TOWARDS A FEDERATION OF AI DATA SPACES

NL AIC reference guide to federated and interoperable AI data spaces

NL AI Coalition

INHOUDSOPGAVE

MANAGEMENT SUMMARY

The ambition of the Netherlands AI Coalition (NL AIC) is to position the Netherlands at the forefront of knowledge and application of Artificial Intelligence (AI) for prosperity and well-being. To achieve this goal, it is deemed crucial to make data widely available to train and fuel the AI algorithms. At first glance a simple task, but data often resides and is protected in organisational silos, unreachable for others to build and use their AI applications.

It is clear that access to data across organisational silos is needed, which is why the data sharing working group of the NL AIC has set the goal of the creation of trustworthy and interoperable AI data spaces. This is not just a Dutch initiative but an international endeavour. The EU wants "a single market for data, where data from public bodies, businesses and citizens can be used safely and fairly for the common good." [1]. We no longer can afford centralised data warehouses with the aim to create an information or distribution monopoly. We need the alternative, called federated AI data spaces, where data does not travel to central data lakes if there is no need to, but can be used straight from the source. The actual design of these AI data spaces is an important step towards fulfilling the goals of the EU and NL AIC. A great and powerful tool for any application, including the ones that are not AI driven. And in the case of AI, access to data by way of federated AI data spaces creates the foundation for the best pattern recognition we can get that underpin the vast promises of AI.

The key to success for such a set-up is organising trust through technical, semantic, organisational, and legal interoperability. This will create an inclusive system where data is shared based on standards that are open and transparent. A special point of standardisation for trust aims to provide the agreements and assurance that data is only used for the purposes as intended by the original keeper or controller of the data. This is called data sovereignty and stands as the foundation in the trust system that is required. To give one example, rather than sending patients data to a central database of a service provider, a solution can be built such that an algorithm is sent to a hospital, where locally the algorithm gets trained in the ICT environment of that hospital. The algorithm and its parameters are trained locally and leaves the hospital with enhanced capabilities, but the patient's data itself remains at the hospital. The algorithm is then allowed to "visit" more hospitals and gets access to multiple sources of data. The end-result is a privacy secure solution and an improved AI algorithm.

In the future, additional documents will be released that are in line with this document and support in organising trust and building interoperable AI data spaces, by serving as:

- reference for developing AI data spaces, providing a rich set of features to support the challenges and requirements of AI, and
- prescriptive guidelines for ensuring trust and interoperability between such individual AI data spaces.

Organisations setting-up AI data spaces in the context of the NL AIC will use these documents for their design. Any party outside the NL AIC that is working on AI and data sharing is also encouraged to use the learnings and tools to better understand potential of AI data spaces.

However, creating and distributing this document is just the first step. The NL AIC aims to build AI data spaces with all relevant partners. The NL AIC is the ideal partner to realise these AI data spaces because of the know-how, open-source software building blocks, sharing of best practices and a road from proof of concepts via pilots, to alfa-beta and launches of real operational AI data spaces.

The Netherlands, by means of the NL AIC, has a good starting position with a strong set of positive examples of both AI and data sharing and has the combined knowledge and skills to make data sharing for AI work.

The NL AIC's goal is to co-create and build ten AI data spaces in The Netherlands based on the guidelines in this document. The ten AI data spaces will be operational in various sectors. Because of the adoption of standards as described later in this document, these AI data spaces can exchange data with other AI data spaces inside and outside the Netherlands. These AI data spaces will be serviced by professional organisations, will be easy to implement use and trustworthy in every aspect. Because of standardisation, scaling up will be possible, service providers can build a profitable business model and vendor lock in is avoided. Thus, the NL AIC contributes to the vision of a thriving eco-system where organisations can safely and with confidence share data, staying in control throughout the process. As a result, AI applications will be fed with what they need to learn and build their algorithms: data from as many sources as possible. The NL AIC has started on this mission in 2019 which will result in a flourishing AI ecosystem with plug & play AI applications across many sectors.

1. INTRODUCTION

Data and data sharing are key ingredients for the implementation of AI.

1.1 The Netherlands AI Coalition and the data sharing working group

Founded in 2019, the Netherlands AI Coalition (NL AIC) has been set up to stimulate AI activities in the Netherlands ensuring a long-term position with this strategic technology. The NL AIC is a (quadruple helix) public-private partnership in which the government, the business sector, educational and research institutions, as well as civil society organisations collaborate to accelerate and connect AI developments and initiatives. The ambition is to position the Netherlands at the forefront of AI creating value for Dutch society, it's organisations and citizens. The NL AIC aims to reach this ambition in alignment with European standards and values. The NL AIC functions as the catalyst for AI applications in The Netherlands [2]. One of the Coalition's areas of interest is 'data sharing'. A dedicated working group is tasked with providing the community knowledge, resources and guidance around responsible data sharing for AI.

1.2 Previous work of the NL AIC data sharing working group

In 2020, the NL AIC data sharing working group:

- has identified the specific challenges for data sharing for advanced data analytics and provided an overview of technologies and architectures that can be used in addressing these challenges [3] [4],
- has outlined the process of how companies can share data for AI, from experimental ("first-time engineering") phase, to a phase of daily practice ("operationalisation") [5] ,
- has developed three PoCs to demonstrate the architectural concepts and technical components for controlled data sharing for AI, using three illustrative and representative cases from the sectors 'government', 'health' and 'energy', and has done a 'GAP-analysis' on the system operations gaps and the governance gaps to be bridged between the architectures and technology as demonstrated in the PoCs and the large-scale deployment and adoption thereof [6]. These PoCs form the starting point in the process from first-time engineering towards operationalisation of a data sharing infrastructure for AI in the Netherlands, as described in [5],
- has caried out a quick scan of the current data sharing ecosystem to validate if the chosen architecture based on IDS is in line with international developments and standards [7].

1.3 The European perspective

Data and data sharing are key ingredients that are clearly on the radar of the European Commission as well, also in the context of AI. Together with an AI White Paper [8] in which the Commission lays out the way forward on AI adoption and addresses the key risks of AI, the Commission has also released a paper on data governance and the role of data in AI [9]. Moreover, its release of the Data Governance Act [10] and the additional input sought on data spaces through OPEN DEI [11] point to the importance that the EU attributes to data and data sharing for our society and economy.

These European documents and position papers build the fundaments upon which the NL AIC will execute the data sharing initiatives. This will ensure that interoperability will be achieved on at least the European level. In addition, work done in the European context does not need to be repeated on a national level. The NL AIC will contribute through concrete deliverables and dissemination of the learnings as a constructive and valuable partner of the EU. The NL AIC also works closely together with GO FAIR to ensure that data is Findable, Accessible, Interoperable and Reusable (FAIR).

Within Europe, Germany has been very active in the formulation of an alternative to centralized solutions to data sharing. German industries felt an increasing dependence on non - European tech companies which in a negative scenario would lead to loss of autonomy and margins. The response has been to come up with concrete alternatives such as International Data Spaces (IDS) and in the last two years the creation of GAIA-X.

Even though GAIA-X is not mature yet, it has strong backing from the German government which has also reached out to France in the first place and connected later to other countries in Europe as well, The Netherlands being one of them.

At this point in time, both GAIA-X and IDS seem to be best placed to deliver the standards needed for interoperability and are therefore guiding many of the efforts we undertake at the NL AIC.

At the same time, because of the relative immaturity of these initiatives, it is important to keep our eyes open for alternative standards that may gain traction.

2. THIS DOCUMENT

This document focusses on data sharing challenges related to the development and operationalisation of AI algorithms.

2.1 Purpose of this document

The ambition of this document is to serve as:

- the reference for developing AI data spaces, providing a rich set of methodologies, tools, processes and building blocks to support the challenges and requirements of AI, and
- prescriptive guidelines for ensuring trust and interoperability between such individual AI data spaces.

Federated AI data spaces and the way in which they are interoperable are not yet exhaustively defined. In this document, it is apparent that certain areas are still under construction. That should not stop anyone from building AI data spaces as described as the advantages are apparent already with the current state and with some areas not fully developed yet.

The development, introduction and adoption of Federated, Interoperable, AI data spaces will be a major goal of the NL AIC data sharing working group for the coming time period 2021 – 2024. During this time period, the data sharing working group aims to help realise 10 AI data spaces. The AI data spaces are based on this document and the full tool kit of tools, methodologies and processes that are continuously built and improved over time standing on the shoulders of work already done by others.

A second purpose of this document is therefore to identify and present new areas: We continue to uncover and create easier ways to build interoperable AI data spaces.

2.2 Scope of this document

This document focusses on data sharing challenges related to the development and operationalisation of AI algorithms. Fully aligned with the European data strategy [12], it is to be expected that AI algorithms are deployed in AI data spaces. AI data spaces are defined as decentralised infrastructures for trustworthy data sharing in data ecosystems based on commonly agreed principles.

This document, together with several other documents form the reference guide that outlines how AI data spaces need to be set up, be managed, and be supported to accommodate the feed of data to AI algorithms and to safeguard trust and interoperability within a single AI data space and across different AI data spaces.

The current scope is focused on the realisation and operationalisation of AI data spaces. There are of course other relevant topics that play an important role in data sharing for AI, such as Privacy Enhancing Technologies (PETs) (including synthetic data) and semantics. These topics will be mentioned where directly applicable but to do justice to these topics, they will be covered in separate documents with a short introduction in the following paragraph.

As a general remark, this document has been written with the typical business architect in mind. This role covers as input the vision for the future of an enterprise and its services which need to be translated into clear ICT deliverables. This means that we are not delving into the details of the actual execution of specific deliverables, but will cover the higher functional descriptive level.

2.3 Position of this document in the context of the deliverables of the NL AIC data sharing working group

In essence, the NL AIC data sharing group wants to create the data sharing infrastructure for AI to enable easy access to data residing in various sources.

This is the corner stone and architectural basis that were clearly identified when the NL AIC was formed. However, it is not the only challenge in the context of data for AI.

Two topics stand out that members of the data sharing working group have identified that are clear obstacles to operational AI solutions:

The first topic has to do with the semantics of the data itself that is being shared. There needs to be an understanding of what this data actually tells us between the parties. The definition of data fields or in any other words, the semantics of data, needs to be known before we let the machines compute the averages, the means, the patterns. Without it, the famous GIGO risk becomes real: garbage in garbage out.

In some cases, this is clear from the start: When different manufacturers build one machine from components that need to be integrated, to make the system work, interface specifications need to be clear. These specifications are only meaningful if there is a true understanding of the data fields that describe the specifications, In other words, the receiving party needs to understand the language of the provider. The machine will not be able to be constructed and function properly without it.

In other instances, the risk simmers below the surface. These are the hidden complexities when parties assume that the definitions at the same, yet the interpretations differ. We believe we mean the same thing, but it was not well enough specified and all of a sudden, we may confuse the AI algorithm with one batch in inches and the other in centimetres. This risk increases even more when we don't have information about the quality of the dataset, and metadata about the represented population.

This preparatory work of true understanding of data sets is required before data can be shared. The working group is considering how to support this process with methodologies, processes, and tools.

The second topic is focussed on another important condition: how do we ensure privacy when data is shared? Note that semantics is a condition for privacy considerations. If one does not know what a dataset or element means, there is no way of knowing if you are dealing with privacy sensitive data and should protect it accordingly. Furthermore, this also applies to algorithms. If one does not know what it does, it cannot be accepted.

There are many solutions available to enhance privacy. These solutions are more widely known as privacy enhancing technologies (PETs) or stated as a principle "privacy-by-design". These PETs are already available, but as with AI data spaces, there is still work to be done. There are therefore two additional potential challenges for the working group: how to make sure that the existing PETs are being used to their full potential. Secondly, how can we build further on the existing toolset so we can develop further and truly create the trust with privacy by design.

This report, 'Towards controlled access to available data for AI', may be considered a master document that provides an overall reference guide to federated, interoperable AI data spaces. Next to this report, there will be two adjacent reports being developed as part of the work by the NL AIC data sharing working group, to provide guidance for implementing an AI data space, or make an AI data space compatible (interoperable) to other AI data spaces that have been developed under the framework of the NL AIC:

1. Reference guide for interoperability within an AI data space (***intra*** data space). This report will provide guidance for implementing an AI data space (either new/from scratch or an existing data space to be made interoperable).
2. Reference guide for interoperability between AI data spaces (***inter*** data space). This report will provide guidance for making multiple data space compatible. Architectural topics will be covered.

