D06.04 Personal Data Spaces - Workshop 1 - Report

Introduction

In early 2020, the European Commission announced the intention of creating a single digital market within the EU to ensure European competitiveness while preserving data sovereignty. To ensure that more and better data becomes available and accessible under the control of those that hold rights over them, the European Commission shared a vision towards the creation of common European data spaces in strategic sectors and domains[1]. *"A common European data space brings together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing"*[2].

Across sector-specific data spaces, horizontal interoperability needs arise, especially in the context of management of personal data. Also for this context, the Data Governance Act[3] introduced the notion of data intermediation services. This concept acts as a steppingstone towards a paradigm shift of personal data spaces that promise individuals "tools and means to decide at a granular level about what is done with their data" (Data strategy, p. 20[4]).

To help European public administrations align with the EU data strategy and perform 'seamless and meaningful' cross-border and cross-domain data exchanges, the SEMIC Action (DIGIT.B4) and the Joint Research Centre (JRC) has begun a series of workshops on the interoperability challenges for personal data spaces.

The available protocols, specifications, and software catering for this paradigm shift are still maturing and this results in a dynamic but scattered landscape. There exist start-ups and SMEs currently on the market – some of which have been active for almost a decade (e.g., Meeco, CozyCloud) – each with their specific technology stack and off-the-shelf products which are relevant for personal data spaces. Companies such as 1001 Lakes also play a role in the implementation of personal data spaces by addressing data spaces from a governance perspective. The publication of the Solid specification[5] (Work in progress, version 0.9.0, 2021-12-17) and its potential uptake as a W3C standard has been leading to the creation of a series of new companies, such as Inrupt, which offer products and services that rely on this specification. Also, large enterprises are supporting the implementation of personal data spaces. For instance, Microsoft and Philips, which have partnered with the local government of the region of Flanders

---

[1] European Commission's Communication on a European strategy for data. Last accessed on 14/02/2023 and available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[2] European Commission's Staff Working Document on Common European Data Spaces. Last accessed on 14/02/2023 and available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

[3] Data Governance Act. Last accessed on 17/02/2023 and available at: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

[4] European Commission's Communication on a European strategy for data. Last accessed on 17/02/2023 and available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN

[5] Solid specification. Last accessed on 17/02/2023 and available at: https://solidproject.org/TR/2021/protocol-20211217

in Belgium, are developing data vaults and wallets for Flemish citizens based on Solid beginning later in 2023.

Witnessing this complex and dynamic landscape, EU Member States expressed their concerns regarding the interoperability between various types of implementations during the SEMIC2021 conference. This concern triggered the joint effort of the SEMIC Action and the JRC, building on the expertise of MyData Global, an organisation helping people and organisations to benefit from personal data in a human-centric way, part of whose work is the promotion of MyData operators.

SEMIC and JRC will organise three workshops revolving around interoperable personal data spaces. Experts representing various stakeholders (see list in Annex 1) and policy and technical experts from the Commission have been invited to take an active role in the preparation of and contribution to the workshops and the resulting white paper. Each workshop will focus on a different aspect of personal data spaces, with the aim of boosting their sustainable development and implementation in Member States or any other organisation to enable improved interoperability.

Specifically, workshop 1 explored the policies and business challenges involved in the adoption of personal data spaces in the EU. This report represents the output of the workshop.

Workshop 2 will focus on semantic and technological interoperability of existing solutions of the different components of the technology stack for implementing personal data spaces. The envisioned output of this second workshop includes a blueprint for such a stack.

Finally, workshop 3 will co-create a 2-year roadmap, based on the outputs of the first and second workshops, for the promotion of legal, organisational, semantic, and technical interoperability that will enable and boost the successful implementation of personal data spaces in the EU.

The lessons learned and outcomes of the workshop series will be collected in a white paper which will be published in the first half of 2023.

In this report, we summarise the outcomes, key conclusions and actions arising from the different sessions of the first workshop. All supporting materials can be accessed from the event page on Joinup[6].

