie behouden.

*A.3.2 Datadelen voor AI in de publieke sector*

Overheidsorganisaties in de VS en Engeland zetten AI in om data uit verschillende bronnen over scholieren te analyseren om kwetsbare jongeren te identificeren met een verhoogde risico op uitval, zonder diploma, training of uitzicht op een baan [28]. Op deze wijze kunnen ze tijdig maatregelen nemen.

Het New York kantoor van de burgemeester voor data-analyse (MODA) [29] is een stedelijk platform voor datadelen waarmee gegevens uit verschillende agentschappen worden verzameld en geanalyseerd om problemen met criminaliteit, openbare veiligheid en de kwaliteit van leven effectief aan te pakken. Het platform maakt het mogelijk voor vele overheidsorganisaties, maar ook allerlei bedrijven, om in te spelen op veranderende burgerpatronen, op een efficiënte manier diensten te leveren en om de impact van maatregelen te kunnen monitoren.

Een analyse van het gebruik van AI in de publieke sector [30], beschrijft hoe veranderingen in de uitvoering van publieke taken grote impact hebben op de maatschappij. Naast potentiele voordelen zijn hiermee ook meerdere ethische vragen van belang. Onder de voordelen zijn:

- verbeterde informatieverwerking, waardoor ambtenaren een verhoogde omvang, reikwijdte en snelheid van informatieverwerking kunnen realiseren,
- versnelde afhandeling van zaken, waardoor hogere kwaliteitsnormen en afnemend foutenpercentages kunnen worden bereikt,
- verbeterde toewijzing van zaken, waardoor hooggekwalificeerden vooral hun tijd aan de kernbesluiten kunnen besteden, en
- een duurzame vermindering van de bureaucratie.

De ethische aandachtspunten zijn:

- de risico op verlies van controle, waardoor AI bepalend wordt en kennis over wat er in het systeem gebeurt verloren gaat,
- legitimatie, wanneer AI het recht krijgt om sociale regels vast te stellen of te interpreteren zonder daartoe bevoegd te zijn, en
- databeveiliging en privacy, waardoor de druk op de burger om steeds meer data prijs te geven wordt

opgevoerd totdat er geen sprake van privacy meer is; zo'n alwetend systeem zal vroeg of laat worden misbruikt.

## A.4. Digitale transformatie: het ecosysteem perspectief

Het is in toenemende mate belangrijk voor bedrijven die willen profiteren van AI om goed onder ogen te krijgen wat deze technologie gaat betekenen voor de manier waarop ze samenwerken met anderen. Naast de positieve voordelen zijn er zeker ook risico's die de veranderingen met zich meebrengen, doordat er grootschalige veranderingen nodig zijn in de manier waarop organisaties hun processen organiseren, nieuwe waarde proposities ontwikkelen en hun marktpositie vormgeven. Zulke grootschalige veranderingen die meerdere organisaties betrekken worden aangeduid als "digitale transformatie", omdat deze veel verder gaan dan de eerste digitale stappen die veelal gericht waren op het verbeteren van efficiëntie. Digitale transformatie betreft een volledige herinrichting van de manier waarop waarde wordt gecreëerd, door nieuwe verdienmodellen. In veel sectoren worden waarde proposities die decennialang gezien werden als een legitieme manier van zakendoen nu opeens gezien als verouderd en aan vervanging toe. Door de verstrekkende- en complexe gevolgen van AI, worden meerder bedrijfsprocessen en verdienmodellen in twijfel gebracht. Een maatschappelijk proces van het opnieuw evalueren van legitieme organisatiepraktijken is gaande, waaronder hoe organisaties samenwerken, datadelen en gezamenlijk voordeel ervaren van AI [31].

Sinds het begin van de digitale revolutie vormen bedrijven steeds vaker samenwerkingen en allianties om toegang te krijgen tot uiteenlopende vormen van kennis en middelen die nodig zijn om te innoveren. Deze zogenaamde bedrijfsecosystemen (opererend in een specifieke context van bepaalde regelgeving, financiering en sociaal-culturele kenmerken) moeten zorgen voor nieuwe kenniscombinaties voor wederzijds profijt in plaats van concurrentie. Helaas, blijkt uit onderzoek, lukt het bedrijven vaak niet om die samenwerkingen dusdanig in te richten dat de innovaties succesvol worden. Er zijn hardnekkige problemen die te maken hebben met de governance van de ecosystemen, waaronder wederzijds vertrouwen, het ontstaan van conflicten, en een terughoudendheid in het delen van de eigen kennis en competenties uit angst voor misbruik door ecosysteem partners [32].

Wanneer we uitzoomen naar het institutionele niveau, en een blik werpen op digitale innovatie en -transformatie vanuit een meta-perspectief, dan wordt het mogelijk om grip te krijgen op hoe constellaties van actoren, infrastructuren en praktijken een verandering teweegbrengen in de rules of the game waarbinnen organisaties moeten opereren [33]. De individuele beslissingen van managers binnen een bedrijf zijn onlosmakelijk verbonden met, en beïnvloed door, de institutionele processen en logica op dit meta niveau. Omgekeerd, zodra een individueel bedrijf een bepaalde activiteit uitvoert, zoals het aanbieden van een nieuwe op AI-gebaseerde dienst, heeft dit gevolgen op de uitkomsten van een gehele industrie [34].

Belangrijke organisatorische vragen die opgelost moeten worden gaan over deze transitieprocessen en governance. Het adresseert hoe organisaties kennis, middelen en datadelen. De antwoorden moeten bedrijven in staat stellen om op een effectieve wijze mee te veranderen in het AI-tijdperk.

## A.5. Het faciliteren van datadelen ten behoeve van AI in Nederland: een bedrijf-strategisch perspectief

Als uitgangspunt dient dat het gebruik van AI voor de Nederlandse bedrijven en organisaties zo laag-drempelig mogelijk gemaakt moet worden, bijvoorbeeld door de ondersteunende technologische bouwblokken als diensten aan te bieden. De uitdaging voor de organisaties wordt daardoor minder om de ondersteunende technologie op orde te hebben, waardoor de aandacht en inzet gericht kan worden

op de (kwaliteit en toegevoegde waarde) van de AI en machine learning algoritmes zelf. Een metafoor die Cassie Kozyrkov van Google gebruikt is die van een restauranteigenaar. Zij hoeft niet zelf een geavanceerde oven te ontwikkelen en kan beter haar tijd besteden aan het ontwikkelen van een menu en het inrichten van het restaurant.

Op deze wijze kunnen bedrijven die AI gaan inzetten zich vooral bezighouden met het ontsluiten van de juiste databronnen en het benutten van de resultaten van de AI analyses. Daarbij dient te worden voorkomen dat een klein aantal grote spelers de beste AI kennis opkopen en mijlen ver voorop lopen op 'gewone' bedrijven met het ontwikkelen van de onderliggende algoritmes, een (schrik)beeld dat wordt beschreven in het recente boek van futuroloog Amy Webb [35]. Daarom zijn de vervolgstappen voor Nederlandse bedrijven vooral op deze activiteiten te richten. Hieronder staan vier gebieden die daarbij aandacht verdienen om het productief gebruik van datadelen en AI in Nederland te stimuleren.

### *A.5.1. Voorkom machtsmisbruik*

Het concept self-sovereignty is in dit document eerder uitgelegd. Door datadelen en AI inzet dusdanig vorm te geven dat de data-eigenaren in controle blijven van hun data, en op een makkelijke- en heldere wijze kunnen bepalen en monitoren hoe hun data wordt gebruikt, zal het steeds moeilijker worden voor bedrijven in een positie van macht (zoals doordat ze veel data verzamelen) om die macht te gebruiken ten koste van andere organisaties of van de eindgebruikers.

Hierbij speelt regulering een sleutelrol. De AVG, en andere nationale en Europese wetgeving in ontwikkeling, legt steeds meer verantwoordelijkheid bij organisaties om op een ethische-, transparante- en burgergerichte manier data te gebruiken. Dit leidt tot een situatie waar dataverzameling en -analyse als een basis voor het uitoefenen van macht minder vaak voor zal komen.

Naast regulering is een hoge concurrentieambitie nodig willen Nederlandse bedrijven zich staande weten te houden in het AI-tijdperk. Dit betekent dat bedrijven uit dit land zich niet langer ondergeschikt weten ten opzichte van bedrijven uit de VS of China. Het nemen van weloverwogen risico's en toegang tot durfkapitaal moeten gestimuleerd worden, maar vooral de eigen ambitie is een aandachtspunt. Te veel Nederlandse bestuurders van startups en scale-ups in Nederland hebben een exit strategie om door een buitenlandse tech-reus opgekocht te worden.