Both the inter as well as the intra data space reference guides reflect the status of the work and are work-in-progress. They will be updated twice a year in the coming period 2022 -2023. Complementing and as input for these two intra and inter AI data space interoperability reference guide, the NL AIC data sharing working group will provide two adjacent deliverables:

- An overarching reference implementation, encompassing a demonstration of the architectural concepts for both the inter and intra AI data space architectures.
- Proof-of-concepts, done in collaboration with NL AIC participants, aimed at both further development and initial implementation of the inter and intra AI data space architectures.

Furthermore, we will prepare a report that outlines the process of organising, implementation and scaling to production-grade AI data spaces. It does not detail actual (technical) specifications for implementation but serves as a guide that helps shape the required activities for organisations towards implementation. This helps non-technical managers become familiar with the AI data space documentation, tools and guides.

Figure 1 graphically depicts the deliverables of the NL AIC data sharing working group in the time period 2021 - 2024 and their interrelationship.

2.4 Structure of this document

This document is structured as follows:

- First, context is provided around the importance of AI, how AI can be defined and how data sharing for AI can be defined.
- Second, challenges related to unlocking the value of AI are presented in Chapter 4. These complications are related to the willingness and ability to share data for AI, to effectively execute AI algorithms and locally execute data apps.
- Third, in Chapter 5 we describe that to overcome the challenges in unlocking the value of AI as described in Chapter 4, parties will need to organise trust and interoperability. This is best done in so-called AI data spaces: decentralised infrastructures for trustworthy data sharing in data ecosystems based on commonly agreed principles as also described in Chapter 5.4.
- Fourth, Chapter 6 and 7 give more detail on how, based on business requirements, and a functional role model (with reference to the IDS reference architecture [13]) one can achieve trust and interoperability in a single AI data space and across AI data spaces.
- Finally, Chapter 8 provides further details on the governance, approach, and roadmap of how the NL AIC will work towards a federation of AI data spaces.

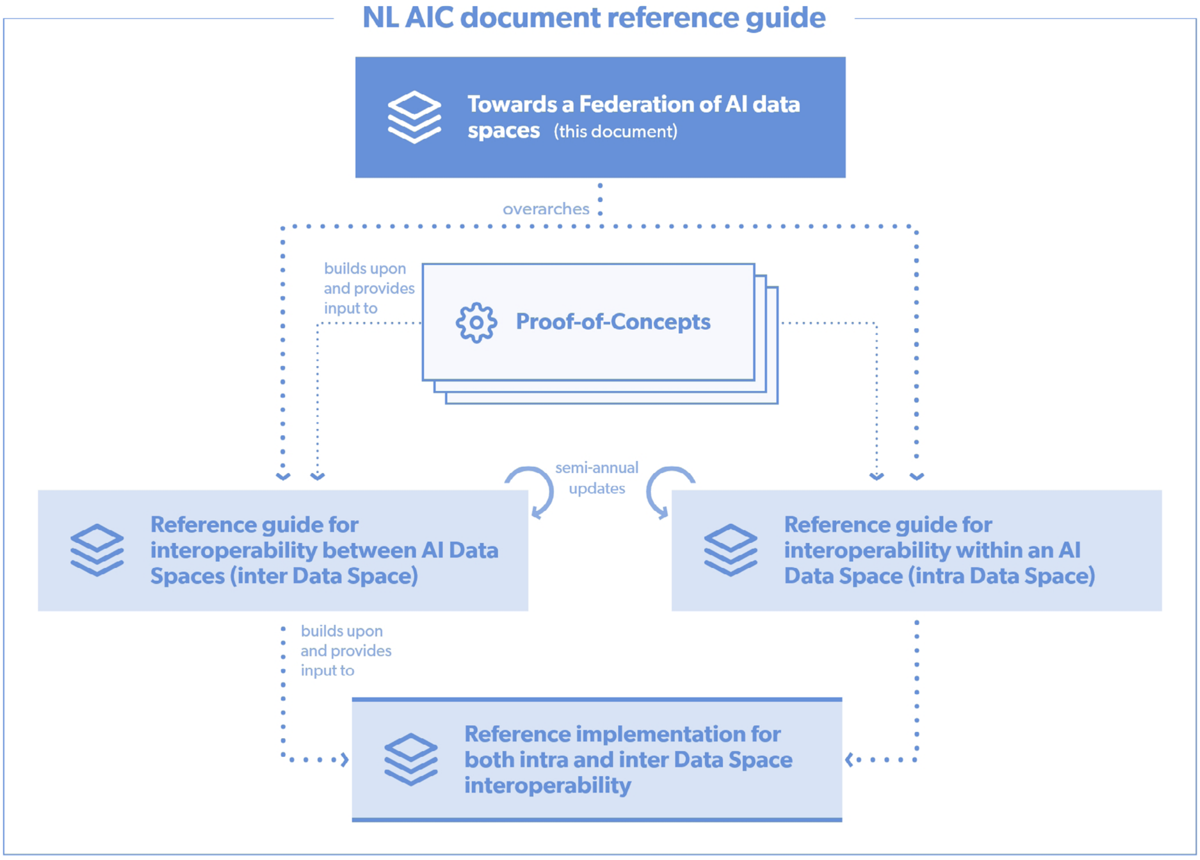

NL AIC document reference guide
Towards a Federation of AI data spaces (this document)
overarches
builds upon and provides input to
Proof-of-Concepts
semi-annual updates
Reference guide for interoperability between AI Data Spaces (inter Data Space)
Reference guide for interoperability within an AI Data Space (intra Data Space)
builds upon and provides input to
Reference implementation for both intra and inter Data Space interoperability

Figure 1 - Deliverables of the NL AIC data sharing working group and their interrelationship.

3. TRANSFORMATIVE IMPACT OF AI ON SOCIETY

AI is transforming everyone’s life by reshaping many industries such as healthcare, mobility, education, energy, and agriculture.

3.1 Artificial Intelligence

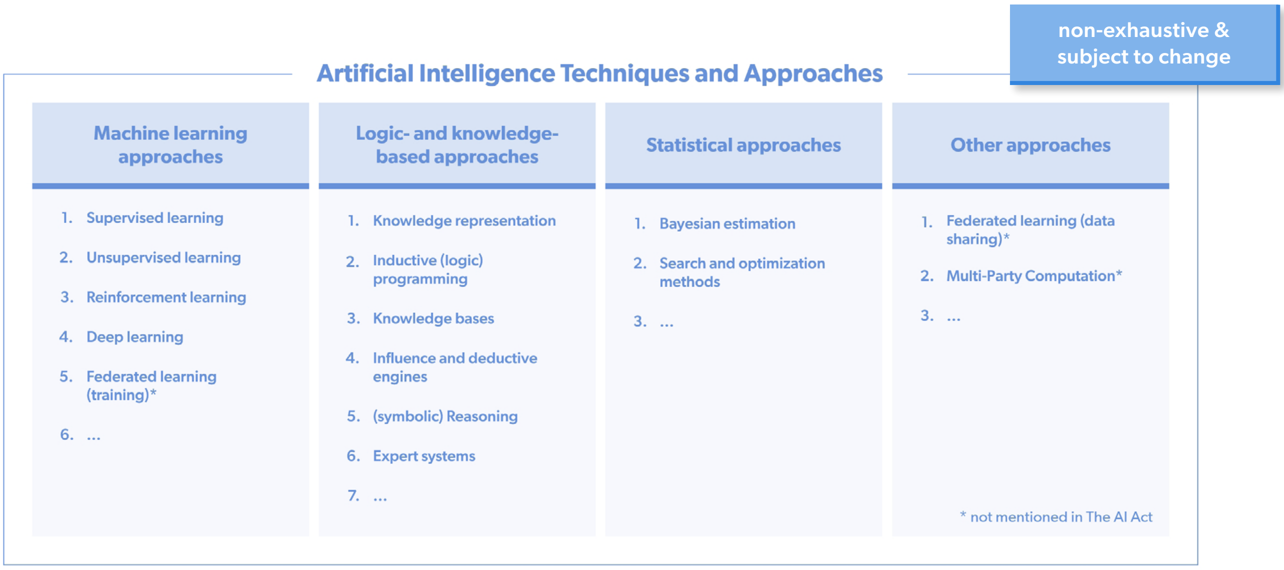
Artificial Intelligence (AI) means different things to different people. The European Union has published many documents on AI, including a definition of AI to avoid misunderstanding and achieve a shared common knowledge of AI [14]. The Trust System for AI data spaces follows the following definition provided by the EU:

> "**Artificial intelligence (AI)** refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)."

On top of the definition for AI, the European Artificial Intelligence Act mentions several AI Techniques and Approaches that are presented in **Figure 2** below [15]. Adaptations of these techniques and approaches may be necessary over time. The figure below provides an overview of the AI techniques and approaches.

3.2 AI will have a transformative impact on society and the economy

AI is transforming everyone's life by reshaping many industries such as healthcare, mobility, education, energy, and agriculture. The global AI market is expected to grow at a compounded annual growth rate of 42.2% to USD 733.7 billion in 2027 [16]. Furthermore, in The Netherlands, experts calculated that fully adopting AI can lead to 1.2% yearly growth in GDP [17]. This tremendous growth is partially caused by the fact that tasks designed for humans can be performed by AI at low cost and at scale [18]. For specific tasks, AI even goes beyond being cheaper and more scalable to the point of outperforming certain human capabilities. Researchers predict that AI will outperform humans in translating languages (by 2024), writing high-school essays (by 2026), driving a truck (by 2027) and working as a surgeon (by 2053) [19].



Artificial Intelligence Techniques and Approaches

non-exhaustive & subject to change

Machine learning approaches	Logic- and knowledge-based approaches	Statistical approaches	Other approaches
1. Supervised learning	1. Knowledge representation	1. Bayesian estimation	1. Federated learning (data sharing)*
2. Unsupervised learning	2. Inductive (logic) programming	2. Search and optimization methods	2. Multi-Party Computation*
3. Reinforcement learning	3. Knowledge bases	3. ...	3. ...
4. Deep learning	4. Influence and deductive engines		
5. Federated learning (training)*	5. (symbolic) Reasoning		
6. ...	6. Expert systems		
	7. ...		

* not mentioned in The AI Act

Figure 2 - AI techniques and approaches

3.3 Life cycle of AI algorithms

If we simplify the life cycle of (most of the) AI algorithms, we can identify two main phases for applying the algorithms: The Development Phase in which data or knowledge is used to train and test/verify the algorithm, and an Operational Phase in which the algorithm is used to, for example, make decisions or predictions based on the learned knowledge. **Figure 3** provides a simplified overview on how an algorithm goes from untrained to deployed. Once deployed, an algorithm should return to the Development Phase (the grey dotted lines) to retrain and verify with new data to improve the accuracy of the algorithm system and mitigate the risks related to concept drift. Similarly, 'Live' data (together with the algorithm output) can also be used in future training and verification data sets. It should be noted that there are also cases of incremental learning where 'Live' data is continuously used to further train the algorithm.

Although AI algorithms will be just about everywhere and will serve an immense range of purposes, for the purpose of the Trust System, only two high level results, that broadly cover all scenarios, should be considered:

1. A Verified Algorithm
2. An Algorithm Output

3.3.1 Verified Algorithm

To get to a point where the algorithm can provide output based on data, an algorithm is trained or improved by exposing it to data. Using the previous example, the algorithm can indicate the likelihood of lung cancer by identifying anomalies in x-rays of lungs. By sharing more x-rays of lungs with and without cancer indications with the algorithm, the algorithm will become more accurate in identifying those indications. Training the algorithm with high quantity of relevant and high-quality data is a necessary step towards unlocking the value of the algorithm.