[6] Event page on Joinup. Last accessed on 17/02/2023 and available at: https://joinup.ec.europa.eu/collection/semic-support-centre/event/first-workshop-personal-data-spaces

Overview of the first workshop & summary of the discussions

Policy work on personal data spaces in the EU - Malte Beyer-Katzenberger (DG CNECT.G1)

The European Commission, as regulator and funder, must address the need for tools and a supportive environment to work both on open and closed data. The political goal is to empower people (as mentioned in the official communication (COM (2020) 66) about the EU data strategy[7]), and to overcome infrastructural obstacles in order to improve public engagement and coordinate data usage.

Some countries or regions, like Flanders, have taken concrete steps in implementing infrastructural solutions based on interoperable personal data spaces. As these solutions remain limited in number and scope, it is increasingly clear that implementing the vision of the EU data strategy requires further coordination before reaching its full potential.

Furthermore, it appears that terms like infrastructure, platform and services are often used interchangeably, creating confusion on what is possible or even desirable. Therefore, the technical landscape, and the roles that each actor places in it requires clarity.

In this realm, the Data Governance Act should serve as a compass, helping governmental agencies find their way in the technical landscape and the required roles. This act is primarily designed to protect individuals' data rights and, at the same time, to provide a framework that facilitates data sharing. The Data Governance Act does not give individuals additional privileges. Instead, it is intended to be complimentary with GDPR and to incentivise the implementation of technical solutions that increase its effectiveness.

The Data Spaces Support Centre (DSSC)[8] should serve as a technical basis for data governance, and the Digital Markets Act[9] (Article 6, paragraph 9) and the Data Act[10] (chapter 2) are aimed at strengthening portability rights and enabling real-time data transfer for users. The Digital Markets Act, in particular, is an important tool to ensure that individuals are able to easily access and transfer their data.

---

[7] European Commission's Communication on a European strategy for data. Last accessed on 17/02/2023 and available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[8] Data Spaces Support Centre. Last accessed on 17/02/2023 and available at: https://dssc.eu/

[9] Digital Markets Act. Last accessed on 17/02/2023 and available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[10] Data Act. Last accessed on 17/02/2023 and available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

The Commission should provide more guidance in understanding the various regulation and how they relate to each other. The European Data Innovation Board[11] can help coordinate this effort.

Finally, funded projects, such as DAPSI[12], DataVault[13], SmashHit[14], and Trust-data[15], were highlighted as potential resources for further implementation. The results of these projects can provide resources to organisations working to improve data governance and accessibility.

What are personal data spaces? - Viivi Lähteenoja (researcher, University of Helsinki, and chair of the board, MyData Global)

What makes personal data spaces distinct from “regular” data spaces is the purpose for which they exist: personal data spaces serve individual people. Personal data spaces can be seen as collaborative environments of interoperating organisations that include service providers catering specifically to individuals.

For an individual person, personal data spaces look like services such as bank accounts. A person can have one or more. They can be accessed via a mobile app. The provider is known and represents one of a number of competing organisations in the market, enabling the individual to have a choice of providers. The person should be able to change relatively easy from one provider to another. Such providers can be private or public organisations.

Because people trust differently, personal data space providers will be many, and they will need to interoperate. Service providers also need to develop workable products and services. These two requirements need to be balanced because interoperability without functionality is just as bad as functionality without interoperability.

Modularity of functionalities – with both centralised and decentralised implementations possible for each module– is key for interoperability.

To conclude, the maturity in the field of personal data spaces is increasing and it’s important to remember we’re on a joint journey towards interoperability.