### *A.5.2. Stimuleer datadelen kennis/competentie: ontwikkelen, integreren*

Hierboven staat beschreven dat Nederlandse bedrijven drie stappen moeten nemen om kennis en competenties over datadelen en AI te kunnen benutten: het identificeren en vinden ervan, het opnemen ervan in de eigen organisatie, en het integreren ervan in de bestaande producten, diensten en processen om tot kansrijke vernieuwingen te komen. Dit betekent op het landelijke niveau dat er meer aandacht moet komen voor onderwijs, zodat men beter weet welke kennis en competenties nodig en relevant zijn, en de ontwikkelingen kunnen begrijpen en op waarde weten te schatten.

Bovendien moeten er substantiële investeringen worden gedaan om kennis en kennishebbenden in het land te houden en te ontwikkelen. Met vele infrastructurele ontwikkelingen neemt de overheid een belangrijke stimulerende rol op zich om haar bedrijven niet achter te laten lopen. Ook voor nieuwe technologieën, kennis en competentieontwikkeling op het gebied van datadelen en AI zullen overheid en bedrijfsleven gezamenlijk moeten optrekken.

Er moeten communities of practice ontstaan voor het delen van kennis en ervaringen om een transsectorale aantrekkingskracht te bieden in het belang van Nederland.

### *A.5.3. Ecosysteem governance voor datadelen*

Door de toenemende complexiteit in datadeel ecosystemen, is er ook in termen van governance een belangrijke rol weggelegd voor de overheid, zowel bij ministeries als lokale overheden, om ervoor te zorgen dat de incentives / prikkels die bedrijven ervaren om mee te doen met datadelen en het inzetten van AI oplossingen over organisatiegrenzen heen elkaar niet tegenwerken.

Hierbij is er een sleutelrol voor onafhankelijke 'orchestrators' die, zonder concurrentiegevoeligheid, geschikte datadeel partners bij elkaar weten te brengen en de voorwaarden voor samenwerking goed weten te borgen.

### *A.5.4. Toon voordelen van flexibele besluitvorming aan*

Er is een mindset verandering nodig onder bedrijfsbestuurders om niet vanuit angst van wat mis kan gaan door data te delen, maar de kansen willen zien en daaraan concrete stappen durven te koppelen. Dit kan worden bereikt door steeds aansprekende voorbeelden te etaleren en breed te bediscussiëren.

Hierbij is een belangrijke verandering nodig in de strategische flexibiliteit van Nederlandse bedrijven. Data-gedreven AI vraagt om een zeer open houding wat betreft de manier van bedrijfsvoering, waarde proposities ontwikkelen in ketens en steeds opnieuw bekijken hoe klanten het beste bediend kunnen worden. Overheid en andere partijen zijn dus gebaat bij het promoten van Nederlandse voorbeelden van strategische flexibiliteit, zoals van fluïde en flexibele verdienmodellen die op een nauwkeurige en waardevolle manier inspelen op nieuwe kansen.

# APPENDIX B: Samenwerkingsmodellen: data, algoritme en resultaat

Een datagestuurd AI-algoritme kent doorgaans zowel een trainingsfase als een operationele fase. Een kennisgestuurd AI-algoritme kent alleen een operationele fase. Zowel de trainingsfase als de operationele fase kunnen worden gekarakteriseerd door een samenwerkingsmodel. Deze definieert de rollen van de betrokken partijen: wie levert data aan, wie verwerkt die data middels het AI-algoritme, en wie gebruikt die data? Deze vragen zijn relevant voor het onderwerp van (gecontroleerd) datadelen voor AI. Het samenwerkingsmodel is namelijk bepalend voor:

- het type van de data dat tussen partijen daadwerkelijk wordt gedeeld: betreft dit de ruwe 'input-data' of de 'verwerkte' data? Hoe gevoelig is deze data?;
- welke (onafhankelijke) organisaties de data nu daadwerkelijk delen en waartussen daarom afspraken voor gecontroleerd datadelen moeten worden gemaakt;
- wat de behoefte aan bijpassende, federatieve, consent management eisen en architecturen zijn om afspraken en autorisaties tussen en over de verschillende partijen te beheren en borgen, en;
- wat de performance eisen zijn (snelheid, communicatie, autorisatie) van de toepassing en of / hoe die met een gedistribueerd veilig AI-algoritme kunnen worden gerealiseerd.

Een samenwerkingsmodel kan worden gerealiseerd met verschillende datadeel technieken. Een overzicht van deze datadeel technieken wordt in appendix D gegeven.

In deze appendix beschrijven we de samenwerkingsmodellen. Tevens beschouwen we een aantal afwegingen, waaronder de keuze/selectie-methodiek om tot een adequaat samenwerkingsmodel te komen, de corresponderende datadeel interfaces (bij organisatie-overgangen), de typering van te delen data, het ontwerp van een veilig gedistribueerd algoritme, en de gevolgen voor de benodigde autorisatie architectuur.

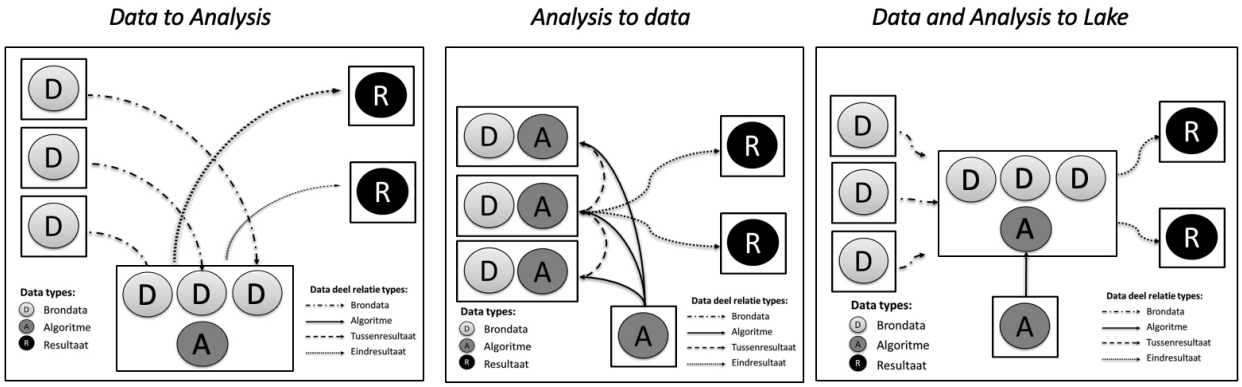
## B.1. Ontwerp opties: samenwerkingsmodellen

De samenwerkingsmodellen beschrijven de samenwerking tussen drie belangrijke partijen (organisaties) voor datadelen ten behoeve van AI:

1. de organisaties of personen die de brondata aanleveren;
2. de organisaties die het AI-algoritme uitvoeren;
3. de organisaties die de resultaten van het AI-algoritme krijgen.

Van elk van de type organisaties kunnen er één of meer instanties betrokken zijn bij het samenwerkingsmodel. Het is mogelijk dat eenzelfde organisatie verschillende onderdelen aanlevert, bijvoorbeeld wanneer één van de organisaties die brondata aanlevert ook het algoritme uitvoert.

Wanneer meerdere organisaties daadwerkelijk willen gaan samenwerken in het ontwikkelen en/of benutten van data-gedreven AI analyses, ontstaat de nieuwe uitdaging over de keuze van een geschikt samenwerkingsmodel, zowel voor de trainingsfase als voor de operationele fase van het AI-algoritme. Voor een deel ligt dat model al vast. Het is bijvoorbeeld duidelijk welke partijen welke brondata in gaan brengen, en wie de resultaten van de analyse gaan krijgen. Soms is er daarbij wel de keuze welke organisatie(s) het algoritme gaan uitvoeren. Daarbij zijn drie basis keuzes te onderkennen, i.e. de samenwerkingsmodellen, zoals geïllustreerd in Figuur 9.




Figuur 9: Samenwerkingsmodellen: 'Data-to-Analysis' (l), 'Analysis to data' (m) en 'Data-and-Analysis-to-Lake' (r).

De drie basis samenwerkingsmodellen zoals geïllustreerd in de figuur zijn:

- *Data-to-Analysis*: De data wordt naar (de uitvoerders van) het AI-algoritme gestuurd en daar verwerkt, samen met data van andere bronnen.

  Een voorbeeldtoepassing voor dit samenwerkingsmodel is het beschikbaar stellen van overheidsdata aan andere partijen. Dit kan het CBS zijn, de Belastingdienst, etc. Deze organisaties kunnen daar hun data analyse op toepassen en de geanalyseerde resultaten beschikbaar stellen voor een breder publiek.

- *Analysis-to-Data:* Het AI-algoritme wordt naar de aanbieders van de databronnen gestuurd, en wordt in hun organisaties uitgevoerd. M.b.v. onderlinge combinatie en communicatie wordt tot een gezamenlijk eindresultaat gekomen.