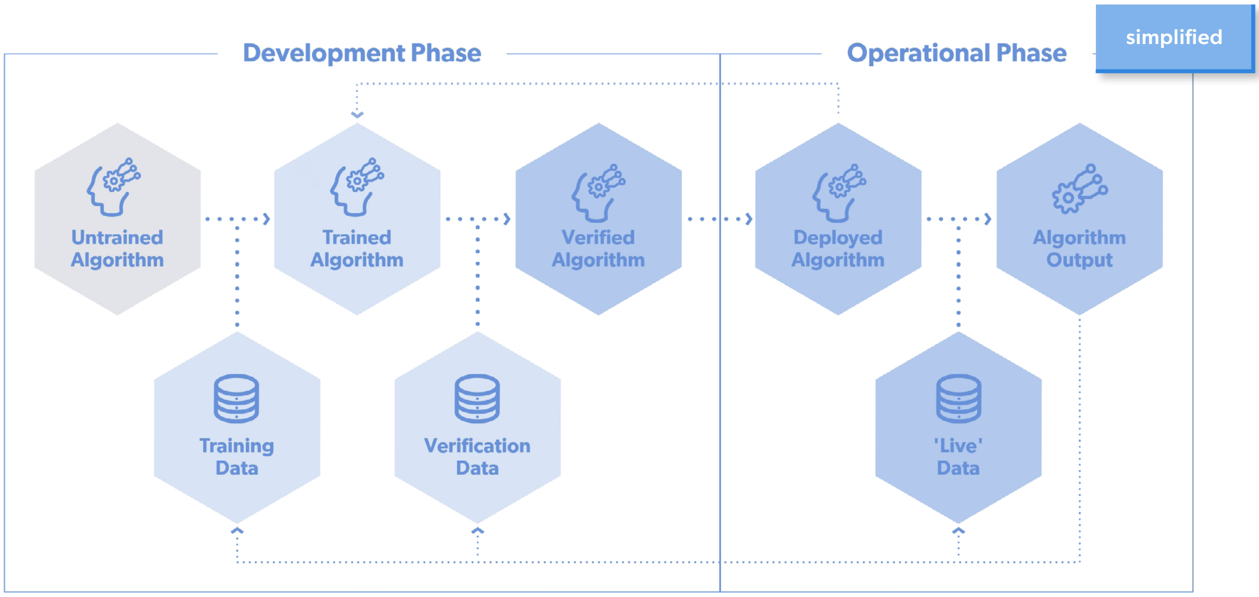


Figure 3 - Development and Operational Phase are common phases of an algorithm.

3.3.2 Algorithm Output

After Training and Verification in the Development Phase, an algorithm can be deployed to, for example make decisions or predictions. Think of a trained algorithm that may be capable to recognise if an x-ray most likely contains indications of lung cancer. Another example can be a bank sharing real time chat data with a chatbot algorithm, that in turn provides real time responses that are tailored to the specific conversation.

3.4 Data is the fuel that determines the impact of AI

Data is a key strategic asset. This certainly holds true for personal data, as data can tell so much about us. But it also holds for business data as it can optimise business ecosystems and supply chains, help the advancement of research, improve the functioning of government agencies and spur the economic and strategic position of countries. Contrary to most physical assets, data can be used repeatedly and simultaneously by different parties. The same data can provide unlimited value, as long as it is shared and does not sit idle in silo's, sealed off from applications that need it.

Data and data sharing are key ingredients that are clearly on the radar of the European Commission, also in the context of AI. Together with an AI White Paper [8], the commission has released a paper on data governance and the role of data in AI [9]. Moreover, the release of the Data Governance Act [10] and the additional input sought on data spaces through OPEN DEI point to the importance that the EU attribute to data and data sharing for our society and economy [20] .

3.5 Data sharing for AI can connect data with AI algorithms

Most of the recent AI techniques rely heavily on the availability of data. Since the exponential growth of data coming from sensors and other sources, the development of AI has accelerated as the large amounts of data and the increase in compute power with the aid of GPUs enabled to efficiently deploy techniques like deep learning to create real value from data. These techniques traditionally relied on storing data at one location in order to process the data and develop AI algorithms. Centrally storing the data means businesses need to trust others to store their data and only use it for the agreed upon purpose or just hope for the best (e.g. develop an AI algorithm). Nowadays, there are different methods to 'connect an AI algorithm with data'. The preferred method depends on the specific context of organisations providing access to their data.

New Privacy Enhancing Technologies (PETs) have been developed where centralising data is no longer necessary to develop AI algorithms. Federated learning is one of these technologies that allow for decentralised training of algorithms [21]. Another technique is secure multi-party computation that allows parties to jointly compute a function over their combined data, while keeping this data private [22]. These techniques make data sharing possible, without losing control over said data. This could enable many opportunities for innovation, with new forms of collaboration, changing business models and new ways of organising society.

Other privacy enhancing technologies are also available such as the use of synthetic data, anonymisation of data and full homomorphic encryption. It should be noted that not all synthetic data is applicable in the context of AI.

4. DATA SHARING FOR AI: CHALLENGES

The previous chapter showed that AI can have a transformative impact on the economy and society. To unlock the value of AI it is crucial to make data widely available to train and fuel the AI algorithms. Data sharing for AI could help with developing and operating such AI algorithms in AI data spaces. However, practically developing and operating AI algorithms is where organisations often struggle.

Ideally, data is easily accessible, with data access and usage control for the data owner. But the reality is often different. Data has inherent value. There may be costs involved in making data available. 48% of organisations report data quality, quantity or availability as one of the largest constraints to develop AI applications [23].

Having access to the necessary data is only part of the problem. Data and AI algorithms may be distributed across multiple parties. In the execution of the AI algorithm, these either need to be brought together or mechanisms for distributed execution need to be in place. Properly executing the AI algorithm, while keeping track of the usage policies of all involved parties, brings more complexity to the table beyond the accessibility of data.

Moreover, there are regulatory restrictions on data sharing and AI, such as the General Data Protection Regulation (GDPR) [24] and the upcoming AI Act [9]. Therefore, organisations and individuals need to be in control on who may use the data, for what purposes and under what conditions (e.g. ethical conditions) [25] [26]. To solve the challenge of fuelling AI algorithms with enough usable and qualitative data, a collaboration between organisations is needed that enables:

1. data sharing for AI,
2. execution of AI algorithms and
3. locally run data apps[1].

However, there are two, non-trivial pre-requisites for this act of sharing and executing which are in the hands of organisations and individuals: the **willingness** and **ability** to share data, execute AI algorithms and/or locally run data apps. These are addressed in the following sections.

4.1 Willingness and ability to share data and/or algorithms

The willingness to share refers to a party being open to sharing data and/or algorithm with another party and that other party being open to receive and trust that data and/or algorithm. In both cases, the willingness to exchange data depends for a large part on (1) the specified purposes (purpose-bound), the legal ground and/or permission to share the data, (2) the level of trust that is present and needed between the two parties, (3) the level to which a party stays in control over who can access his data and for what use, i.e. data sovereignty, and (4) the business relevance (e.g. gain insights, help society).

There are also regulatory restrictions on data sharing, such as the General Data Protection Regulation (GDPR). These regulations are there to protect us all and must be adhered to. However, these regulations and their diverging interpretation, the value of data in itself and the technological and practical hurdles slow down the development and introduction of new data analytics applications, despite the significant advantages that may be achieved when larger volumes and different types of data are ubiquitously available. As such, permission management, encompassing the aspects of obtaining lawful ground to share data, the associated management authorisations and accountability management are of major importance. This specifically applies when sensitive (personal) data is to be shared.

Moreover, ethical opinions and legal conditions on sharing such sensitive (personal) data are subject to societal debate and vary per organisation, sector / application area and change over time. This introduces a risk for organisations who incorrectly share data (or cause a data leak). This results in bad public relations and potentially heavy GDPR fines.

[1] Data apps are data processing applications used to process and/or analyse data. Examples of data apps are anonymisation/pseudonymisation apps, semantic conversion apps, data quality management apps, data pre-processing/cleaning apps

The easiest way to avoid this risk is to not share data at all, which is happening now. The work of the NL AIC should give organisations the feeling that data sharing becomes risk-free.

Trust can apply to a whole range of aspects, such as trust about who the parties are, trust about the quality and origin of the data, trust about the legal and ethical functioning of the algorithm or trust in the other party's information security policies.

Data sovereignty is a natural person's or corporate entity's capability of being entirely self-determined regarding its data. It allows a legal person to exclusively decide on the usage of its data. It requires organisations to be in control over the conditions under which their data is shared and how it may be processed by other parties.

In addition, there needs to be a rationale for all parties involved. The relevant parties are first and foremost the data owner and consumer. There needs to be a coverage of costs and risks, a benefit (financial or non-financial), a legal requirement or a larger societal relevant goal for all involved and made clear to the decision makes.

The ability to share refers to a party having the right capabilities to sharing data and/or algorithm with another party and that other party having the right capabilities to receive that data and/or algorithm. The ability to exchange data depends on the level of interoperability. This interoperability can apply to a whole range of aspects, such as the obvious interoperability of data formats and semantics, interoperability of exchange protocols and interoperability of algorithm and execution environment, but also interoperability of security requirements, business models and legal frameworks.

4.2 Willingness and ability to execute AI algorithms

The willingness to execute AI algorithms refers to a party (receiving party) being open to execute an AI algorithm that they received from another party and that other party being willing to have their AI algorithm executed by the party that receives the AI algorithm. Similar to the willingness to share, both cases depend for the most part on the level of trust that is present between the two parties.

The ability to execute refers to a party having the right capabilities to execute the AI algorithms of another party and that other party having the right capabilities to let their AI algorithm be executed by the party that receives the AI algorithm. The ability to execute depends on the level of interoperability between the involved parties. Furthermore, involved parties need to have the organisational capabilities to execute AI algorithms. A party needs capabilities such as an environment to execute an AI algorithm.

4.3 Willingness and ability to run data apps

To be usable for AI algorithms, pre-processing and enriching of data prior to being fed to the AI algorithm may be needed. Pre-processing may for instance be needed for:

- de-identification (anonymisation, pseudonymisation)
- data analysis
- imputation
- bias considerations
- outlier detection
- semantic conversions and mapping
- quality monitoring and control

Being able to invoke and execute data apps for doing this pre-processing and enriching of data is pivotal in developing a flexible and extensible infrastructure for data sharing for AI. Optimally, these data apps are re-usable by data providers and are provided as generic data apps from an app library.

The willingness to run data apps again refers to a party (receiving party) being open to run data apps that they received from another party. The willingness to share such data apps may be less an issue as compared to both previous cases (on sharing data and sharing AI algorithms) as these pre-processing data apps are less sensitive and may even be provided on an open source basis. However, it is crucial that the data apps do not share relevant information on the data and that the apps 'just' work locally in an AI data space.

The ability to run data apps refers to a party having the right capabilities to both invoke and execute these data apps originating from an external party. On the one hand it needs to have the processing capabilities to execute the data apps and on the other hand it needs the mechanisms to orchestrate the data apps and their information flows to jointly fulfil the required pre-processing and enriching functions while providing the data provider with adequate mechanism for maintaining data sovereignty.

5. THE SOLUTION DIRECTION: ORGANISING TRUST AND INTEROPERABILITY IN A FEDERATION OF AI DATA SPACES

In practice, parties are currently already often organised in communities that jointly pursue a common approach on sharing data based on joint agreements. These ‘decentralised infrastructures for trustworthy data sharing in data ecosystems based on commonly agreed principles’ can generically be referred to as AI data spaces, in line with the terminology as used by the European OPEN DEI initiative [20]. As described in [7], many of such AI data spaces already exist within various sectors. There will undoubtedly be new AI data spaces and AI data spaces will disappear or merge.

To build successful AI data spaces, parties need building blocks for managing trust, data sovereignty and (legal, operational, ...) agreements to share data and AI algorithms, as well as capabilities to execute AI algorithms and data apps. Currently the European OPEN DEI endeavour [11] (let by the European Commission) aims at defining the building blocks and standards for data spaces, with the goal of realising interoperability both between the building blocks within specific data space instances (i.e. intra data space interoperability) and between various data space instances (i.e. inter data space interoperability). Jointly, they pursue the bigger goal of an overarching common European data sharing environment.

This chapter describes how AI data spaces adhering to these developments provide the fundament for realising the goals of the NL AIC data sharing working group in jointly realising cross-sectoral, interoperable, AI data spaces to benefit the capabilities of AI in the Netherlands while being aligned the emerging EU data strategy.

5.1 The European data strategy: towards a federation of data spaces

In earlier chapters, the point was made that a new way of data sharing is emerging. One way of looking at this development is the big change from a centralised data space operated by a single organisation (often a platform) to a federation model. Put in other words: *'a change from one central data powerhouse to democratisation of data'*. The advantage of the central data space model is its simplicity. There are however, also several disadvantages: Loss of control and centralisation of power leads to an uneven division of financials gains and blocks innovation. Moreover, Data Providers are faced with both a threat of lock-in and with major integration efforts in case of participation in multiple data spaces is needed. A data space aims to simplify and enable data sharing between organisations of all sizes. It also increases the level of control organisations (and individuals) have over their data.

The change is therefore inevitable and we must all learn to deal with a more complex reality of multiple data spaces where owners of data agree on the ways of working in communities of choice. At the same time, it is to be noted that there will not be just one single European data space. Individual sectors or communities are expected to develop their own instance data spaces, resulting in a multitude of data spaces. It is obvious that being able to seamlessly share data over these data spaces yields clear advantages. It extends the reach and scope of accessible data and allows new business models and solutions to be developed across sectors and regions. These considerations lead to the joint vision and ambition of a federation of interoperable data spaces. This vision is shared with the European ambition as set in the European data strategy [1] and the European OPEN DEI initiative [11] [20] aiming at a federation of interoperable European data spaces.