[11] European Data Innovation Board. Last accessed on 17/02/2023 and available at: https://digitalhealtheurope.eu/glossary/european-data-innovation-board/
[12] DAPSI. Last accessed on 17/02/2023 and available at: https://dapsi.ngi.eu/
[13] DataVault. Last accessed on 17/02/2023 and available at: https://www.datavaults.eu/
[14] SmashHit. Last accessed on 17/02/2023 and available at: https://smashhit.eu/
[15] Trust-data. Last accessed on 17/02/2023 and available at: https://www.trusts-data.eu/

Parallel Session 1 - Björn de Vidts - Data Utility Company Flanders (Belgium)

The Data Utility Company (DUC)[16] in Flanders is working towards creating a level-playing field and generating trust in sharing personal data in B2B use cases. They have joined forces with SolidLab[17], a collection of university departments with expertise in personal data technologies. They want to bring specific sectorial use cases to the market, such as in the field of HR and health. During his presentation, Björn de Vidts presented a few examples of value streams and use cases that will be put in production in collaboration with the company Randstad Belgium[18], where users will be able to share their diploma data and make better career decisions. Furthermore, they also mentioned media and smart mobility as interesting fields for further exploration.

The DUC offers a full set of solutions and services, for which the Solid protocol[19] is a "go-to" component since "it is an open standard; it has a consent mechanism; and
it supports data portability."

Björn de Vidts explained that they build on and work with the OSLO[20] team at semantic level to ensure semantic interoperability of their solutions. The OSLO team have a unique methodology with a triple helix to manage approvals via decree, advisory committee, and working groups to ensure the legal, business, and technical control of the produced semantic models. This triple perspective is vital to establish trust.

There are also other actors in Flanders (Belgium) dealing with personal data technologies for different use cases, some of them directly involved with the DUC on concrete collaborations. This emerging ecosystem strives to create solutions for the policy objectives described in the first session.

Parallel Session 2 - Marcello Grita - Swedish Public Employment Service

The presentation of Marcello Grita focused on the need for trust when handling data with verifiable credentials being a potential solution for this challenge. He presented several use cases, such as schools that do not want to retain data longer than necessary, or international transactions of health records, in which the data holder needs to authorise the transaction. In most cases, in the EU, data sharing between parties is not easy, independently from the national/regional network they operate in. The proposal put forward by Marcello Grita includes sharing information with a

[16] Data Utility Company (DUC). Last accessed on 17/02/2023 and available at: https://www.vlaanderen.be/digitaal-vlaanderen/het-vlaams-datanutsbedrijf/the-flemish-data-utility-company
[17] SolidLab. Last accessed on 17/02/2023 and available at: https://solidlab.be/
[18] Randstad specialises in solutions in the field of flexible work and human resources services. Their services range from regular temporary staffing and permanent placement to inhouse, professionals, search & selection, outplacement and other HR Solutions.
[19] Solid Protocol. Last accessed on 17/02/2023 and available at: https://solidproject.org/TR/protocol
[20] OSLO. Last accessed on 17/02/2023 and available at: https://www.ugent.be/mict/en/research/projects/2016/oslo-open-standards-for-linked-governments

node at national level which will transfer it with the agreed communication mechanism to another node in another country. Marcello Grita informed that the Swedish Public Employment Agency already begun implementing this proof-of-consent. The development is open source and can be reused or enriched. Lastly, he mentioned there is also the need for legal support to limit or allow certain usages of data. For example, it is technically possible to prevent an actor to receive certain type of data, (e.g., health information should not be accessible by life insurance businesses). However, individuals could be instigated to deliver 'blocked' information through other channels (e.g., a subsidiary not registered as insurance). It is therefore extremely important that the technical solution is aligned with the law to prevent undesirable outcomes.

A plenary discussion on obstacles and risks followed Marcello Grita's presentation, which include:

- The lack of transparency about where data is stored, processed, and managed;
- The need to tackle business, technical and legal challenges at the same time;
- The need to create more general solutions for interoperable personal data spaces rather that use-case driven once:
    - Individuals who are using services in these spaces want an intuitive experience, bringing the different building blocks together into a coherent and seamless service.
    - Solution providers should avoid creating silos between domains by using proprietary standards.
- The need for historical access to personal data records; and
- The data sovereignty, understood here as the idea that data is subject to laws and governance structures of a country where it is collected, can act as an obstacle to the management of personal data.