  Een voorbeeldtoepassing voor dit samenwerkingsmodel is het zoeken van afwijkend gedrag in netwerk verkeer, zodat organisaties cyber security aanvallen kunnen detecteren. Alle organisaties hebben een eigen netwerk dat ze beheren, waar digitaal verkeer overheen gaat. Gezamenlijk kunnen ze een goed overzicht krijgen van verdacht verkeer, wat kan duiden op een cyber security aanval.

- *Data-and-Analysis-to-Lake*: De data wordt centraal bij een vertrouwde derde partij verzameld (een 'data lake'), en het AI-algoritme wordt daar uitgevoerd. De vertrouwde derde partij communiceert de resultaten verder naar de belanghebbende organisaties.

  Een voorbeeldtoepassing voor dit samenwerkingsmodel is het analyseren van genetische data van verschillende biobanken. Elke biobank levert gevoelige genetische data, die niet door anderen mag worden ingezien. Gezamenlijk laten de biobanken AI-algoritmen los op de virtueel gedeelde data voor medische doeleinden.

  Een ander voorbeeld is dat van een cloud service provider waarbij organisaties hun data opslaan en daarop gezamenlijk een AI-algoritme loslaten. De cloud service providers leveren deze mogelijkheid als dienst.

## B.2. Ontwerpaspecten

Zoals de voorbeelden in de vorige sectie illustreren is het kiezen van het juiste samenwerkingsmodel doorgaans maatwerk en zal per use case bekeken moeten worden. De verschillende samenwerkingsmodellen hebben hun eigen kenmerken, die bepalend zijn voor de (technische inrichting van) de ondersteunende infrastructuur. Daarbij zijn generieke bouwblokken in de ondersteunende datadeel infrastructuur nodig die de grote diversiteit aan

data analyse toepassingen op basis van de verschillende samenwerkingsmodellen zo laagdrempelig mogelijk aan de gebruikers ter beschikking stellen, zodat het gebruik ervan voor de organisaties zo behapbaar en laagdrempelig mogelijk wordt. In sectie 4.1 , Figuur 4, is daarbij een initiële opzet van een gelaagd ecosysteem van rollen met generieke bouwblokken op twee 'lagen': de laag voor het laagdrempelig toegankelijk maken van ondersteunende data analyse functies en de laag voor het ondersteunen van de daarvoor benodigde datadeel functies.

Er zijn daarbij enkele theoretische hulpmiddelen ontwikkeld voor het ondersteunen van de selectie voor een specifiek samenwerkingsmodel. Voor "digitale data markten" worden in [36] metingen beschreven die ondersteuning bieden voor de technische invulling van het samenwerkingsmodel. Verder heeft TNO de CO-ARCH methodologie ontwikkeld [37] om inzicht te krijgen in het vereiste samenwerkingsmodel en te komen tot concrete technische IT blueprints voor elk van de betrokken organisaties.

Voor het ontwerp en de inrichting van het samenwerkingsmodel is een aantal ontwerpaspecten van belang. Deze worden in de volgende paragrafen beschreven.

### *B.2.1. Gedistribueerd AI-algoritme*

AI-algoritmen zijn doorgaans intensieve algoritmen in de trainingsfase, met veel iteraties die veel rekenkracht kosten. In de verschillende samenwerkingsmodellen kan er ook nog veel communicatie bij komen kijken vanwege het transport van data en de gedistribueerde uitvoering van het algoritme. Bovendien zorgt de gevoeligheid van data ervoor dat extra security mechanismen moeten worden ingebouwd. Dat betekent dat de performance eisen wel eens in het gedrang kunnen komen: zijn de resultaten tijdig beschikbaar, zijn de interfaces in staat om voldoende data per tijdseenheid te transporteren, lekt er geen gevoelige data naar ongeautoriseerde partijen? Wanneer data niet gedeeld hoeft te worden, of op één plek kan worden opgeslagen, kan het AI-algoritme lokaal (bij één partij) worden geoptimaliseerd. Als het samenwerkingsmodel en de gestelde eisen aan gevoelige data dit niet toestaan, dient het AI-algoritme gedistribueerd te worden uitgevoerd, met additionele security mechanismen om te zorgen dat tussenresultaten geen beveiligingslek vormen.

Dat betekent een gedistribueerd en veilig ontwerp van het AI-algoritme, waarvoor de juiste expertise en ervaring nodig is. In het bijzonder wanneer organisaties verschillende gevoelige informatie hebben over dezelfde personen, is dit een uitdaging.

### *B.2.2. Datadeel interfaces: formaat en beschikbaarheid*

Het samenwerkingsmodel beschrijft welke partijen data gaan aanleveren en aan wie. Dat betekent dat er afspraken gemaakt moeten worden over het formaat van die data (syntax), de betekenis ervan (semantiek), en welke interfaces gebruikt worden voor de uitwisseling ervan.

De uitvoering van het AI-algoritme zal doorgaans op een gedistribueerde manier (over verschillende partijen) plaatsvinden. De meeste AI-algoritmen kennen ook een iteratieve aanpak, wat betekent dat er herhaaldelijk data gedeeld zal moeten worden tussen de verschillende partijen. Dit heeft gevolgen voor de datadeel interfaces en stelt eisen aan de tijdige beschikbaarheid van de juiste data.

### *B.2.3. Consent / autorisatie architectuur*

Een andere zeer relevante organisatie specifieke eigenschap van data is de gevoeligheid ervan. Aan welke juridische, vaak privacy gerelateerde eisen, dient de (bewerking van de) data te voldoen? Welke (soort) partijen mogen de data inzien? Vanuit de AVG is doorgaans toestemming (consent) van de persoon nodig om persoonsgegevens voor een bepaald doel te mogen verwerken. Indien nodig moeten de organisaties hier dus voor zorgdragen.

Los van de juridische aspecten kan data ook vanuit commercieel perspectief gevoelig zijn, en kan deze niet zomaar gedeeld worden. Dit soort kenmerken zijn zeer bepalend voor de technische inrichting van het platform, en de benodigde architectuur voor het beheren van consent en autorisaties ('machtigingen').

### *B.2.4. Data kwaliteit management*

Niet alleen de syntax en semantiek van de te delen data is relevant, maar ook de kwaliteit ervan. Afhankelijk van hoe data wordt opgeslagen binnen de organisatie, dienen er verschillende bewerkingsslagen te worden gedaan voordat de data aan de datadeel interfaces kan worden aangeboden. Denk bijvoorbeeld aan het omgaan met ontbrekende waarden, het categoriseren van data, het herstellen van foute data, etc. Voor- en nabewerking van data kan nodig zijn om aan kwaliteitseisen van de AI-algoritmen en van de data-ontvanger te voldoen.

### *B.2.5. Beschouwingen op de ontwerpaspecten*

De vier genoemde ontwerpaspecten zijn in elk samenwerkingsmodel in meer of mindere mate aan de orde. Tabel 4 geeft een indicatie van de complexiteit van elk van de ontwerpaspecten voor de drie basis samenwerkingsmodellen.

Het gedistribueerd ontwerp van het AI-algoritme zal met name complexiteit opleveren wanneer het AI-algoritme door verschillende organisaties zal worden uitgevoerd. Dit betreft daarom met name het 'analysis-to-data' samenwerkingsmodel.

De interface complexiteit (de hoeveelheid afstemming en afspraken die daarvoor gemaakt moeten worden) hangt af van de hoeveelheid interfaces, de vergelijkbaarheid en de individuele complexiteit ervan. Deze is het geringst voor het 'analysis-to-data' samenwerkingsmodel.

Hoe meer restricties er zijn op de (gevoelige) data, hoe hoger de complexiteit van de consent / autorisatie architectuur. In het 'analysis-to-data' samenwerkingsmodel betreft dit alleen (tussen) resultaten, waardoor de complexiteit in dit geval het laagst zal zijn. Kanttekening is wel dat de juridische noodzaak voor user consent sterk afhankelijk is van de specifieke use case, en de overige security maatregelen die genomen zijn.

Het datakwaliteit aspect hangt af van de hoeveelheid data waarvan de kwaliteit zal moeten worden beheerst. Voor elk van de samenwerkingsmodellen zal dit vergelijkbaar 'hoog' zijn, ongeacht of de data naar de analyse wordt gebracht of v.v.

| **Model** | *Data-to-Analysis* | *Analysis-to-Data* | *Data-and-Analysis-to-Lake* |
|---|---|---|---|
| **Gedistribueerd algoritme** | Laag | Hoog | Laag |
| **Interface complexiteit** | Hoog | Medium | Hoog |
| **Consent/autorisatie** | Medium | Laag | Hoog |
| **Data kwaliteit beheer** | Hoog | Hoog | Hoog |

Tabel 4: Complexiteit van ontwerpaspecten per samenwerkingsmodel

## B.3. Digitale datamarkten: besturingsmodel

Bij het datadelen ten behoeve van AI is er een aantal organisaties die hun krachten bundelen en datadelen om een AI-algoritme uit te voeren. In de uitvoeringsketen dienen ze hierbij allen baat te hebben om daadwerkelijk de keten in gang te zetten en houden. Digitale datamarkten kunnen hiervoor een besturingsmodel vormen, waarbij de verschillende organisaties elkaar kunnen 'ontmoeten' en tot afspraken kunnen komen: organisaties die data aanleveren (de aanbieders), organisaties die het markt algoritme uitvoeren, en organisaties die de resultaten gebruiken (de vragers).