At this point, it is good to further clarify the individual concepts as expressed in the common goal of the federation of interoperable European data spaces:

- **Data space**

The EU OPEN DEI initiative [11] is working towards (alignment of) the reference architecture for data spaces. It has defined a data space [20] as a *'decentralised infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed principles'*, providing three types of building blocks as will be outlined in section 5.2.

- **Federation**

In a federation of data spaces, each individual data space instance has a high degree of autonomy in developing and deploying its own internal agreements and ICT landscape [1]. However, jointly the individual data space instances pursue a common goal of being able to share data in a trusted manner. Therefore, interface agreements and specifications are the essential design artefact for a federation of data spaces to manage and co-ordinate the information flows between federated data spaces.

- **Interoperable**

For the federation of data spaces to seamlessly interconnect, interoperability between data spaces is key. data space interoperability is more than merely the interoperability of its technical components. An approach to systematically address the interoperability challenges is provided by the new European Interoperability Framework as developed by the European Commission. The framework distinguishes four interoperability levels (technical, semantic, organisational and legal interoperability) under an overarching integrated governance approach. To enable interoperability between data spaces, each of these interoperability levels needs to be addressed.

The vision and ambition of federated and interoperable data spaces closely align with the goals of the NL AIC data sharing working group in jointly realising a cross-sectoral data sharing infrastructure to benefit the capabilities of AI in the Netherlands. As such, this vision and ambition are further referred to as *'federated, interoperable, AI data spaces'*.

In addition to the European data strategy [1] and the EU OPEN DEI initiative [11] on federated and interoperable data spaces, several initiatives exist or are being developed that address a variety of related challenges and topics on data sharing, e.g. GAIA-X, the data sharing Coalition, GO FAIR and many others. To pursue alignment and complementarity, the solution direction for federated AI data spaces extends upon these existing initiatives.

5.2 Building blocks for AI data spaces

As described, the federated data spaces approach is currently pursued by the European Union. A dynamic landscape unfolds with a multitude of already existing data spaces [20], new emerging data spaces and data spaces that are disappearing or merging. In the emerging picture, organisations have the option to join, retract, be active in data spaces in different ways. As data providers, possibly at a price, as data consumers to develop and deploy new and better AI algorithms or as service providers for onboarding data providers and consumers or in providing the data space building blocks.

This dynamic landscape can only function properly if there is a certain level of standardisation and efficiency in the way these data spaces function. This specifically applies to the building blocks that constitute those data spaces. It is to be realised that in defining and standardising these data space building blocks, more is needed than merely technical building blocks and the interoperability thereof. As such, in its work on data space design principles [20], the EU OPEN DEI initiative distinguishes three types of building blocks:

1. building blocks such as *data platforms,* providing support for effective data sharing and exchange as well as for engineering and deployment of data exchange and processing capabilities;

2. building blocks such as *data marketplaces,* where data providers can offer and data consumers can request data[2], as well as data processing applications;
3. building blocks *ensuring data sovereignty,* i.e. the ability for each stakeholder to control their data by making decisions as to how digital processes, infrastructures, and flows of data are structured, built and managed, based on an appropriate governance scheme enabling specification of terms and conditions.

With these types of building blocks as basis, participants can share (potentially) sensitive data within a data space and between data spaces in a trusted and secure manner. The infrastructure of the data space based on these three types of building blocks is referred to as a 'soft infrastructure' [20] providing the required technical, semantic, organisational and legal concepts as defined in the New European Interoperability Framework [27].

5.3 Interoperability within and across AI data spaces: development lines

AI data spaces provide the building blocks for managing trust, data sovereignty and (legal) agreements to share data and / or algorithms and building blocks to execute AI algorithms and data apps. In view of the European ambition on federation of European data spaces, both individual data spaces and multiple data spaces need adequate governance to realise interoperability within and across data spaces. Therefore, a distinction is made on two development lines for data spaces:

- **Intra data space interoperability, between the various building blocks within an individual AI data space instance.**

The definition of federation as provided in section 5.1 indicates that individual AI data space instances have a high degree of autonomy in developing and deploying their own internal agreements and ICT landscape. From that perspective it is to be noted that intra data space interoperability is aimed at providing a reference architecture based on common building blocks and evolution path for developing AI data space instances in an efficient and aligned manner, providing a rich set of features to support the challenges and requirements for AI. It leaves individual data spaces the option for internally deviating from the reference architecture.

- **Inter data space interoperability, between multiple data space instances.**

Interoperability between AI data space instances is key for the federation of AI data spaces to seamlessly interconnect. As described in section 5.1, this is a main goal of the NL AIC data sharing working group in jointly realising a cross-sectoral data sharing infrastructure for AI, and aligns with the EU data strategy. As such, inter data space interoperability requires prescriptive guidelines for individual data space instances to ensure interoperability between them.

Both intra and inter data space interoperability development lines are illustrated in **Figure 4**.

[2] Note: data marketplaces only aggregate metadata and do not store the actual data

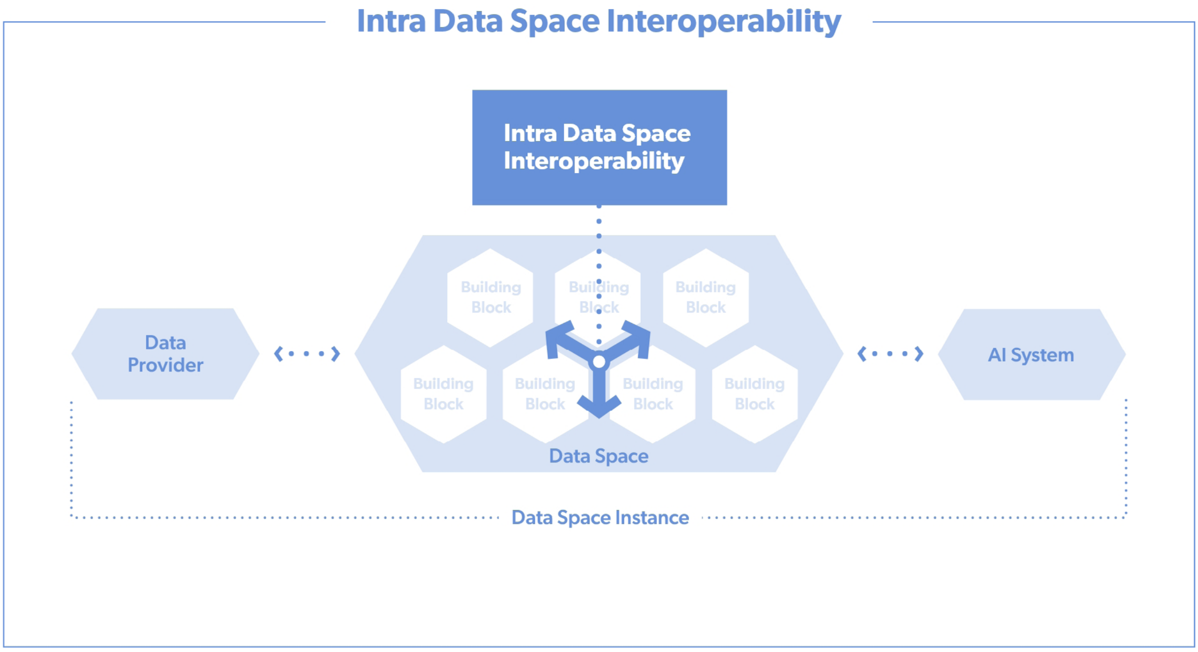


Figure 4a - Intra data space interoperability development line.

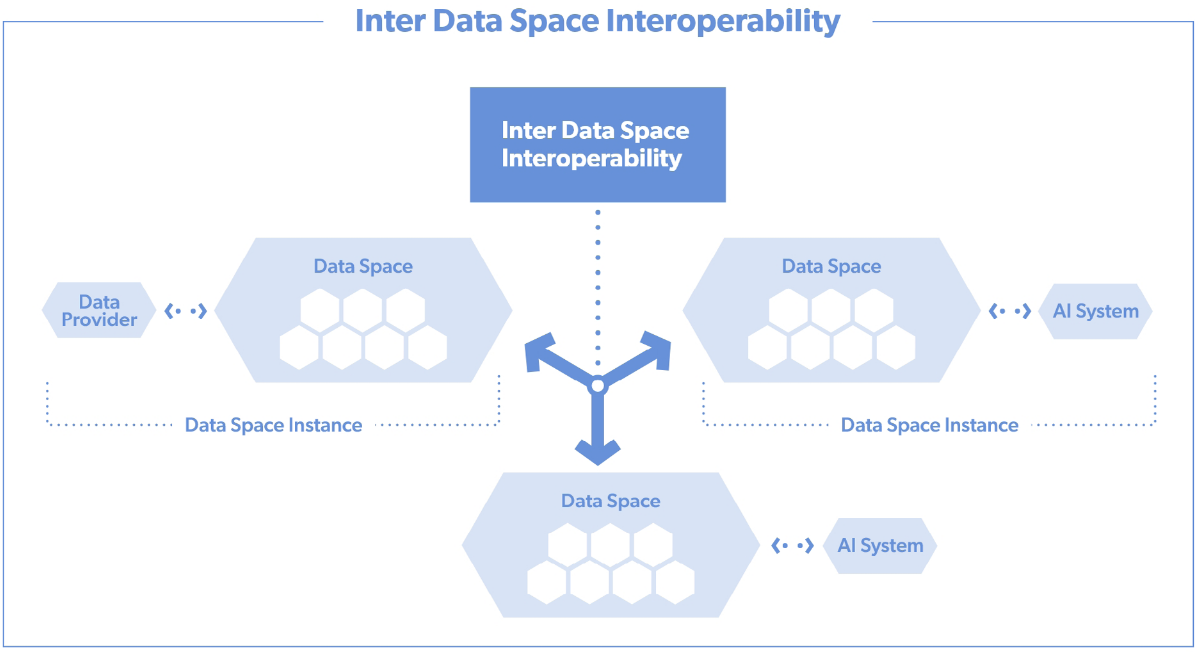


Figure 4b - Inter data space interoperability development line.

5.4 AI data space: interoperability levels

Data space interoperability (both intra data space and inter data space) is more than merely the interoperability of its technical components. An approach to systematically address the interoperability challenges is provided by the new European Interoperability Framework as developed by the European Commission [27]. The framework distinguishes four interoperability levels (technical, semantic, organisational and legal interoperability) under an overarching integrated governance approach as depicted in Figure 5.

Each of the four functional levels needs to be addressed in developing AI data spaces and their intra and inter data space interoperability. Within each of these levels, specific interoperability topics for intra and inter data space interoperability can be further distinguished, as described in the following paragraphs.

5.4.1 Technical level

The technical level covers the software and hardware components for controlled, sovereign and secure sharing of data. It consists of five sub-levels with topics that require adequate governance:

- *Secure peer-to-peer connectivity (or 'Handshake'),* handling aspects such as the secure interaction protocol and remote attestation, as well as a meta-data message information model.
- ***Identity and authentication,*** which is done within an AI data space at two levels: (1) as legal identities, to identify and authenticate natural persons, organisations or software components as legal entities, and (2) as AI data space members and as such adhering to the AI data spaces (legal and organisational) agreements.

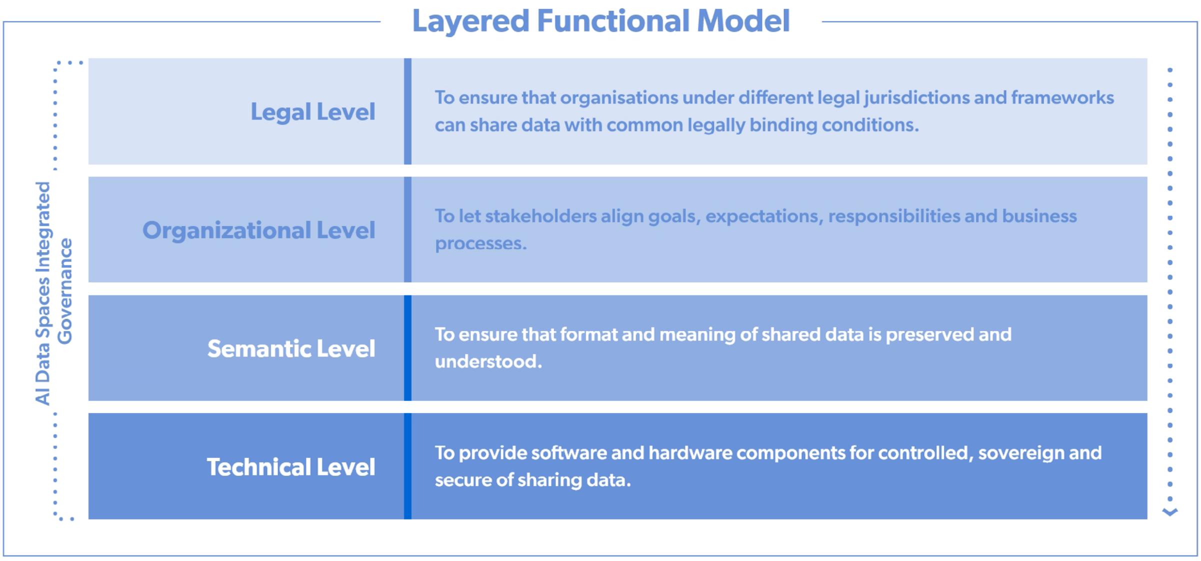

Layered Functional Model
AI Data Spaces Integrated Governance
Legal Level
To ensure that organisations under different legal jurisdictions and frameworks can share data with common legally binding conditions.
Organizational Level
To let stakeholders align goals, expectations, responsibilities and business processes.
Semantic Level
To ensure that format and meaning of shared data is preserved and understood.
Technical Level
To provide software and hardware components for controlled, sovereign and secure of sharing data.