Opportunities and use cases have also been discussed. These included:

- Adapting laws to better suit digital data handling and creating a legal framework for interoperability in the EU;
- Improving processes while digitising them;
- Creating machine-friendly legislation; and
- Giving access to data rather than replicating data.

By seizing these opportunities, a considerable amount of the obstacles and risks could be handled.

The discussion concluded by stating that, to be truly interoperable in the EU, it is important to start by defining ecosystem roles, increase coordination among actors and establish trust. It was also emphasised that consent and consent auditing tools are required for a Minimum Viable Product of personal data spaces to emerge.

Parallel Session 3 - Mikko Rusama - CDO City of Helsinki

The municipality of Helsinki is working to move from a reactive to a proactive service delivery and from outright exploitation to human-centric use of data. This includes anticipating citizens' needs, triggering personalised services, empowering individuals with their personal data and seeking their consent. The city is also working on a Minimum Viable Product (MVP) for a MyData operator implementation. The MVP focuses on a generic consent management solution, while ensuring compliance with data protection regulation and transparency in data processing.

In a second part of this session, participants tackled the issue of consent and trust. Ana Garcia noted that, in Finland, citizens generally trust the government. This may ease the implementation of personal data spaces, particularly when it comes to consent. On the contrary, for countries where there is a general lack of trust in the government, many European citizens would probably find it hard to give consent to something they do not understand. Mikko Rusama added that without trust it is not possible to work with data. In Finland, there is a high level of trust towards media and public authorities. To tackle trust issues, cities need a clear legal basis process personal data. They must also protect citizens including people who are not capable of protecting their own data. Participants also agreed that a human-centric approach is needed for personal data spaces to become a reality. Simple consent management is therefore a goal. External solutions, such as personal AI, were suggested. The group of participants discussed the need for a 'virtual guardian angel' as a concept in this field. It would help individuals to manage consent for personal data through a functional solution. The latter is key to enable individuals to manage many permissions. In this realm, the city of Helsinki sees an active role for other cities as well: directly as guardian angels for citizens, proposing services or to ensure the responsible and lawful use of data.

To conclude the discussion, the group stressed the importance of control and sovereignty, collective interest management, semantics of personal data spaces and the importance of trust and identity management in implementing personal data spaces. They also raised concerns about interoperability, accountability, and ethics surrounding personal AI.

Understanding the business models - Panel discussion with start-ups and SMEs

Panel discussion participants:

- Meeco[21] unlocks the power of permissioned personal data and digital assets with enterprise infrastructure, to enable people to securely access, control.

- Digita[22] is a Digitech start-up that aims at enabling people and organisations to share data without concern. To achieve their goal and mission, they identify the following problems in society:

[21] Meeco. Last accessed on 17/02/2023 and available at: https://www.meeco.me/about-meeco
[22] Digita. Last accessed on 17/02/2023 and available at: https://www.digita.ai/

    - It must be more human-centric;
    - Facilitating reuse across different data space organisations;
    - Providing trust around personal data.

- Konsolidate[23] is a Flemish start-up who co-creates, accelerates, and shapes the decentralised future together with its clients and the best-in-class Solid development and consultancy.

- Visions[24] is a data intermediary who shares data between the data source and the data users. They do not store data themselves. Through Visions and its ecosystem, one has access to innovative and individualised services thanks to a control of your data that makes you master of your destiny.

- 1001 Lakes[25] offers a rulebook by which they guide their clients with the creation of a data spaces and how to govern them.

- iGrant[26] is a consented data exchange platform that enables access to the right data for businesses while complying with regulations. It helps organisations, both private and public, to unlock the value of personal data using centralised and decentralised (Web 3.0) technologies.