Een voorbeeldtoepassing in dit samenwerkingsmodel is de digitale veiling. De aanbieders van data (of goederen) brengen hun data in, de vragers zijn geïnteresseerd in de data (of goederen). Het veiling algoritme wordt uitgevoerd via het platform door de marktorganisaties, die op een veilige manier, rekening houdende met de commerciële strategieën van de vragers en aanbieders, dat een economisch verantwoorde prijs ontstaat voor de goederen. Aanbieders hebben bijvoorbeeld een minimum prijs waarvoor ze hun goederen willen verkopen, en vragers een maximum prijs waarvoor ze willen kopen, en de taak van de rekenpartijen is om aan die voorwaarden te voldoen, zonder dat die commerciële informatie bij de verkeerde partijen bekend wordt.

Om de digitale datamarkten te faciliteren zijn in de ondersteunende datadeel infrastructuur specifieke bouwblokken nodig die de leverende en vragende partijen bij elkaar brengen en het daadwerkelijk delen van data en algoritmes mogelijk maken en ondersteunen. De generieke bouwblokken in de initiële opzet van het gelaagd ecosysteem in sectie 4.1, Figuur 4, kan daarvoor worden gebruikt.

# APPENDIX C: Juridisch kader

Eén van de factoren die de beschikbaarheid, het gebruik en de uitwisseling van data beperkt is het juridisch kader (wettelijke regime), of juist het ontbreken daarvan.

In de achtereenvolgende secties van deze appendix worden twee belangrijke aspecten van het juridisch kader voor datadelen ten behoeve van AI uitgediept: de wettelijke bepalingen voor het delen van persoonlijke data en de wettelijke eisen aan en onderdelen van de datadeel overeenkomsten waarin de juridische, commerciële en gebruiksvoorwaarden worden vastgelegd.

## C.1. Wettelijke bepalingen voor het delen van persoonlijke data

Bij het delen van data is het van belang om na te gaan of sprake is van het delen van data die tot een persoon te herleiden is. Voor deze data geldt sinds mei 2018 de Algemene Verordening Gegevensbescherming (AVG). De AVG geeft invulling aan artikel 8 van het Handvest van de Grondrechten van de Europese Unie: "*Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.*". Het gaat hierbij overigens niet zozeer om de directe afscherming van persoonsgegevens (beveiliging van gegevens) maar om de bescherming van een persoon betreffende de verwerking van zijn persoonsgegevens, zoals uit vergelijking met andere wettelijke kaders blijkt (onder meer Conventie 108 van de Europese Unie).

In Nederland is de AVG uitgewerkt in de Uitvoeringswet AVG (UAVG). De UAVG neemt de AVG als uitgangspunt en vult deze aan daar waar de AVG dit toestaat. Omdat de AVG een verordening is heeft deze directe doorwerking in alle lidstaten (specifieker: alle landen die deel uitmaken van de Europese Economische Ruimte). De AVG biedt een wettelijk kader dat op onderdelen nadere precisering behoeft. Zo spreekt de AVG over gegevensbescherming door ontwerp en door standaardinstellingen zonder in detail duidelijk te maken wat dit inhoudt. Hier zal in de loop der tijd nadere invulling aan worden gegeven, onder meer door de Europese Commissie zelf en door de Europese privacy toezichthouders, verenigd in de Europese Groep van Gegevensbeschermers (European Data Protection Board).

In de volgende paragrafen worden de belangrijkste bepalingen van de AVG toegelicht, uitgaande van de verwerking van persoonsgegevens, inclusief bepalingen die de AVG stelt ten aanzien van geautomatiseerde besluitvorming. De toepassingen van AI-algoritmes zullen met deze bepalingen te maken kunnen krijgen. Ook wordt kort stil gestaan bij het bredere kader dat discriminatiewetgeving biedt. In de tekst wordt op enkele plaatsen gerefereerd aan de bijzondere positie van wetenschappelijk onderzoek binnen de AVG.

### *C.1.1. Beginselen van de AVG*

De AVG is van toepassing op data die tot een natuurlijke persoon te herleiden is. Dat wil zeggen dat een persoon direct ("Dit is Karel") of indirect ("Dit is een persoon die in deze groep te herkennen is vanwege zijn specifieke haarkleur") te identificeren is. De AVG is alleen van toepassing op levende personen. Wel kan het zijn dat nabestaanden bepaalde rechten kunnen laten gelden, bijvoorbeeld omdat zij indirect ook identificeerbaar zijn door de gegevens van de overledene. De AVG biedt bescherming aan alle personen die zich binnen de EU bevinden (ook toeristen) en geldt voor alle activiteiten waarin persoonsgegevens van personen binnen de EU verwerkt worden (art 3: territorialiteitsbeginsel). Het begrip 'verwerken' is ruim gedefinieerd (art 4, lid 2): verzamelen, structureren, organiseren, opslaan, aanpassen, terugvinden, raadplegen, gebruiken, ontsluiten bij verzending, vernietigen van persoonsgegevens vallen alle onder verwerken.

Om data te mogen verwerken moet een aantal beginselen in acht genomen worden (art 5). Deze beginselen vormen de kern van de AVG. Data moet:

1. rechtmatig, transparant en behoorlijk worden verwerkt;.
2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet verder worden verwerkt op manieren die niet overeenkomen met die doeleinden ('doelbindingsprincipe');
3. toereikend en ter zake zijn en beperkt tot wat noodzakelijk is ('dataminimalisatieprincipe');
4. juist zijn en zo nodig geactualiseerd ('kwaliteitsprincipe');
5. worden bewaard op een manier waardoor personen niet langer identificeerbaar zijn dan echt nodig is;
6. beveiligd worden door het treffen van passende technische en organisatorische beveiligingsmaatregelen.

Deze principes moeten altijd in acht genomen worden. Ze zijn in de AVG verder uitgewerkt. Uitgangspunt daarbij is dat de verwerking noodzakelijk is in een democratische samenleving en dat de verwerking proportioneel is (inbreuk op de rechten en vrijheden van betrokkenen die passend is voor het doel dat wordt nagestreefd) en dat ook gekeken wordt naar de mogelijkheid om de inbreuk zo beperkt mogelijk te houden door toepassing van andere verwerkingsmaatregelen (subsidiariteit).

Tegelijkertijd is ook duidelijk dat de principes nadere invulling behoeven. Zo is het begrip 'passend' niet verder gearticuleerd in de AVG zelf, op enkele basale aanduidingen na. Die invulling biedt een zekere speelruimte aan de verwerkingsverantwoordelijke (de persoon of organisatie die verantwoordelijkheid draagt voor de verwerking, dat wil zeggen doel en middelen bepaalt van de verwerking).

In het geval van verwerking van persoonsgegevens voor wetenschappelijk en historisch onderzoek (of archivering in het algemeen belang of verwerking voor statistische doeleinden) gelden bepaalde uitzonderingen. Zo wordt voor deze verwerkingen verondersteld dat – indien sprake is van de verwerking van al eerder verzamelde gegevens – het doel van de verwerking niet in strijd is met het oorspronkelijke doel. Er wordt in die gevallen dus altijd aan de eis van doelbinding voldaan. Wel is dan nog een legitieme grondslag nodig (zie volgende paragraaf). Voor wetenschappelijk onderzoek mogen betrokkenen (de personen over wiens gegevens het gaat) ook aangeven dat hun gegevens voor ruim aangegeven doeleinden van onderzoek mogen worden ingezet ('domeinen van onderzoek'). Dit, omdat het doel van het onderzoek niet altijd op voorhand nauwkeurig is aan te geven. Het onderzoek moet dan wel aan aanvullende ethische waarborgen voldoen.

### *C.1.2. Grondslagen voor verwerking*

De AVG geeft zes grondslagen die aangeroepen kunnen worden om de rechtmatige verwerking van data aan te tonen. Iedere verwerking moet aantoonbaar aan ten minste één van deze grondslagen voldoen. Het betreft de volgende grondslagen (art. 6):

1. de verwerking vindt plaats op grond van de vrijelijk gegeven, specifieke, geïnformeerde en ondubbelzinnige toestemming van de betrokkene;
2. de verwerking is noodzakelijk om aan een overeenkomst te voldoen;
3. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting;
4. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of een derde te beschermen;
5. de verwerking is noodzakelijk voor de uitvoering van een taak van algemeen belang;
6. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde.