Figure 5 - Layered functional model as aligned with the New European Interoperability Framework [27].

- *Authorisation* encompasses the definition, registration and enforcement of access and usage control policies, to prevent data being mis-used.
- *Data, processing and service brokering,* entailing the management and exposure of metadata on the data, processing and service resources available in individual AI data spaces.
- *App enabling* to invoke and orchestrate the execution of (third party) data apps in a secure environment, i.e. an Application Execution Environment (AEE) interworking with the Policy Enforcement Framework (PEF) to enforce data usage policies and supporting Cloud integration to provide the processing functionality for AI algorithms.

5.4.2 Semantic level

At the semantic level, it may be obvious that a shared and common semantic data model to be jointly used by Data Providers and Data Consumers has major advantages in minimising complexity for interconnection and collaboration. However, such a jointly used common semantic data model may appear to be an utopia. Therefore, mechanisms for semantic conversion need to be supported in the AI data space architecture. Enabled by the IDS-connector (security gateway) architecture as recently standardised [28], this may be taken care of by means of semantic management data apps. Semantic management data apps may be developed for specific semantic conversions or for enabling easy-to-use mapping between semantic models.

5.4.3 Organisational level

The organisational level refers to the way in which the agreements, expectations and processes are aligned to achieve the common goals for controlled data sharing. This includes the onboarding and certification (according to common and accepted criteria), aligned service level agreements (for realising overarching expectations and quality control) and aligned operations and customer processes (for improved operating efficiency and enhanced customer experience). It also includes business agreements around topics such as intellectual property of data-derived results, revenue sharing, academic authorship and pay-for-data.

5.4.4 Legal level

The aspect of legal interoperability between AI data spaces presents a major challenge. Currently, legal aspects are mainly dealt with within a single AI data space by pre-defining the set of multi-lateral legal agreements to which individual Data Providers and Data Consumers are bound to adhere to when signing up for joining the AI data space. However, this provides interoperability challenges on the legal aspects in case a Data Service Provider and a Data Consumer are member of different (or even no) AI data spaces, with varying multilateral legal agreements, and possibly under differing legal jurisdictions. To address this challenge, a joint legal agreement is required, which at run-time is supported by a process for verification of legal status for data transactions.

6. INTRA DATA SPACE DEVELOPMENT LINE: INTEROPERABILITY WITHIN AN AI DATA SPACE

The intra data space development line defines a reference architecture for the development of specific AI data space instances, providing a rich set of features to support the challenges and requirements of AI. As such, the following sections in this chapter address its business requirements (expressed in terms of architectural principles), the underlying business role model and the intra data space building blocks providing its generic and re-useable capabilities, subsequently.

As indicated in section 5.3, the development line as described in this chapter is aimed at providing a reference architecture and evolution path for developing AI data space instances in an efficient and aligned manner, providing a rich set of features to support the challenges and requirements for AI and based on generic and re-usable building blocks. It leaves individual AI data space instances the option for internally deviating from the reference architecture.

The subsequent sections in this chapter address the intra data space development line by describing its business requirements in terms of architectural principles, define its underlying business role model and present its constituting generic and re-usable building blocks. The detailed (technical) design of the intra data space reference architecture will be elaborated in a future publication.

6.1 Business requirements: architectural principles for AI data spaces

The business requirements define the main strategic and organisational functions and needs of AI data spaces. The business requirements are expressed by means of architectural principles for AI data spaces. Together, they provide the fundament to address the challenges as defined in chapter 4 on the willingness and ability to share data, execute AI algorithms and/or locally run data apps.

6.1.1 Seamless integration with the permission management system

Before a data provider is allowed to share data with an AI algorithm, the permission to do so must be obtained and accounted for. Permission management for sharing data with AI algorithms has various complexities both on the aspects of obtaining the appropriate lawful ground to share data, the associated management of authorisations and usage conditions and accountability management. This for instance applies when sensitive (personal) data is to be shared. Moreover, ethical considerations and legal conditions on sharing such sensitive (personal) data are subject to societal debate and are expected to vary per sector / application area and change over time.

As such, permission management, encompassing both the lawful ground management, authorisation management and accountability management, is of major importance when developing AI data spaces. Within the NL AIC, the topic of permission management is addressed by the Human Centric AI working group (ethical, legal and societal aspect). Therefore, a reference architecture for the permission management system will be developed in collaboration between the working groups of data sharing and Human Centric AI.

6.1.2 Sovereignty over ICT-resources through enforceable policies: data, algorithms, apps, compute, …

Sovereignty is a natural person's or organisation's capability of being entirely self-determined with regard to its ICT-resources, being (amongst others) data, AI-algorithms, apps and computational power. Capabilities for sovereignty allow the legally entitled person or organisation to exclusively decide about the usage of its ICT-resources, requiring organisations to be in control over the conditions under which their ICT-resources are shared and they may be processed by other parties.

Sovereignty requires building blocks from the AI data spaces to define, manage and support policies on sharing their ICT-resources, including operational statements and the enforcement thereof. These building blocks are required for controlling (access to and usage of) ICT-resources.

Within AI data spaces the variety of involved ICT-resources and their legally entitled entities (including both data providers, AI-algorithm providers, app providers and providers of computational power) provides complexity to providing a coherent set of capabilities for enabling adequate levels of sovereignty and control to each of the stakeholders. Moreover, interdependency between these capabilities will exist and must be taken care of. For instances, for a data provider to set a policy on whether an app or AI algorithm may get access to its sensitive data, he will need sufficient information on the features of the app or AI-algorithm (e.g. on which data attributes are actually used, the level of deep learning, the combination of data sources or the dissemination of the results) to make the judgement whether he should allow the app or AI-algorithm access to his data. This judgment should be highly automated and requires (FAIR) metadata not just on the AI data space but also on the apps or AI-algorithms.

6.1.3 Enabled for locally executing data apps at the data provider: distributed data analytics

Data apps may be used to process data locally within the (security) domain of the data provider or data consumer. This is referred to as 'app enabling'. Locally executing data apps may for instance be used for data enrichment, for semantic conversion, data quality management and de-identification (anonymisation, pseudonymisation).

It is to be realised that local deployment of data apps within a data providers security domain will not only be instantiated and managed by the data provider itself. There may be apps originating, instantiated and managed by external third parties. Hence, two cases may be distinguished:

- ***Data provider app enabling***, in which the data provider is in the lead for instantiating, configuring and managing apps within its security domain.
- ***Third party app enabling***, in which a third party is in the lead for instantiating, configuring and managing apps within a security domain of a data provider.

A specific type of locally executing data apps is for distributed data analytics. Privacy Enhancing Technologies are becoming available for which the data to be processed does not have to be gathered into a single database or location. As such, federated learning is able to learn by distributed data analytics algorithms. Furthermore, secure Multi-Party Computation offers possibilities to execute algorithms on encrypted data without external parties having the opportunity to decrypt the source data itself. These technologies can be used in case the different data sources cannot be simply brought together. This is also addressed in the following architectural topic on collaboration models.

6.1.4 Supporting various collaboration models

Data sharing for AI encompasses AI Models accessing data from different sources to achieve a desired result, e.g. a verified AI model or an AI model output. Unfortunately, the different data sources for AI algorithms cannot always simply be brought together. Either because the amount of data is too large to process, or other reasons like confidentiality, ethical and legal considerations. Think of privacy restrictions due to GDPR or company confidentiality, for example. These reasons imply that data should remain with its provider or administrator and not to be transferred to other organisations: only access to data is provided instead of sharing the data.

To distinguish the various types of interactions between the providers of data and AI algorithms four archetypes have been identified that need to be supported by the reference architecture for AI data spaces, referred to as collaboration models [29]:

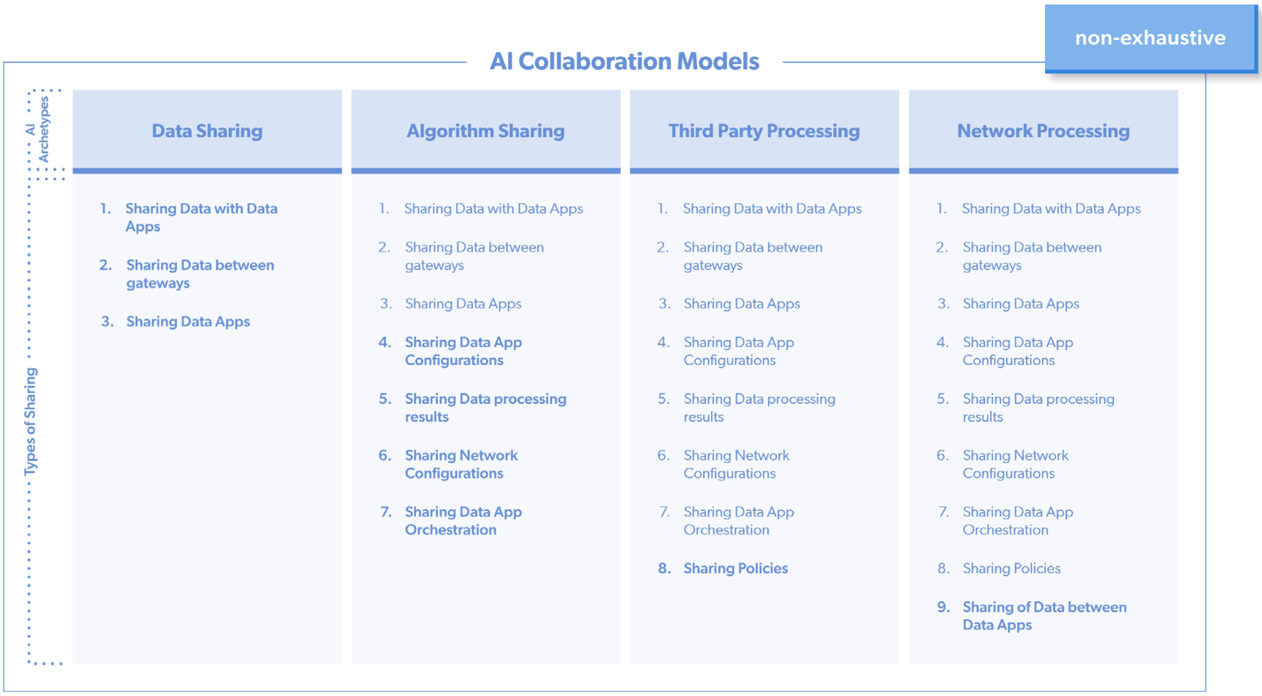
1. ***data sharing,*** in which the data is transferred from the data provider to the organisation executing the AI algorithm.
2. ***Algorithm Sharing,*** in which the AI algorithm is transferred and executed in the security domain of the data provider.
3. ***Third Party Processing,*** in which both the data and the AI algorithm are transferred and executed in the security domain of a (trusted) third party.
4. ***Network Processing,*** in which the execution of the AI algorithm is done in a distributed manner by a network of parties, e.g. in the case of Federated Learning or secure Multi-Party Computation.

data sharing for AI encompasses the different AI Archetypes and types of information sharing that occurs in each Archetype. **Figure 6** provides a non-exhaustive overview of the (for now) identified archetypes.

The different AI collaboration models will be further described in a future publication.

6.2 Business role model for AI data spaces

As described in section 5.1, the vision and ambition of ‘federated, interoperable, AI data spaces’ forms the fundament for the NL AIC data sharing working group in jointly realising a cross-sectoral data sharing infrastructure to benefit the capabilities of AI in the Netherlands. A data space has been defined by the European OPEN DEI initiative [20] as a decentralised infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed principles. Within a data space, participants can share (potentially) sensitive data in a trusted and secure manner.