Key takeaways of the panel discussion

In a panel discussion facilitated by Paul Theyskens, the panel members disclosed their vision on four topics related to personal data spaces, namely: the current business models of personal data space implementers, the interoperability challenges implementers face, the benefits of using a personal data space for public and private parties and finally the next steps a personal data space implementer should bear in mind. The discussion provided insights on the importance of business models, governance, and the need for public-private collaboration to drive innovation.

Current business models of personal data space implementers

One of the companies, Meeco, explained that we are in a cross over period between physical and digital human beings, where transparent and trust-based exchange of data is crucial for making better decisions in areas like voting, health, and supply chain management. Overall, their focus was on rewiring society from a policy, legal, and commercial point of view. For several panel members, their business models started with public funds for pilots followed by larger-scale projects. With the first services offered for different use cases, some of them have diversified their revenue sources by broadening their services for different users, becoming for instance product or service providers.

[23] Konsolidate. Last accessed on 17/02/2023 and available at: https://www.konsolidate.eu/
[24] Visions. Last accessed on 17/02/2023 and available at: https://visionspol.eu/en/
[25] 1001 Lakes. Last accessed on 17/02/2023 and available at: https://1001lakes.com/
[26] iGrant. Last accessed on 17/02/2023 and available at: https://igrant.io/

Interoperability challenges

There are already concrete applications released in the market which are technically robust. To scale it up, organisations and individuals face several challenges. Firstly, they must make the shift to the new paradigm. Secondly, sharing data does not start overnight. To work, it requires common semantic understanding, supporting technologies, policy and legal frameworks, etc.

Thirdly, Meeco acknowledged the importance of standards, but also pointed out that there are already many existing foundational standards in areas such as security and APIs. Standards are necessary but not sufficient. When it comes to data intermediaries, Visions emphasized the importance of allowing different data intermediaries to interoperate, creating networks that can be scaled. Such interoperability networks will be based on standards but extended to face the concrete challenges of any implementation. Only then, by federating and aligning a critical number of parties involved, a fair market will emerge where individuals will be free to move from one intermediary to another, without a new level of lock-in. Finally, a last important challenge raised concerned the governance.

Benefits for public and private actors

When asked for a concrete and measurable benefit for the end-user, Digita explained that they were digitising the entire procedure for a Dutch company, which would provide a better user experience for the end-users of notaries, for which the notaries were ready to pay for.

Next steps for personal data space implementers

A key aspect in this journey is to incentivise both public and private organisations to get started with personal data spaces. Therefore, the priority is to demonstrate the value of personal data being (re-used) by individuals themselves to motivate organisations to make extra efforts towards personal data spaces. To achieve this, 1001 Lakes highlighted the importance of listening to customers. He also suggested that a rulebook thinking could improve the collaboration on the level of data spaces, including personal data spaces. In addition, better individual control of personal data requires interoperable intermediaries. Lastly, public and private organisations should collaborate more: there are various ways, from creating the right environment for private organisations to innovate, to publicly led or funded initiatives and public-private partnerships but, in the end, what matters is the willingness to start this collaborative journey.

Wrap-up by Seth Van Hooland

Seth Van Hooland discussed the evolution of business models in the field, from consultancy towards products. 1001 Lakes is transitioning from consultancy to a standardised product. Digita inquired about funding possibilities and mentioned that today it is often provided by the Commission or other public funding sources. The European Commission is interested in learning from innovators and small companies to boost innovation and create data space solutions.

Key findings

Personal data spaces are the European way to implement human-centric values regarding personal data. One way to answer the question “What are personal data spaces?” was circulated prior to the workshop via the so-called ”Provocation paper”. This text has been iterated based on the workshop and included in this report as a proposed description of personal data spaces in Appendix 2.

The first workshop was an energising event with lively and wide-ranging discussions. The various obstacles, opportunities and needs identified during the sessions were derived below into a structured list of key questions. This list represents the questions, identified by the participants of the first workshop, which need to be answered to support the sustainable emergence of the personal data spaces.