De eerste grondslag wijkt af van de andere vijf. Grondslag

2 tot en met 6 geven een noodzakelijkheid aan: het is noodzakelijk om gegevens te verwerken vanwege een contract, een publieke taak, etc.. In feite geeft dit ook de aanpak aan van het aanroepen van een grondslag: kijk of er sprake is van een noodzaak tot verwerking van gegevens (die correspondeert met de grondslagen 2 tot en met 6) en alleen als dit niet mogelijk is, kan de eerste grondslag (toestemming) ingeroepen worden. Daarmee is toestemming de grondslag die alleen dan wordt ingeroepen als er geen noodzakelijkheid voor de gegevensverwerking aangevoerd kan worden. Bij grondslag vijf (taak van algemeen belang) wordt verondersteld dat deze taak ook een grond vindt in een wettelijke regeling. Dat hoeft niet een wettelijke regeling te zijn die één op één naar deze taak verwijst. De laatste grondslag, het gerechtvaardigd belang, is een lastige. In de Overwegingen van de AVG wordt verwezen naar voorbeelden als fraudebestrijding en direct marketing (Overweging 47). Ook wordt daarin verwezen naar de verwachting van betrokkenen: kan een betrokkene in redelijkheid verwachten dat zijn/haar gegevens voor dat specifieke doel verwerkt worden? Rond deze grondslag speelt momenteel de vraag hoe breed dit gerechtvaardigd belang genomen mag worden.

### *C.1.3. Gewone gegevens en bijzondere gegevens*

De AVG maakt onderscheid tussen '*gewone persoonsgegevens*' en '*bijzondere categorieën van persoonsgegevens*' (art. 9). Waar de AVG voor de gewone (dat wil zeggen: de gegevens die niet tot een bijzondere categorie behoren) een "Ja, mits …" benadering voorstaat, is dat bij de bijzondere categorieën een "Nee, tenzij …" benadering. Alleen als er een specifieke uitzonderingsgrond ingeroepen kan worden, is het toegestaan deze gegevens te verwerken. Uiteraard moet er ook dan een legitieme grondslag en een rechtmatig doel kunnen worden aangevoerd.

De AVG geeft een limitatieve opsomming van de bijzondere categorieën van persoonsgegevens: "… *persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid …*" (art. 9).

De uitzonderingsgronden om deze gegevens toch te mogen verwerken zijn velerlei, waaronder uitdrukkelijke toestemming (blijkend uit een op schrift gestelde verklaring), noodzaak vanwege wettelijke voorschriften in specifieke omstandigheden (arbeidsrecht, sociale zekerheids- en sociale beschermingsrecht), een zwaarwegend algemeen belang, gegevens die kennelijk openbaar zijn gemaakt, belang voor de volksgezondheid, arbeidsgeneeskunde en wetenschappelijk/historisch onderzoek.

Van belang voor datadelen ten behoeve van AI-gerelateerde activiteiten is het verbod dat de AVG daarnaast maakt om bij automatische besluitvorming waarvan het besluit een rechtsgevolg of ander aanmerkelijk effect veroorzaakt, bijzondere categorieën van persoonsgegevens te gebruiken. Dit wordt verder geadresseerd in paragraaf C.1.6.

### *C.1.4. Rechten van betrokkenen*

Om rechten uit te kunnen oefenen moet een betrokkene weet hebben van de verwerking van zijn of haar gegevens. Het informeren van de betrokkene over een verwerking, het doel ervan, de gevolgde aanpak, de partijen die verantwoordelijk zijn voor de verwerking, en de logica van de gebruikte algoritmes hoort bij het transparantiebeginsel van de AVG. Hier kan alleen van worden afgeweken bij wetenschappelijk onderzoek waar deze bekendmaking in redelijkheid niet gevraagd kan worden of waar bekendmaking negatief op de resultaten van het onderzoek uit zou werken (art 89, lid 2). In alle andere gevallen dient de betrokkene uitvoerig te worden geïnformeerd. Alleen dan kunnen betrokkenen hun rechten fatsoenlijk uitoefenen. Die rechten zijn (art. 15, 16, 17, 18, 20, 21):

- het recht op inzage,
- het recht op rectificatie, het recht op gegevensverwijdering,
- het recht op beperking van de verwerking,
- het recht op gegevensoverdracht, en
- het recht op bezwaar tegen verwerking.

Deze rechten zijn in sommige gevallen aan restricties verbonden. Zo mag afgeweken worden van deze rechten in het geval van wetenschappelijk onderzoek (geldt voor art. 15, 16, 18 en 21; zie artikel 89, lid 2). Maar in de regel vormen ze het fundament voor betrokkenen om een zekere mate van regie over hun gegevens te kunnen voeren.

### *C.1.5. Plichten van verwerkingsverantwoordelijken*

Tegenover deze rechten staan plichten van de verwerkingsverantwoordelijken. Behalve het voldoen aan de rechten van betrokkenen bestaan deze plichten uit de plicht om een registratie bij te houden van verwerkingen, en om passende veiligheidsmaatregelen te treffen (art. 30, 24, 25 en 32). Een verwerkingsverantwoordelijke heeft ook de plicht om zich ervan te vergewissen dat een verwerker (een partij die werkt in opdracht van de verwerkingsverantwoordelijke) in staat is om aan de plichten te voldoen rond gegevensbeveiliging (art 28 en 29). Een datalek moet gemeld worden (tenzij dit lek geen privacyrisico oplevert voor de betrokkene; art 33 en 34). Tot slot, bij verwerkingen met een hoog risico is een gegevensbescherming beoordeling verplicht. Zo'n beoordeling impliceert ook dat gekeken wordt naar maatregelen om geconstateerde privacyrisico's aan te pakken. Blijkt dit niet mogelijk dan moet de Autoriteit Persoonsgegevens om advies over de voorgenomen verwerking worden gevraagd (art. 35 en 36).

### *C.1.6. Automatische besluitvorming en profilering*

Een aparte categorie van gegevensverwerking betreft die verwerkingen waarbij sprake is van volledig geautomatiseerde besluitvorming. Dit houdt in dat een systeem zonder enige vorm van menselijke tussenkomst tot een besluit komt. Het gaat dan om besluiten die rechtsgevolgen hebben (bijvoorbeeld de toekenning van een uitkering) of andere aanmerkelijke effecten (bijvoorbeeld al dan niet door een wervingsprocedure heen komen). Dit soort systemen is niet toegestaan. Dit zou dus zeker kunnen gelden voor systemen die gebruik maken van AI of machine learning en volledig zelfstandig tot een besluit komen. Zolang een dergelijk besluit geen rechtsgevolgen heeft of een ander aanmerkelijk effect is er niet veel aan de hand. Pas als sprake is van een besluit met rechtsgevolgen of een ander aanmerkelijk effect stelt de AVG dat dit niet is toegestaan. Zo'n besluit mag dus niet volledig door een systeem afgehandeld worden.

Ook hier biedt de AVG echter een aantal uitzonderingen (art 22, lid 2). Het is toegestaan volledig geautomatiseerde besluitvorming toe te passen voor het afsluiten van een overeenkomst of als sprake is van de uitdrukkelijke toestemming van de betrokkene. Daarnaast mag een dergelijk systeem gebruikt worden om te voldoen aan een Unierechtelijke of lidstaatrechtelijke bepaling, mits voldoende waarborgen zijn getroffen om de rechten en vrijheden van de betrokkene te beschermen. In het eerste geval (overeenkomst of uitdrukkelijke toestemming) moet overigens wel sprake zijn van betekenisvolle menselijke tussenkomst, waardoor niet langer sprake is van een volledig geautomatiseerde besluitvorming. Waar de tekst van de AVG zelf spreekt over een recht op menselijke tussenkomst (daarmee suggererend dat een actie van een betrokkene nodig is om dit recht te effectueren) hebben de toezichthouders dit restrictief uitgelegd: het betekent dat er geen specifiek beroep op deze uitzondering gedaan hoeft te worden maar de verwerkingsverantwoordelijke dat in alle gevallen moet regelen [38].

Tot slot stelt art 22 dat de verwerking van bijzondere categorieën van persoonsgegevens via automatische besluitvorming alleen is toegestaan als er sprake is van uitdrukkelijke toestemming van de betrokkene of als de verwerking noodzakelijk is vanwege een zwaarwegend maatschappelijk belang (art 22, lid 4).