AI Collaboration Models

non-exhaustive

AI Archetypes	Data Sharing	Algorithm Sharing	Third Party Processing	Network Processing
Types of Sharing	**1. Sharing Data with Data Apps** **2. Sharing Data between gateways** **3. Sharing Data Apps**	1. Sharing Data with Data Apps 2. Sharing Data between gateways 3. Sharing Data Apps **4. Sharing Data App Configurations** **5. Sharing Data processing results** **6. Sharing Network Configurations** **7. Sharing Data App Orchestration**	1. Sharing Data with Data Apps 2. Sharing Data between gateways 3. Sharing Data Apps 4. Sharing Data App Configurations 5. Sharing Data processing results 6. Sharing Network Configurations 7. Sharing Data App Orchestration **8. Sharing Policies**	1. Sharing Data with Data Apps 2. Sharing Data between gateways 3. Sharing Data Apps 4. Sharing Data App Configurations 5. Sharing Data processing results 6. Sharing Network Configurations 7. Sharing Data App Orchestration 8. Sharing Policies **9. Sharing of Data between Data Apps**

Figure 6 - AI collaboration models.

The International Data Spaces Reference Architecture Model (IDS RAM [30]) provides an architecture and design for developing the data spaces in line with the design principles and building blocks as defined by OPEN DEI and is currently (aimed at) becoming part of the EU Data Strategy. The IDS architecture has recently been standardised [28]. Moreover, a quick scan of the current data sharing initiatives by the NL AIC data sharing working group [7] has indicated that the choice for IDS is in line with international developments and standards and a safe way to pursue by the NL AIC.

Therefore, the reference architecture for AI data spaces is based on IDS. Its role model is based on the IDS role model [30], and tailored into the 'NL AIC role model', i.e. a specific implementation of the IDS role model applicable for AI data spaces. The most important adaptation to the IDS role model is the introduction of a separate role which will provide processing capacity to execute the AI algorithms (AI Operator) and a role which will be responsible for the orchestration of bringing together the data and AI algorithms (AI Orchestrator). The Data Consumer role in IDS corresponds to the AI Orchestrator role (as the formal consumer of data) and AI Operator role (as the technical consumer of the data). The formal and technical responsibilities are thus separated, giving room for parties which are only responsible for the technical execution and parties that orchestrate the controlled data flows and algorithm execution.

In **Figure 7** the AI data spaces role model is given together with a mapping to the IDS role model.

As Figure 7 shows, the AI data spaces role model distinguishes eight core roles. These are described in **Table 1.**

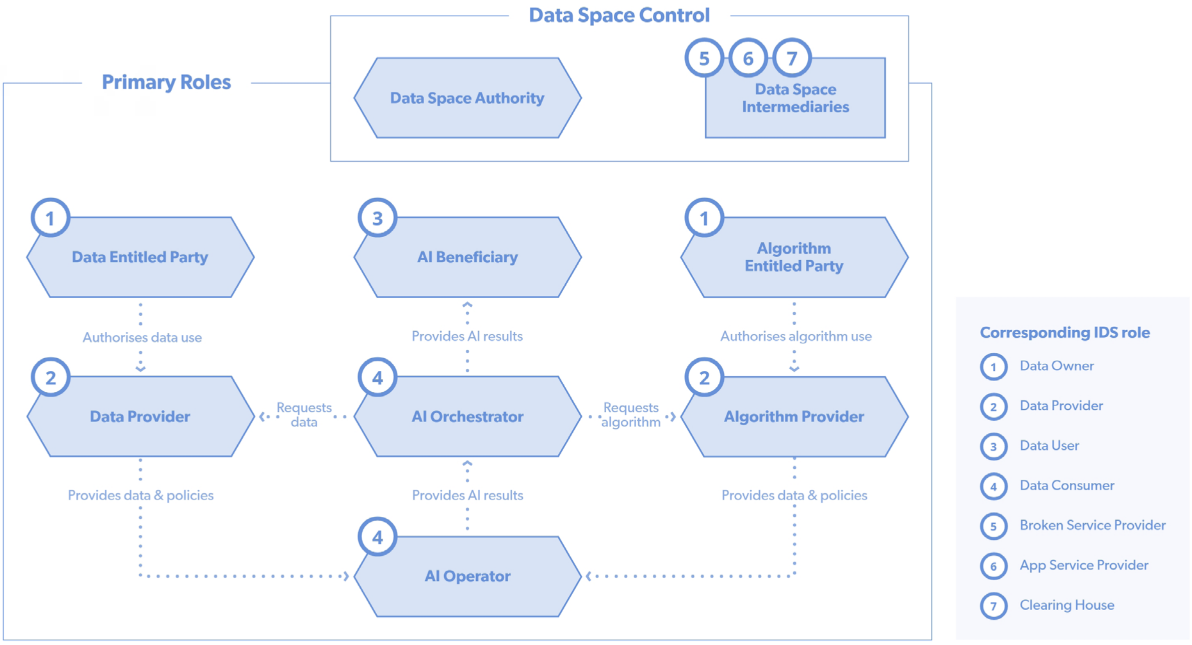


Figure 7 - AI data spaces role model and its mapping to the IDS role model.

#	Core Role	Description
1	AI Beneficiary	The two desired results of an AI interaction are the algorithm output and the verified algorithm. The AI Beneficiary role refers to the party that is interested in this result and therefore initiates an AI interaction. This means that the AI Beneficiary receives the results that are requested from the AI Orchestrator. The AI Beneficiary is responsible for initiating an AI interaction in the ecosystem via an AI Orchestrator.
2	AI Orchestrator	The AI Orchestrator orchestrates the intended AI interaction and ensures that the AI algorithm yields the intended results for the AI Beneficiary. The AI Orchestrator properly manages and provides policies for what it orchestrates, and the end result it is holding to the AI Operator. The AI Orchestrator understands what core components for AI are required and is tasked with bringing these together. The AI Orchestrator is responsible for identifying and bringing together relevant data and algorithm. The AI Orchestrator is also responsible for properly assessing policies that are relevant to the intended AI result. Lastly, the AI Orchestrator is responsible for the proper logging of (parts of) transactions for which policies are evaluated and enforced.
3	AI Operator	The AI Operator is responsible for providing the core component 'environment for execution of algorithm with data'. This functionality is called the 'Application Execution Environment'. Within this environment, algorithms are executed with the required data in order to produce the intended results of the AI algorithm. Next to providing the Application Execution Environment, the AI Operator is responsible for properly assessing policies that are relevant during the execution. Lastly, the AI Operator is responsible for the proper logging of policy enforcement and what execution activities are processed.
4	Data Provider	Data Providers hold data in the ecosystem. The Data Provider properly manages policies for the data it is holding. It enforces access policies and provides additional policies to the AI Operator. The Data Provider also manages the quality and availability of data on behalf of Data Entitled Parties. The Data Provider makes data available for approved AI use cases. The Data Provider is also responsible for properly assessing policies that are relevant to them. Lastly, the Data Provider is also responsible for the proper logging of (parts of) transactions for which policies are evaluated and enforced.
5	Data Entitled Party	Data Entitled Parties have one or more entitlements, e.g. having control over or being the subject of the data of the Data Provider. The Data Entitled Party has the right to define the terms and conditions of use of data to which it is entitled. The Data Entitled Party is responsible for managing terms and conditions of use of data to which it is entitled, in their own systems or elsewhere in the ecosystem.
6	Algorithm Provider	Algorithm Providers hold the algorithm in the ecosystem. The Algorithm Provider properly manages policies for the algorithm(s) it is holding. It enforces access policies and provides additional policies to the AI Operator. The Algorithm Provider also manages the quality and availability of algorithm(s) on behalf of Algorithm Entitled Parties. The Algorithm Provider makes algorithm(s) available for approved AI use cases. The Algorithm Provider is also responsible for properly assessing policies that are relevant to them. Lastly, the Algorithm Provider is also responsible for the proper logging of (parts of) transactions for which policies are evaluated and enforced.
7	Algorithm Entitled Party	Algorithm Entitled Parties have one or more entitlements to the algorithm of the Algorithm Provider. The Algorithm Entitled Party has the right to define terms and conditions of use of the algorithm to which it is entitled. The Algorithm Entitled Party is responsible for managing terms and conditions of use of algorithms to which it is entitled, in their own systems or elsewhere in the ecosystem.
8	Data Space Authority	AI data spaces, comprising of the previously described roles, may potentially grow very large. In these larger ecosystems, in which not all participants may directly know each other, certain functionality is needed to ensure that interactions between parties are supported. The data space Authority is responsible for the (legal and operational) agreements within a data space and for managing a registry of participants. The data space Authority is also responsible providing a clearing house for those data sharing patterns that require central clearing of transactions.

To implement these core roles of AI data spaces, a set of generic building blocks (capabilities) have been identified and defined that should be developed in an interoperable manner, i.e. intra data space interoperability. These intra data space architecture and building blocks are elaborated in a future publication.

6.3 Building blocks and structure for AI data spaces

Generic and reusable building blocks provide capabilities for the parties fulfilling the roles in the AI data space role model as described in the previous section. For AI data spaces the building blocks are categorised into 'data space authority' building blocks, 'data processing' building blocks and 'data sharing' building blocks. These building blocks are depicted in **Figure 8**.

The figure shows that the structure of an AI data space with three categories of:

1. The data space ***authority building blocks*** provide the functions associated to the 'agreement framework' as depicted in, which are sometimes also referred to as the 'trust framework'. The scheme owner provides the AI data space governance framework for managing the commonly agreed upon procedures within the AI data space, e.g. on legal agreements and, conditions certification, applicable standards and architecture and the certification policy. The 'data space authority administrator' provides the supporting functions to manage participating entities in the AI data space, including the onboarding and accession criteria and processes, management of the identities and attributes of participants.

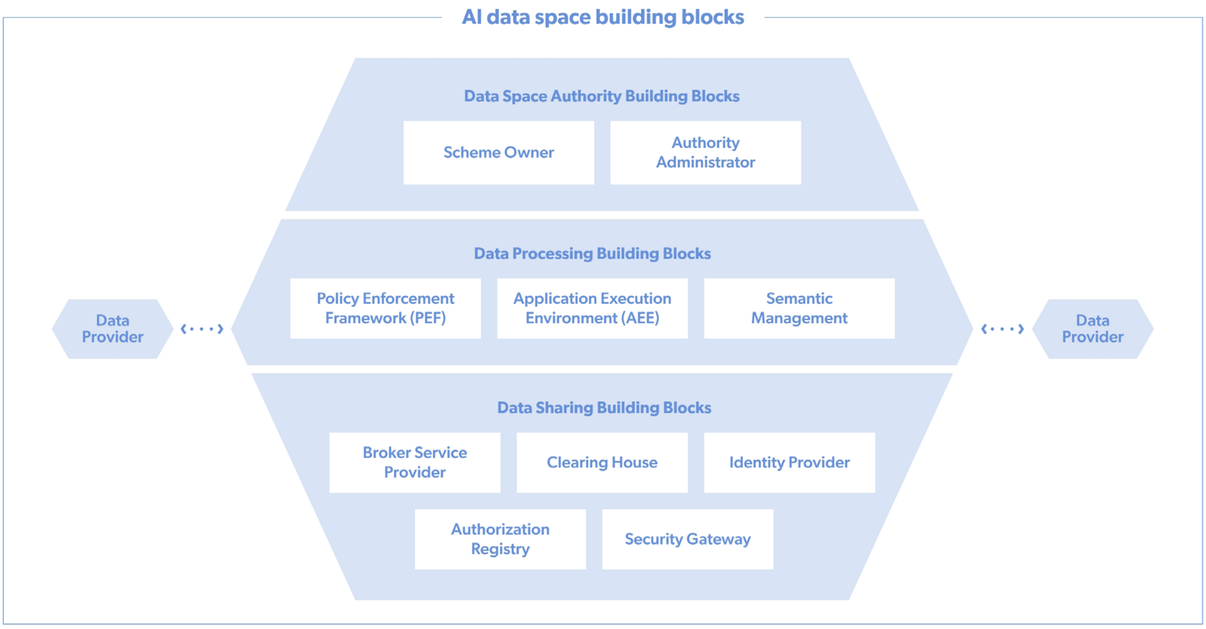

AI data space building blocks
Data Space Authority Building Blocks
Scheme Owner
Authority Administrator
Data Processing Building Blocks
Policy Enforcement Framework (PEF)
Application Execution Environment (AEE)
Semantic Management
Data Provider
Data Provider
Data Sharing Building Blocks
Broker Service Provider
Clearing House
Identity Provider
Authorization Registry
Security Gateway

Figure 8 - AI data space building blocks

2. The ***data processing building blocks*** provide edge processing (computing) capabilities for data apps, e.g. for data apps for managing semantics (format conversion or mapping) of for supporting locally executing AI algorithms based on Federated Learning or secure Multi-Party Computation. Cloud integration could provide the manner for implementation thereof, with GAIA-X potentially being a good match. Moreover, data control and data sovereignty are enabled through integration with the Policy execution Framework (PEF).