Overall questions:

- **Why?** We need define the rationale for why we want to build personal data spaces;
- **What?** We need to clarify the current sea of partly overlapping and interrelated technologies we all use;
- **How?** We need to take a sufficiently holistic approach across different business, legal, technological, societal, and other viewpoints and remain focused enough to make progress;
- **Who?** We need to define who is (going to be) paying for personal data spaces.

A preview of specific questions to be tackled in the context of the second workshop (subject to further refinement and addition):

- How will **identification** be ensured by personal data spaces in an interoperable way, reusing solutions that exist already?
- How will personal data spaces handle **access control** (permissions like, but not limited to, consent) in an interoperable way?
- How do we **model** data in an interoperable way, across sectors and spaces?
- How do we **log and monitor** the data exchanges and usages?

Further highlighted questions:

Definition	• What is the appropriate mechanism to establish a legally coherent definition of a personal data space? • How does the (within itself sometimes contradictory) legal language on roles and actors map onto a) practice and b) existing frameworks?
Values	• How do we incorporate European values into implementations of personal data spaces? • How do we move beyond the organisation-centric focus, looking into internal optimisation and siloed problem-resolution, to a

	collaborative approach, considering the entire ecosystem and based on shared principles, protocols and data modelling methodologies that would benefit multiple stakeholders at the same time?
Coordination	• How do we coordinate and align the different efforts in this field? • What is the role of the different tools and mechanisms of rulebooks in governing personal data spaces?
Business models	• What are the different business models currently used by companies in this field?
Interoperability	• How do we incorporate and build on the (semantic) interoperability frameworks developed for “generic” data spaces? • How do we ensure that we promote “true” interoperability and not “just” integration(s)? • Is technology really a trivial question in this field? That is, are the hardest questions for (interoperable) personal data spaces elsewhere? • How do we implement the principle of modularity on the level of infrastructure (services)?
Consent	• From a policy perspective, how do we handle delegating (some aspects of) consent to representatives or proxies: collectives or other non-for-profit organisations or software like “guardian angel” tech and personal AI assistants?
Data	• What is the role of synthetic personal data in the practical development and deployment of personal data spaces?
Member States	• What should a Member State consider when implementing a personal data space?

Next steps

Following up on the main outcomes from this first workshop, the next steps towards interoperable personal data spaces include:

1. **A second workshop, to be held on 1 March 2023 in Ispra, Italy, and which will be a technical deep dive into the interoperability of MyData operators and Solid implementations.** The workshop will focus on getting hands-on with technical interoperability between various types of personal data implementations and to learn about participants' approaches to and their experience with interoperability. The objective of this second workshop is to identify how existing and potentially new personal data space technologies can ensure semantic and technical interoperability by working hands-on on a use case. The aim of the use case is to identify the key building blocks which will show how personal data space technologies can be used to create an architecture that is conformant to MyData principles. These building blocks will include Identity, Data Modelling, Service Management, Access Control, Governance and Logging.

2. **The third and (for now) final workshop on personal data spaces will take place in Ghent, Belgium, and focus on the co-creation of a vision on what personal data space providers will bring to Member States for the next two years.** The goal is to draft a roadmap up until 2025 on some of the questions raised above for the advancement of EU-wide interoperable personal data spaces in the coming years. A more detailed scope and agenda will be disclosed later.

3. **A white paper will be published to describe the state-of-play of personal data spaces and related interoperability challenges as** the key outcome of this workshop series.

Appendix 1 – Contributors to the workshop series organisation

Contributors

- Viivi Lähteenoja (University of Helsinki, MyData Global)
- Max Leonard (Inrupt)
- Emmet Townsend (Inrupt)
- Joss Langford (Coelition)
- Paul Theyskens (MaaS Alliance, MyData Global)
- Esther De Loof (SolidLab)
- Marcello Grita (Swedish Public Employment Service, JobTech)
- Florian Barthélemy (PwC Belgium)
- Catarina Arnaut (PwC Belgium)
- Arne Van Der Stuyft (PwC Belgium)
- William Verbeeck (PwC Belgium)

Consulted

- Katryna Dow (Meeco)
- Benjamin André (CozyCloud)

Appendix 2 – What are personal data spaces? A description

Personal data is simultaneously essential for delivering on the promise of data spaces and at the heart of the most nightmarish scenarios to which increased accessibility and processing of data can lead. Any work in data spaces cannot afford to ignore the personal nature of at least some of the data that these spaces deal with or the normative implications thereof. In other words, personal data has a special role when discussing questions of (semantic and other kinds of) interoperability of data spaces.