Binnen de AVG worden problemen rond profilering (de geautomatiseerde evaluatie van een persoon op basis van bepaalde persoonskenmerken om daarmee specifieke situationele kenmerken – economische situatie, gezondheid, beroepsprestaties, etc. – te analyseren of te voorspellen) veelvuldig op een lijn gesteld met problemen rond automatische besluitvorming. De veronderstelling hierachter is dat het opstellen van een profiel een volledig geautomatiseerd besluitvormingsproces kan zijn dat vervolgens een dwingend karakter heeft voor de personen die aan de betreffende kenmerken voldoen en ook tot rechtsgevolgen of tot een ander aanmerkelijk effect kan leiden. AI en machine learning systemen zijn door hun vermogen tot clustering en herkenning van patronen systemen die aan de basis van vele profileringsstrategieën kunnen staan.

### *C.1.7. Logica van algoritmes*

In het kader van de transparantie rond de gegevensverwerking geeft de AVG ook aan dat betrokkenen "nuttige informatie" over de logica van de geautomatiseerde besluitvorming moeten krijgen (art. 13, 14 en 15). Wat dit in de praktijk in moet houden is onderwerp van discussie. Soms wordt de vrees geuit dat dit kan betekenen dat organisaties inzicht moeten geven in hun bedrijfsgeheimen. Ook is de vrees te beluisteren dat dit voor specifieke besluitvormingssystemen intrinsiek niet mogelijk is (bijvoorbeeld bij neutrale netwerken).

Een overzicht van de discussie en een uitwerking van wat bekend staat als de functionele insteek kan gevonden worden in [39]. Hoewel de discussie nog zeker niet ten einde is, lijkt deze functionele insteek hier een goed richtsnoer te bieden. Die houdt in dat gezocht wordt naar het bieden van informatie die door betrokkenen te begrijpen is en die de kern van de aanpak weergeeft zonder dat per se de exacte werking van de achterliggende algoritmes toegelicht moet worden. Daarmee komt het recht op nuttige informatie te staan in het licht van de transparantie-eisen die de AVG stelt en de mogelijkheden om betrokkenen zinvol te betrekken bij een zekere mate van regie over wat er met hun gegevens gebeurt.

### *C.1.8. Het verbod op discriminatie en de rechten van de mens*

Behalve de AVG zijn ook andere wettelijke kaders van belang voor het delen en verwerken van data voor AI-systemen. Het verbod op discriminatie dat ook in de AVG te vinden is (zie Overwegingen 75 en 85) vindt zijn sterkste uitwerking in het Europees Verdrag voor de Rechten van de Mens (EVRM), in Nederland terug te vinden in artikel 1 van de Grondwet en in het strafrecht. In Nederland is het College voor Bescherming van de Rechten van de Mens de instantie die ziet op de bescherming van deze rechten. Daarmee heeft dit College een duidelijke taak, naast de Autoriteit Persoonsgegevens die ziet op de naleving van de (U) AVG.

Een verschil tussen de AVG en de grondwettelijke bescherming tegen discriminatie is dat er in het geval van discriminatie een duidelijke casus aangegeven moet worden waarin de discriminatie zichtbaar gemaakt kan worden. De rechtsbescherming bij de AVG kan daarentegen ook ingeroepen worden wanneer bepaalde regels niet of niet goed gevolgd zijn. Discriminatie kan op directe wijze of op indirecte wijze plaatsvinden. Discriminatiegronden vanuit het strafrecht overlappen ten dele met de bijzondere categorieën van persoonsgegevens uit de AVG maar bevatten ook gronden die niet in de AVG genoemd worden zoals gender en leeftijd.

### *C.1.9. Bias*

Een probleem dat verbonden lijkt te zijn aan het gebruik van grote datasets is dat deze sets op een of andere wijze onderhevig zijn aan een vorm van bias. Dit kan ook leiden tot nieuwe vormen van discriminatie, zoals op basis van een device die iemand gebruikt. De nieuwe vormen van discriminatie die hierbij kunnen ontstaan

door AI worden belicht in [40]. Het onderkennen en aanpakken van deze nieuwe vormen van discriminatie betekent dat de huidige rechtsbescherming opnieuw doordacht zal moeten worden.

## C.2. Elektronische datadeel overeenkomst: juridische context

Om het delen van data tussen organisaties juridisch te borgen, zijn datadeel overeenkomsten nodig. Om dit grootschalig tussen organisaties, over sectoren en toepassingsgebieden mogelijk te maken, heeft het daarbij de voorkeur om dit langs digitale/elektronische weg te faciliteren. Dit wordt aangeduid als een elektronische datadeel overeenkomst. In deze overeenkomst erkennen partijen dat er data heen en weer gaat, waarbij beide partijen hun eigen verantwoordelijkheid erkennen en zich aan de wet houden.

De wetgeving schrijft een aantal eisen voor om elektronische datadeel overeenkomsten rechtsgeldig te laten zijn, welke in de achtereenvolgende paragrafen van deze appendix worden toegelicht.

### *C.2.1. Datadeel overeenkomsten: bespiegelingen rondom inrichting.*

Voor het realiseren van elektronische datadeel overeenkomsten kunnen verschillende vormen worden onderscheiden.

Een veel voorkomende vorm is een afsprakenstelsel. Hierbij wordt voor een ecosysteem van organisaties (bijvoorbeeld binnen eenzelfde sector) een gezamenlijke datadeel overeenkomst opgesteld waaraan zowel data aanbieders als data consumenten in het ecosysteem zich conformeren. Voorbeelden hiervan zijn:

- *iSHARE*, het afsprakenstelsel, voortkomend uit de logistieke sector,
- *Medmij*, het afsprakenstelsel voor uitwisseling van gezondheidsgegevens,
- *Elektronische toegangsdiensten (ETD),* het stelsel dat eHerkenning reguleert,
- *Incoterms*, een internationale standaard over de rechten en plichten van de koper en verkoper bij internationaal transport van goederen, ontwikkeld en gepubliceerd door de Internationale Kamer van Koophandel (ICC).

Een aandachtspunt bij het gebruik van een afsprakenstelsel is de toepasbaarheid wanneer datadelen (en daarmee ook een datadeel overeenkomst) nodig is met een organisatie buiten het eigen ecosysteem waarop het afsprakenstelsel van toepassing is. Er kan daarbij niet a priori verwacht worden dat deze 'externe' organisaties zich ook aansluiten en conformeren aan het eigen afsprakenstelsel.

Een aanpak zal dan nodig zijn die onderhandeling over datadeel overeenkomsten tussen organisaties mogelijk maakt. Dit aspect van onderhandeling van datadeel overeenkomsten wordt bijvoorbeeld genoemd in de referentie architectuur van het International Data Spaces (IDS) initiatief [26], zonder daar momenteel al concreet invulling aan te geven. Randvoorwaardelijk hiervoor is wel een geformaliseerd semantisch fundament dat ervoor zorgt dat organisaties die actief zijn in verschillende sectoren en rechtsgebieden elkaar ondubbelzinnig begrijpen.

Dit aspect van samenwerking en interoperabiliteit van juridische datadeel overeenkomsten tussen organisatie en ecosystemen is essentieel voor het grootschalig mogelijk maken van datadelen. Het dient daarom in de verdere uitwerking voor datadelen ten behoeve van AI voldoende aandacht te krijgen.

### *C.2.2. De verplichte regels voor een elektronische datadeel overeenkomst*

Een elektronische (datadeel) overeenkomst is een overeenkomst die langs elektronische weg tot stand is gekomen [41]. Om volgens het Nederlandse recht rechtsgeldig te zijn, moeten voor het aangaan van een elektronische overeenkomst drie stappen worden

doorlopen. Het begint met een aanbod dat de data-aanbieder doet aan de wederpartij, dat aanbod kan vervolgens worden aanvaard (of er wordt een nieuw aanbod teruggedaan) en die aanvaarding moet de data-aanbieder weer bevestigen. Zolang de bevestiging niet is ontvangen kan de wederpartij de overeenkomst ontbinden. Het niet op tijd bevestigen van een aanbod geldt als een verwerping daarvan.