3. The ***data sharing building blocks*** provide the hardware and software components to enable controlled data sharing with data sovereignty between data providers and data consumers. They are based on the roles as defined in the IDS Reference Architecture Model (IDS RAM [30]).

The individual building blocks and how they are interrelated will be further elaborated in a future publication.

Figure 9 depicts the data space structure with the categorisation of the building blocks, including the mapping to the NL AIC role model. Moreover, the OPEN DEI design principles for data spaces [20] identify and describe a soft infrastructure stack with 12 building blocks that provide the basic capabilities for a data space. How these are mapped on a data space structure is also included in Figure 9.

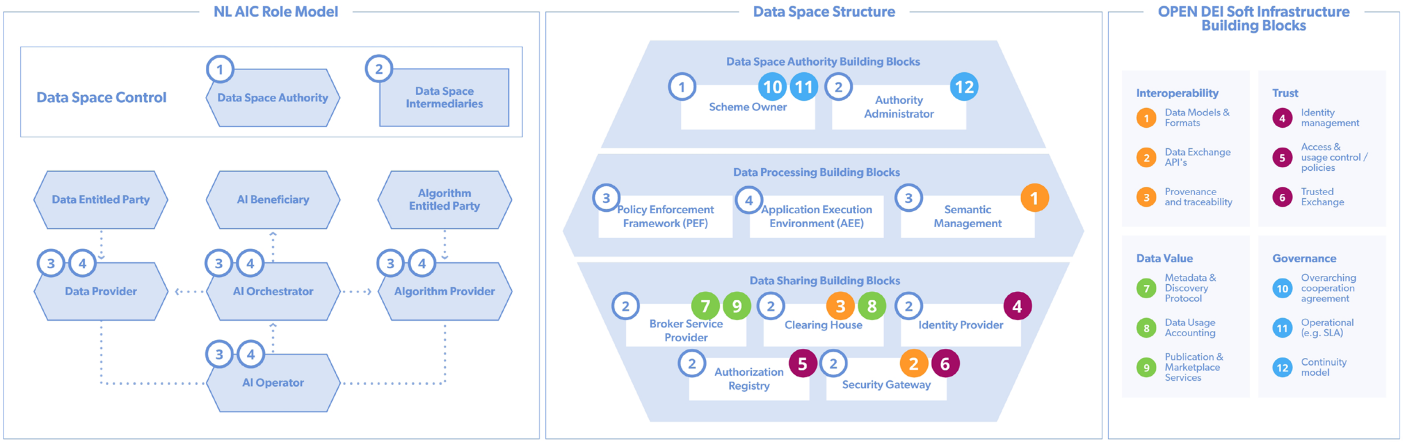


Figure 9 - Data space structure (center) including mapping on the NL AIC Role Model (left) and the 12 building blocks in the OPEN DEI soft infrastructure stack (right).

7. INTER DATA SPACE DEVELOPMENT LINE: INTEROPERABILITY ACROSS AI DATA SPACES

There will not be just one single AI data space to rule the world. Individual sectors or communities are expected to develop their own AI data space instances. Being able to seamlessly share data over these AI data space instances yields clear advantages. It extends the reach and scope of accessible data and allows new business models and services to be developed across sectors and regions.

To enable interoperability across AI data space instances an overarching interoperability governance framework is required on the technical, semantic, organisational and legal level, in line with the implementation as described in chapter 5.4.

The following sections in this chapter address the business requirements and architecture of such an overarching interoperability governance framework for a federation of AI data spaces.

7.1 Business requirements: architectural principles for federation of AI data spaces

In this section, the business requirements are expressed by means of architectural principles for the federated AI data spaces providing the ability to share data and algorithms between AI data space instances, to effectively execute calculation intensive AI algorithms and to locally process (large amounts of) data and to locally execute data apps, as stated in the subsequent section of chapter 4.

7.1.1 Single entry point for multiple data sharing relationships across AI data spaces

Data Providers are faced with both a threat of lock-in by specific AI data spaces and with major integration efforts in case participation in multiple data sharing relationships or AI data spaces is needed, e.g. on defining and enforcing data control and sovereignty capabilities.

As alternative, a single entry point for the data provider is needed to simultaneously manage and control his data sharing relationships, yielding clear operational benefits over siloed approaches in user-friendliness, complexity, efficiency and costs [31]. Such a single entry point is also referred to as ‘security gateway’. Moreover, it prevents data providers from a threat of lock-in and from major integration efforts on managing data control and sovereignty capabilities over multiple data sharing relationships.

7.1.2 Data sovereignty and control based on standardised frameworks

As described in 6.1.2, data sovereignty requires organisations to be in control over the conditions under which their data is shared and how it may be processed by other parties. This requires building blocks from the data sharing system to define, manage and support their data sharing policies, operational data sharing statements and the enforcement thereof. These building blocks are required for controlling (access to and usage of) data flows.

This not only holds within an AI data space instance (intra), also between AI data space instances (inter). To ensure interoperability of data sovereignty and control building block across AI data space instances, these building blocks should be based on standardised frameworks and be jointly agreed upon. For instance, for defining and enforcing data sharing policies, various standards exist, requiring a joint agreement on which to use within AI data spaces. The widely used XACML policy framework [32] provides a standard for access control, whereas the ODRL policy framework [33] [34] provides a standard covering both access and usage control. For this reason, ODRL has been adopted by IDS which on its turn provides the basis for the reference architecture for AI data spaces as described in a future publication.

7.2 Federation of AI data spaces architecture development

The data sharing Coalition is an open and growing, international initiative in which a large variety of organisations collaborate to drive cross-sector data sharing at scale. In their 'data sharing Canvas' [35], a comparison has been made between various harmonisation options (i.e., the Full Harmonisation model, the Bilateral Harmonisation model and the Partial Harmonisation model) to enable interoperability across data spaces, which is also applicable for AI data spaces.

In the 'data sharing Canvas' [35], a motivation is provided for preferring the partial harmonisation model, in which various limitations of both other models are overcome by introduction of a new role, a 'data space Proxy'. The role of a Proxy is to absorb the complexity of harmonisation for data spaces and its participants as much as possible by implementing all harmonisation requirements. This enables a data provider in one data space to share data with a data consumer in another data space, while limiting impact for both the data provider and the data consumer.

The proxy model for partial harmonisation is depicted in **Figure 10**.

The main functionality of the proxies is to translate data space specific transactions to their harmonised equivalents:

- Proxies will translate AI data space specific language to a harmonised language in the Harmonisation Domain to enable multilateral end-to-end Interoperability,
- Proxies will facilitate Trust across AI data spaces by conforming to the rules and agreements of an overarching Trust Framework,
- Proxies will enable the discovery of data providers across AI data spaces.

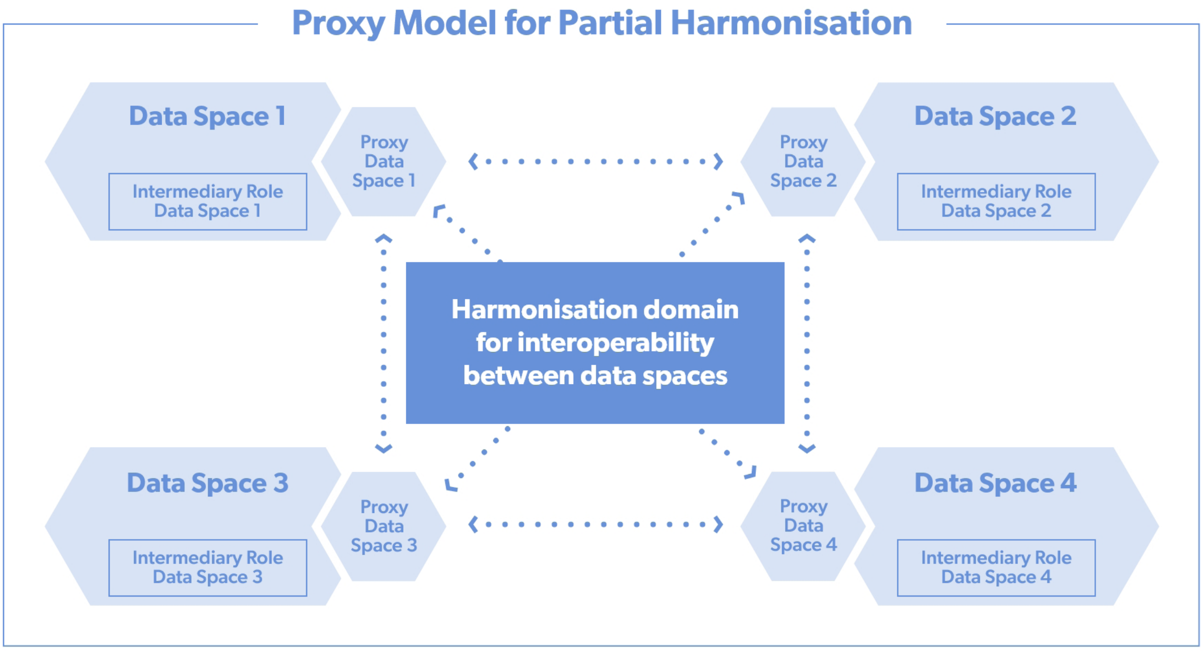

Proxy Model for Partial Harmonisation
Data Space 1
Intermediary Role Data Space 1
Proxy Data Space 1
Data Space 2
Intermediary Role Data Space 2
Proxy Data Space 2
Harmonisation domain for interoperability between data spaces
Data Space 3
Intermediary Role Data Space 3
Proxy Data Space 3
Data Space 4
Intermediary Role Data Space 4
Proxy Data Space 4

Figure 10 - Visual representation of the proxy model, applied to data space interoperability.

The Proxies implemented by all AI data spaces will form a network, the Harmonisation Domain, which enables actors in one AI data space to share data effortlessly with actors in another AI data space.

An overarching 'AI data space Trust Framework' addressing the joint (legal, operational, semantic and technical) agreements between adhering AI data spaces will be pivotal in realising data space interoperability. Amongst others, it provides an overarching legal framework, to which the individual AI data space instances (and their participants) agree to adhere.

The Proxy model with a Harmonisation Domain as architecture to enable interoperability across data space instances still needs further detailing and refinement, which is currently work in progress in the data sharing Coalition. Continuous alignment between the NL AIC and the data sharing Coalition is needed to ensure that the NL AIC is aware of timing and scope of that work so it can adjust its own activities accordingly and to ensure the needs from the NL AIC community to enable interoperability across AI data spaces are taken into account in the activities of the data sharing Coalition.

8. DOCUMENT DEVELOPMENT

This chapter outlines the further development of this document. To this end, the following sections address the governance of the document development and the development roadmap, respectively.

8.1 Governance in documentation development

Providing future AI data spaces with the right tools for implementation requires a fine balance between expert recommendation and fit with future AI data space participant needs. As briefly introduced in chapter 1, the NL AIC deploys a dedicated working group tasked with guiding this process, the data sharing working group.

The data sharing working group consists of a program office, with dedicated experts that lead activities of the working group, and participants of the working group. These participants are AI and data sharing experts with a wide variety of backgrounds that are interested in NL AIC activities and data sharing topics in particular. A subset of these participants is active in the Advisory Board (more frequent meetings and active contribution to working group deliverables).

The Data sharing program office has delivered this document based on learnings from AI data space proof of concepts (as referenced in chapter 1.2) and dialogue with the data sharing working group participants and Advisory Board.

During development, the NL AIC's data sharing working group keeps close contact with initiatives such as FAIR, like-minded coalitions such as the data sharing Coalition, international initiatives such as IDSA, FiWare and EU initiatives started in the context of European data spaces. This close contact is for the purpose of limiting unnecessary deviations in content, direction and standards.

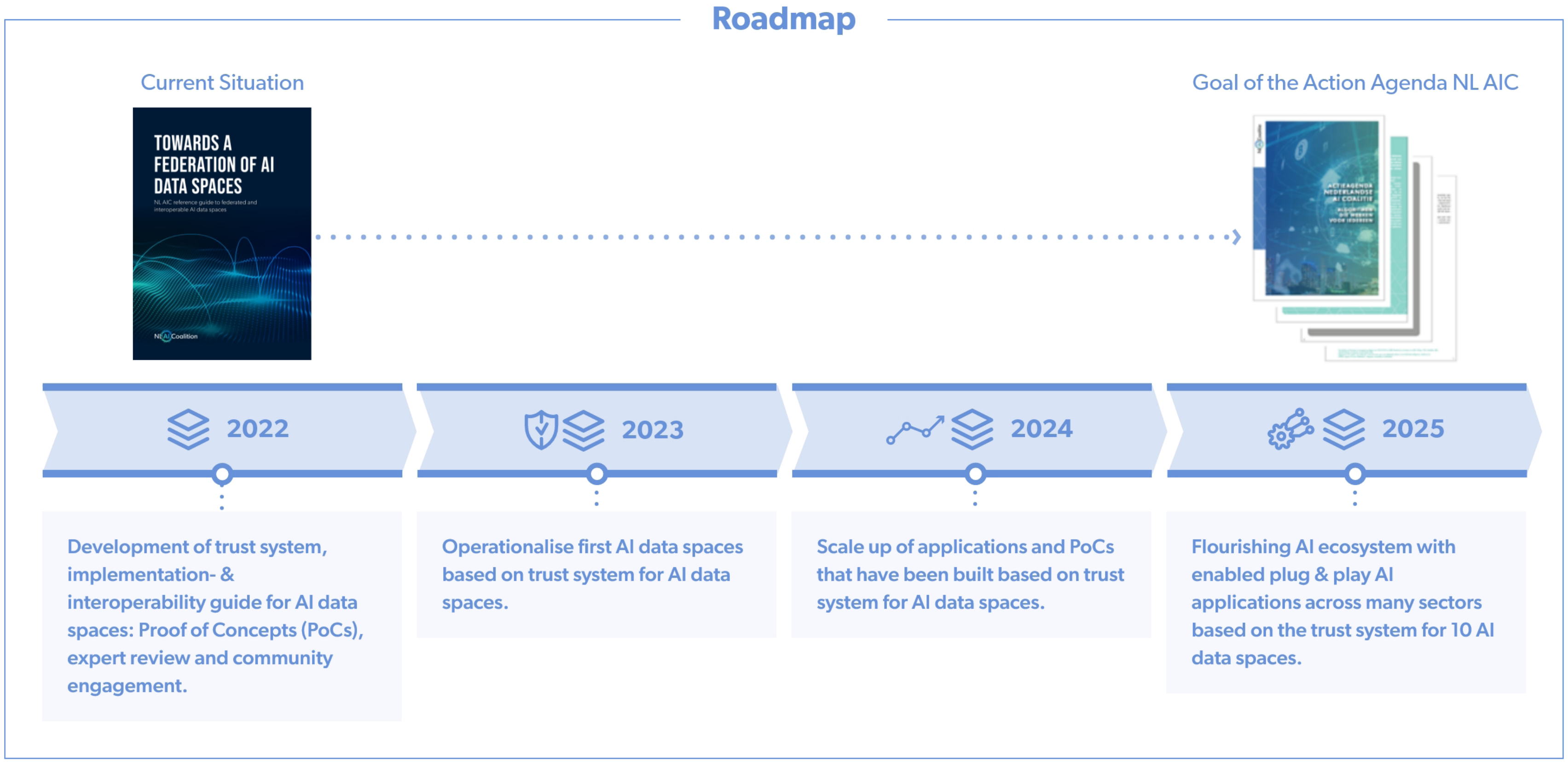
8.2 Development roadmap

The development, introduction and adoption of Federated, Interoperable, AI data spaces will be a major goal of the NL AIC data sharing working group for the coming time period 2022 – 2025. During this time period, the data sharing working group aims to help realise 10 AI data spaces based on the reference documentation. This document outlines the vision for establishing Federated, Interoperable, AI data spaces. This document is complemented by two documents that provide more details on how organisations can build and develop interoperable data spaces:

1. Reference guide for ***intra*** data space interoperability. This report will provide guidance for implementing a data space (either new/from scratch or an existing data space to be made interoperable). Privacy enhancing technologies are covered on this report.
2. Reference guide for ***inter*** data space interoperability. This report will provide guidance for making multiple data space compatible, including semantic aspects. Architectural topics will be covered.

The NL AIC data sharing working group aims to release initial versions of these documents by the end of 2021. Versions will be developed in accordance with the aforementioned documentation development governance.

Based on reference documentation, over the coming years the NL AIC data sharing working group actively pursues and supports development of 10 Federated, Interoperable AI data spaces.



Roadmap

Current Situation

Goal of the Action Agenda NL AIC

TOWARDS A FEDERATION OF AI DATA SPACES
NL AIC reference guide to federated and interoperable AI data spaces
NL AI Coalition

2022

Development of trust system, implementation- & interoperability guide for AI data spaces: Proof of Concepts (PoCs), expert review and community engagement.

2023

Operationalise first AI data spaces based on trust system for AI data spaces.

2024

Scale up of applications and PoCs that have been built based on trust system for AI data spaces.

2025

Flourishing AI ecosystem with enabled plug & play AI applications across many sectors based on the trust system for 10 AI data spaces.

Figure 11 - High-level roadmap for the development of the reference architecture documentation as part of a multi-year approach

REFERENCES

[1] European Commission (2020). “data sharing in the EU – common European data spaces (new rules)”. 2020. URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules-_en

[2] NL AIC (2021). “About NL AIC”. 2021. URL: https://nlaic.com/en/about-nl-aic/

[3] The Netherlands AI Coalition (NL AIC) working group data sharing (2020). “Verantwoord datadelen voor AI”. URL: https://nlaic.com/wp-content/uploads/2020/03/Verantwoord-datadelen-voor-AI.pdf.

[4] The Netherlands AI Coalition (NL AIC), data sharing working group (2020). “Responsible data sharing in AI”. URL: https://nlaic.com/wp-content/uploads/2020/10/Responsible-data-sharing-in-AI.pdf.

[5] The Netherlands AI Coalition (NL AIC), data sharing working group. ‘Van First-time-Engineering naar Operatisatie”. URL: https://nlaic.com/wp-content/uploads/2020/08/NL-AIC-Naar-First-time-Engineering-en-Operationalisatie.pdf.

[6] The Netherlands AI Coalition (NL AIC), data sharing working group (2020). “GAP-analysis- From data sharing proofs-of-concept towards operation of the system architecture”. March 2021. URL: https://nlaic.com/wp-content/uploads/2021/03/NL-AIC-GAP-Analysis.pdf.

[7] Langley, D. et al. The Netherlands AI Coalition (NL AIC), data sharing working group (2020). “AI Ecosystem & Market Analysis - Quick scan of data sharing market to validate blueprint of the NL AIC“. February 2021. URL: https://nlaic.com/wp-content/uploads/2021/02/AI_Ecosystem_and_Market_Analysis_Data_Sharing_4-feb-2021.pdf.pdf

[8] European Commission (2020). “On Artificial Intelligence - A European approach to excellence and trust”. European Union, 2020. URL: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

[9] European Commission (2021). “A European approach to Artificial intelligence,” European Union, 2021. URL: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

[10] European Commission (2020). “Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act),”. European Union, 2020, URL: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

[11] EU OPEN DEI Initiative. URL: https://www.opendei.eu/.

[12] European Commission (2020). “A European strategy for data,”. European Union, 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

[13] IDSA (2019). “IDS-RAM 3.0”. 2019. URL: https://internationaldataspaces.org/ids-ram-3-0/

[14] European Commission (2019). “A definition of Artificial Intelligence: main capabilities and scientific disciplines”. 2019. URL: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[15] European Union Law (2021). “Artificial Intelligence Act”. 2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

[16] Grand View Research (2021). “Artificial Intelligence Market Analysis Report”. 2021. URL: https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market

[17] NL AIC (2021). “Onderzoek McKinsey: Economische en maatschappelijke kansen van AI voor Nederland”. 2020. URL: https://nlaic.com/nieuws/onderzoek-mckinsey-economische-en-maatschappelijke-kansen-van-ai-voor-nederland/

[18] MMC Ventures (2019). “The State of AI 2019: Divergence”. 2019. URL: https://www.stateofai2019.com/chapter-2-why-is-ai-important/

[19] Journal of Artificial Intelligence Research (2018). “Viewpoint: When will AI exceed human performance? Evidence from AI experts”. 2018. URL: https://www.google.com/l?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwio1vqrmYXvAhXLnKQKHcFEAYUQFjAOegQIGRAD&url=https%3A%2F%2Fjair.org%2Findex.php%2Fjair%2Farticle%2Fdownload%2F11222%2F26431%2F&usg=AOvVaw2iuG9X62R9MrKjfnPt3UwH

[20] EU OPEN DEI Initiative. “Design Principles for data spaces – Position Paper”. Version 1.0. April 2021, https://design-principles-for-data-spaces.org/.

[21] TNO (2021). “Federated learning: maak kennis met privacybestendige data analyse”. 2021. URL: https://www.tno.nl/nl/aandachtsgebieden/informatie-communicatie-technologie/roadmaps/data-sharing/federated-learning/

[22] TNO (2021). “Secure Multi-Party Computation: gezamenlijk gevoelige data analyseren zonder deze te delen”. 2021. URL: https://www.tno.nl/nl/aandachtsgebieden/informatie-communicatie-technologie/roadmaps/data-sharing/secure-multi-party-computation/

[23] MIT Technology Review. “The global AI agenda: Promise, reality, and a future of data sharing”. URL: https://mittrinsights.s3.amazonaws.com/AIagenda2020/GlobalAIagenda.pdf.

[24] European Parliament & Council of the European Union. (2016). “General Data Protection Regulation”. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[25] 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.

[26] Richter, H., Slowinski, P.R. 2019. “The data sharing Economy: On the Emergence of New Intermediaries”. IIC 50, 4–29 (2019). https://doi.org/10.1007/s40319-018-00777-7.

[27] European Union (2017). “New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations”. URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

[28] Deutsches Institut für Normung (2019). “DIN SPEC 27070: ‘Reference Architecture for a Security Gateway for Sharing Industry Data and Services”. URL: https://www.beuth.de/de/technische-regel/din-spec-27070/319111044.

[29] Zhang, L. Cushing, R., Gommans, L., de Laat, C., and Grosso P. 2019. “Modelling of Collaboration Archetypes in Digital Market Places,” IEEE Access, Volume 7, pp. 102689 - 102700, July 2019.

[30] Otto, B., Steinbuss, S., Teuscher, A., and Lohmann, S., IDSA (2019). “International data spaces: Reference Architecture Model Version 3,” International data spaces Association – IDSA, URL: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf.

[31] Bastiaansen, H., Kollenstart, M., Dalmolen, S. and van Engers, T. (2020). “User-Centric Network-Model for Data Control with Interoperable Legal data sharing Artefacts - Improved Data Sovereignty, Trust and Security for Enhanced Adoption in Interorganisational and Supply Chain IS Applications”. Proceedings of the Twenty-Fourth Pacific Asia Conference on Information Systems, Dubai, UAE, June 2020. URL: https://aisel.aisnet.org/pacis2020/172/.

[32] OASIS 2013, ”eXtensible Access Control Markup Language (XACML) Version 3.0”, OASIS Standard. 2013. URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[33] World Wide Web Consortium (W3C), ”ODRL Information Model 2.2”, W3C Recommendation. 2018. URL: https://www.w3.org/TR/odrl-model/.

[34] World Wide Web Consortium (W3C), ”Vocabulary & Expression 2.2”, W3C Recommendation. 2018. URL: https://www.w3.org/TR/odrl-vocab/.

[35] data sharing Coalition (2021). “data sharing Canvas - A stepping stone towards cross-domain data sharing at scale”. URL: https://datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf.

Colofon

This document is a result of the work being done in the NL AIC data sharing working group. It builds further upon the previous results of the working group, i.e. the report on identifying the specific challenges for data sharing for advanced data analytics and overview of technologies and architectures that can be used in addressing these challenges [3] [4], the description of the development process from first-time engineering towards operationalisation [5] and the GAP-analysis on the three data sharing proofs-of-concept in 2020 [6].

Authors INNOPAY

Christian van Ramshorst
Vincent Jansen
Leon Kluiters
Eefje van der Harst

Authors TNO

Harrie Bastiaansen
Joost Adriaanse
Frans van Ette
Gjalt Loots

The authors would like to thank the Advisory Board members of the data sharing working group for their valuable feed-back and input.

Contact:

The Netherlands AI Coalition
E-mail — info@nlaic.com
Website — nlaic.com

November 2021