Om (juridisch) gelijk te worden gesteld met de schriftelijke overeenkomst legt artikel 6:227a van het Burgerlijk Wetboek (BW) de volgende vier eisen op aan de elektronische overeenkomst[1]:

1. *Raadpleegbaar door partijen:* Wanneer de overeenkomst in een elektronisch document is vastgesteld, waarborgt de wetgever dat partijen wat dat betreft dezelfde mogelijkheden hebben door voor gelijkstelling te eisen dat het elektronisch document door partijen raadpleegbaar is. Partijen dienen elkaar de middelen ter beschikking te stellen die nodig zijn om de opgeslagen elektronische overeenkomst te raadplegen. Aan deze voorwaarde kan worden voldaan doordat ieder der partijen de overeenkomst kan opslaan voor raadpleging op een later tijdstip. Een andere mogelijkheid is dat één der partijen de elektronische overeenkomst opslaat en de wederpartij zich elektronisch toegang kan verschaffen tot de opgeslagen gegevens (zie Tweede Kamerstuk TK 2001-2002, 28 197, nr. 3, p. 53).
2. *Authenticiteit in voldoende mate gewaarborgd:* Elektronische bestanden kunnen vrij eenvoudig onopgemerkt worden gemanipuleerd. Deze gedachte ligt ten grondslag aan het vereiste dat de authenticiteit van het elektronisch document in voldoende mate is gewaarborgd. Er zijn technieken voorhanden die het mogelijk maken om eventuele manipulatie van elektronische verklaringen te signaleren. De digitale handtekening is hiervan een voorbeeld. Deze biedt de ontvanger van de ondertekende elektronische verklaring de mogelijkheid vast te stellen of de integriteit van de verklaring is aangetast. Voor meer informatie zie [42] [43].
3. *Moment van totstandkoming met voldoende zekerheid vastgesteld:* In het elektronisch rechtsverkeer kan het tijdstip van totstandkoming van de overeenkomst op verschillende wijzen worden vastgesteld. Zo kan een onafhankelijke derde partij, de elektronische overeenkomst voorzien van een door hem digitaal ondertekende elektronische tijdstempel (zie Tweede Kamerstuk TK 2001-2002, 28 197, nr. 3, p. 54).
4. *Identiteit van partijen met voldoende zekerheid vastgesteld*: Deze voorwaarde kan worden vormgegeven door adequate mechanismes van elektronische identificatie en authenticatie, mogelijk door (vertrouwde) derde partijen vormgegeven.

In de context van een elektronische datadeel overeenkomst heeft de data-aanbieder een informatieplicht. Dit betekent dat deze partij op een duidelijke en begrijpelijke manier informatie moet geven over: (i) de manier waarop deze overeenkomst tot stand komt en wat daarvoor nodig is, (ii) hoe het contract op een later moment is in te zien, (iii) de manier waarop gemaakte fouten ontdekt en hersteld kunnen worden, (iv) de taal van de overeenkomst en (v) eventuele gedragscodes die van toepassing zijn en hoe deze via elektronische weg bekeken kunnen worden.

### *C.2.3. Optionele onderdelen van een datadeel overeenkomst*

Naast de verplichte regels voor een elektronische datadeel overeenkomst is er aantal optionele onderdelen die kunnen worden opgenomen in de datadeel overeenkomst:

1 In het tweede lid van artikel 6:227a BW wordt daarop uitzondering gemaakt voor de overeenkomsten waarbij de tussenkomst van de rechter, een overheidsorgaan of een beroepsbeoefenaar met een publieke taak nodig is. Vanwege tijd- en budgetbeperkingen valt dit onderwerp buiten de reikwijdte van dit stuk.

- *Verwerkingsovereenkomst,* die vastlegt op welke manier een andere partij omgaat met de persoonsgegevens die verzameld zijn. Er wordt bijvoorbeeld vastgelegd hoe de gegevens beveiligd worden en voor welke doeleinden persoonsgegevens worden verwerkt. De belangrijkste elementen in een verwerkingsovereenkomst zijn: (i) gebruiksrecht persoonsgegevens, (ii) rechtmatigheid verwerking, (iii) juistheid over te dragen persoonsgegevens, (iv) beveiliging, (v) vergoeding, (vi) duur en beëindiging en (vii) aansprakelijkheid.
- *Duiding partijen,* welke aspecten omvat zoals de naam van partijen in het Handelregister, de vestigingsgegevens bij de KvK, de naam van de vertegenwoordiger (BPR) met functie volgens de arbeidsovereenkomst.
- *Juridische kwalificatie*, die de meest voorkomende (juridische) definities bevat voor de termen gebruikt in de overeenkomst, b.v. 'Derde Partij, 'Overeenkomst', 'Gebrek', 'Incident', etc..
- *Geheimhouding*, waarin het karakter van vertrouwelijke informatie wordt geduid en de zorgplicht van partijen ten aanzien van de informatie wordt benoemd (ook als informatie geen vertrouwelijke informatie is).
- *Intellectueel eigendom,* waarin de licentieovereenkomst en de gebruiksrechten worden beschreven.
- *Aansprakelijkheid,* waarin de aansprakelijkheid voor de geleden en/of te lijden schade wordt beschreven voor de partij die toerekenbaar tekortschiet in de nakoming van de verplichtingen uit de overeenkomst.
- *Privacy- en beveiligingsafspraken,* gericht op het treffen van passende technische en organisatorische maatregelen om een op de risico's afgestemd beveiligingsniveau te waarborgen van de rechten van betrokkenen, waaronder het identificeren van de grondslag waarop persoonsgegevens gedeeld mogen worden en het benoemen van de toepasselijke nationale, internationale en EU wet- en regelgeving en bindende gedragscodes.
- *Geschillenbeslechting,* voor het identificeren van het recht dat de datadeel overeenkomst beheerst en de bevoegde rechter/rechtbank voor geschillen tussen de partijen.
- *Duur en beëindiging,* met de aanvangsdatum en beëindigingsdatum van de datadeel overeenkomst, en de procedure voor verlenging of ontbinding ervan.
- *Doelbinding,* met de formulering van de doelstelling van samenwerking/delen van data.
- *Derde partijen,* met de beschrijving van (de wijze van) te betrekken diensten van derden, bijvoorbeeld met betrekking tot extern (juridisch) advies.

### *C.2.4. Van het Nederlandse naar het Europese perspectief*

Vanuit het Europees perspectief zijn (nog) geen aanvullende wetgeving en richtlijnen van toepassing op de datadeel overeenkomst.

De Europese wetgever heeft wel een verordening voor vrij verkeer van niet-persoonlijke data opgesteld, waarvoor wordt beoogd om deze verordening uiterlijk 29 mei 2020 te implementeren. De verordening moet verzekeren dat niet-persoonsgegevens vrij kunnen circuleren in de interne markt. De Europese Commissie betoogt dat de interne markt nu wordt belemmerd door nationale eisen die verplichten dat gegevens alleen op het eigen grondgebied of op het grondgebied van bepaalde andere lidstaten worden bewaard. De voorgestelde verordening verbiedt het aan de lidstaten om deze eisen nog langer te stellen en bevat de verplichting dat bestaande eisen worden ingetrokken. Uitzonderingen zijn slechts beperkt mogelijk, om redenen van openbare veiligheid en onder strikte voorwaarden. Ook aan private partijen zal het niet langer zijn toegestaan om bewaring in specifieke lidstaten te eisen, bijvoorbeeld in contracten. Locatieeisen worden vaak gesteld met het oog op de uitvoering van publieke taken. Nationale autoriteiten moeten

toegang hebben tot databestanden, onder andere in het kader van de strafrechtelijke rechtshandhaving. Het voorstel onderkent dit en voorziet in administratieve samenwerking tussen nationale autoriteiten die de toegang tot gegevens die zich in andere lidstaten bevinden moet garanderen.


1000
500
500
100
100
LEVEL
0
0
100
100
500
1000

# APPENDIX D: Technieken voor datadelen

Deze appendix bevat een overzicht van een aantal (technische) ontwikkelingen die momenteel als relevant wordt beschouwd voor het vormgeven van infrastructuren voor gecontroleerd en betrouwbaar datadelen ten behoeve van AI. Daarbij wordt in de achtereenvolgende secties onderscheid gemaakt tussen de architecturen die datadelen tussen organisaties mogelijk maken, beveiligingstechnieken om data te beschermen bij het delen van data ten behoeve van het uitvoeren van AI applicatie en aanpalende technieken. De informatie in deze appendix is een samenvatting van een uitgebreidere beschrijving van de ontwikkelingen [41].

## D.1. Datadeel architecturen

De architecturen in deze sectie maken datadelen tussen organisaties volgens het netwerk-model (zoals beschreven in sectie 3.1) mogelijk.

### *D.1.1. International Data Spaces (IDS)*

IDS is een Europees initiatief om op gestandaardiseerde wijze en op basis van een referentie-architectuur het (gecontroleerd) delen van gegevens mogelijk te maken. IDS adresseert drie grote uitdagingen voor datadelen in de data-economie: interoperabiliteit, vertrouwen en bestuur voor het uitwisselen van data. Hierbij wordt gebruik gemaakt van bestaande normen en technologieën, evenals bestuursmodellen die goed worden geaccepteerd in de data-economie. De ontwikkeling van IDS wordt aangestuurd vanuit een sterke community van belanghebbenden: de IDS Association (IDSA, [27]).

### *D.1.2. iSHARE*

Het Nederlandse iSHARE-initiatief voor de logistieke sector realiseert een uniforme reeks afspraken voor identificatie, authenticatie en autorisatie, zodat organisaties logistieke gegevens op een eenvoudige en gecontroleerde manier kunnen delen, ook met nieuwe en voorheen onbekende partners [42].

### *D.1.3. Amsterdam Data Exchange (AMDEX )*

AMDEX is een initiatief van de Amsterdam Economic Board om lokale, Europese of internationale samenwerking op een transparante open datamarkt te bewerkstelligen [43]. Het biedt infrastructuur en gemeenschappelijke regels voor het creëren van een vertrouwde en veilige omgeving waaraan geïnteresseerde partners kunnen deelnemen om platforms te genereren voor real-time gegevens gestuurde samenwerking.

## D.2. Beveiligingstechnieken voor datadelen

De beveiligingstechnieken voor datadelen in deze sectie zijn ter bescherming van persoonsgegevens voorafgaand aan de verwerking ervan. Daarnaast bieden secure multi-party computation (MPC) en federated learning ook extra bescherming tijdens de uitvoering van het AI-algoritme door te zorgen dat tussen- en eindresultaten van de berekening niet gevoelig zijn.

### *D.2.1. Secure Multi-Party Computation (MPC)*

MPC is een verzameling van innovatieve cryptografische technologieën die het mogelijk maakt dat meerdere partijen gezamenlijk rekenen met data, alsof ze een grote database hebben met al hun data, maar zonder dat ze elkaars data kunnen zien [44]. De deelnemende partijen bepalen wie de uitkomst van de berekening (het resultaat van het AI-algoritme) mag inzien. MPC biedt zeer veilige oplossingen voor het delen van (privacy of commercieel) gevoelige data voor AI (of andere rekendoeleinden).

Een voorbeeld van wat je met MPC zou kunnen doen is secure set intersection. Dat betekent dat, gegeven twee of meer gevoelige databases van items of personen,

je op een veilige manier kunt bepalen welke items of personen ze gemeenschappelijk hebben, zonder de rest van de informatie uit de databases te onthullen.

Technieken die bij MPC gebruikt worden zijn o.a. homomorfe encryptie en secret sharing. Homomorfe encryptie is een bijzondere vorm van vercijferen van data, die het mogelijk maakt om bepaalde berekeningen, zoals optellingen, te kunnen doen zonder de data te hoeven ontcijferen. Met secret sharing wordt elk data element opgedeeld in nietszeggende 'shares'. Elke deelnemende partij in de berekening krijgt voor elk data element een share. Door te rekenen met de shares is het mogelijk om gezamenlijk berekeningen uit te voeren op de data elementen, zonder informatie over die data elementen prijs te geven.

MPC maakt het mogelijk dat partijen gezamenlijk op een zeer veilige en innovatieve manier hun AI-algoritme uitvoeren op gevoelige data, zonder dat ze elkaars data leren.

### *D.2.2. Federated learning*

Machine learning is een belangrijke tak van AI, waarbij computers kunnen leren van data via analytische modellen. Federated Learning is een vorm van machine learning met gedistribueerde data, waarbij het algoritme zo wordt opgezet dat de data die tussen partijen wordt uitgewisseld minder gevoelig is [45]. Het algoritme is doorgaans iteratief, en tijdens elke iteratie wordt informatie uitgewisseld. Gevoelige persoonlijke data wordt daarbij typisch lokaal, d.w.z. door de eigenaar van de data, geaggregeerd voordat die gedeeld wordt met andere partijen.

Federated learning is vooral bekend in het gezondheidsdomein. Initiatieven die hiervan gebruik maken zijn bijvoorbeeld Personal Health Train [15] en DataShield [46].

### *D.2.3. Differential privacy*

Differential privacy is een manier om te voorkomen dat de uitkomsten van statistische analyses niet te herleiden zijn tot personen [47]. Door ruis toe te voegen aan persoonlijke data, zal de geaggregeerde waarde van die data niets zeggen over de individuele waarden, zelfs wanneer de database herhaaldelijk wordt bevraagd. Differential privacy kenmerkt zich door een wisselwerking tussen privacy en nauwkeurigheid. Hoewel differential privacy niet direct bedoeld is voor complexe AI-algoritmen, kan het wel worden gebruikt in combinatie met federated learning of MPC om de output van AI-algoritmen te beschermen.

### *D.2.4. Anonimiseren en pseudonimiseren*

Anonimiseren en pseudonimiseren zijn twee technieken om te voorkomen dat data valt terug te leiden naar personen. Hoewel ze in de GDPR genoemd worden als juridische kwalificaties, beschrijven we ze hier als technieken. Anonimiseren komt neer op het verwijderen van identificeerbare informatie uit gegevens, om te zorgen dat het niet langer persoonsgegevens zijn. Bij pseudonimiseren wordt die identificeerbare informatie niet verwijderd, maar verhaspeld (vaak met een hashfunctie) tot een pseudoniem. Zonder additionele informatie is het niet mogelijk om te bepalen welke persoon onder een bepaald pseudoniem schuilgaat. In tegenstelling tot anonimisatie maakt pseudonimisatie het wel mogelijk om verschillende data (attributen) van dezelfde persoon aan elkaar te koppelen.

Door te koppelen met andere bestanden valt data, waarvan de identificeerbare informatie is verwijderd, soms toch terug te leiden naar personen. Door bovendien attribuut informatie te vervangen door synthetisch gegenereerde data met vergelijkbare statistische eigenschappen, is die herleiding een stuk moeilijker.

Een Bloom filter is een minder gebruikelijke, geavanceerde vorm van pseudonimiseren. Oorspronkelijk worden Bloom filters gebruikt om op een snelle manier te kijken of één of meerdere elementen in een database zitten of niet. Omdat er eenzelfde soort verhaspeling plaatsvindt als bij pseudoniemen, kun je het filter ook gebruiken om op een privacy vriendelijke

manier te checken of personen voorkomen in een database, zonder informatie over die personen prijs te geven [48].

## D.3. Gerelateerde technieken

We noemen nog enkele technieken die gebruikt kunnen worden voor datadelen, maar die niet direct de vertrouwelijkheid van data beschermen.

### *D.3.1. Self Sovereign Identity (SSI)*

De term SSI wordt gebruikt voor de ontwikkeling dat een persoon of organisatie zelf zijn eigen identiteit kan bezitten en beheren zonder de tussenkomende van externe administratieve autoriteiten. Doel is het daarbij dat personen in de digitale wereld kunnen interacteren in eenzelfde mate van vrijheid en vertrouwen als in de offline wereld. SSI is daarbij een manier om digitale identiteiten te managen, zodat gebruikers de controle houden over hun data [49]. Een gebruiker heeft een persoonlijk kluisje waarin hij diverse certificaten bewaart, die hij bij organisaties kan aantonen. De oplossing is privacy vriendelijk in de zin dat de gebruiker de controle heeft over zijn eigen data.

### *D.3.2. Distributed ledger / blockchain*

Een distributed ledger is een decentrale manier om grote hoeveelheden transacties (contracten, documenten, etc.) op te slaan, zonder centrale beheerder of centrale gegevensopslag [50]. Distributed ledger is gebaseerd op een peer-to-peer netwerk met consensusalgoritmen over replicatie, delen en synchronisatie van digitale gegevens die geografisch verspreid zijn over meerdere sites, landen of instellingen. De technische oplossing garandeert de integriteit van de informatie, oftewel opgeslagen informatie kan niet meer veranderd worden.

Een vorm van distributed ledger is het blockchain-systeem, met zowel een 'public' als een 'private' variant.

### *D.3.3. Ontology Based Access Control (OBAC)*

Een ontologie is een algemene beschrijving van eigenschappen van objecten (dingen). Een ontologie kan ook gebruikt worden om kennis van data te structureren, in de vorm van een kenniskaart (knowledge graph). Wanneer er veel verschillende soorten data gedeeld moet worden kan met de ontologie gedefinieerd worden welke data door wie (access) en waarvoor (usage) gebruikt kan worden. Ontology Based Access Control (OBAC) is de methodiek om op deze wijze de toegangscontrole tot data te laten afhangen van de ontologie [51]. Zo helpen ontologieën om data interoperabel te maken en de data op de juiste wijze te ontsluiten.

# Colofon


| | |
|---|---|
| Auteur(s) | F.T.A. (Frans) van Ette, MSc |
| | H.J.M. (Harrie) Bastiaansen, PhD |
| | P.J.M. (Thijs) Veugen, PhD |
| | C.J. (Cor) Veenman, PhD |
| | F.W. (Freek) Bomhof, MSc |
| | Prof. dr. ir. D. (David) Langley |
| | S. (Somayeh) Djafari, LL.M |
| | L. (Laura) van den Aarssen, PhD |
| | M.J. (Marc) van Lieshout, MSc |
| Contact | Nederlandse AI Coalitie |
| | Coalitiedesk - info@nlaic.com |
| | www.nlaic.com |
| Vormgeving | S. (Sergio) Kepel |
| Uitgave | Maart 2020 |