In view of addressing the needs for available personal data for the benefit of individuals, companies, and societies, and/or mitigating the potential harms stemming from personal data processing, a constellation of similar ideas has emerged over at least the past decade and a half. Variously termed ideas around giving individuals better control over personal data availability and processing, or solutions for "human-centric data management", have been described, developed, or promoted by several people and organisations from at least the "infomediaries" of the last century.

In February of 2020, the European Commission published a communication entitled "A European strategy for data", which highlighted the EU's ambition for increased technological sovereignty both for the bloc as a whole and for its citizens. A centrepiece of this strategy was the adoption of the concept of "data space", which had been promoted for some years by organisations like International Data Spaces Association.

In addition to announcing the creation of nine sectoral data spaces such as the "health data space", the strategy document also introduced the concept of "personal data spaces". They are included with the explicit motivation to support individuals "to be empowered to be in control of their data through tools and means to decide at a granular level about what is done with their data". This motivation, as well as explicit references to the MyData movement and "consent management tools, personal information management apps, … as well as personal data cooperatives or trusts acting as novel neutral intermediaries in the personal data economy", place the strategy document firmly in the tradition of what was referred to as "human-centric data management" above.

While the basic idea of empowering individuals regarding personal data is not new, public sector focus and efforts for realising these "human-centric data management" ideas have only seen limited uptake in the EU in the past. With the prominent promotion of these ideas and the introduction of the concept of "personal data spaces" in the EU data strategy, this is beginning to change.

However, significant conceptual, and practical confusions persist about the specific term "personal data space", exactly how it is related to the similar, preceding ideas of "human-centric data management", and precisely how one is implemented.
This short paper presents a working description of what "personal data spaces" are. The concept is considered through several distinct but overlapping perspectives and the description here

presented considers the following aspects: 1) definitions found in EU legal and policy documents, 2) conceptual features, 3) design and implementation features, both of which are, and finally 4) what personal data spaces look like from the points of view of organisations and individuals.

Legal and policy descriptions of personal data spaces

The purpose of personal data spaces is for individuals to "be empowered to be in control of their data" . They are "tools and means to decide at a granular level about what is done with their data". (Data strategy, p. 20.)

Personal data spaces enable people to reuse, share, and enable the joint use of data. Through, for example, data intermediation service providers, personal data spaces facilitate individuals "exercising the rights of data subjects in relation to personal data" (DGA, art 2(11).)
Personal data spaces can be described in the language of sectoral data spaces as purpose-specific (but only in that their purpose is to empower individuals), cross-sectoral or horizontal, and "interoperable frameworks of common standards and practices", (DGA, Recital 27).

Conceptual features of personal data spaces

The phrase "personal data space" should be read as "data space for a person" and not as a "data space for personal data". In other words, personal data spaces are data spaces that are particular to an individual (as opposed to being specific to a domain or industry vertical like health, mobility, public administration, etc.). This conceptualisation is in line with the basic tenets of human-centricity, namely that the focus is on the person (and not the data).

Because personal data spaces are always specific to individuals, one individual may have more than one personal data space, but one personal data space can only be controlled (directly or through an authorised representative) by one individual.

Personal data spaces, like sectoral data spaces, can be described as collaboration environments with models of interoperating between organisations. Organisations collaborating in the context of data spaces will each fulfil one or more roles in the architecture of the data spaces. In addition to other roles, all data spaces will always include roles, and actors fulfilling these roles, that provide infrastructure services and those that provide end-user services.

In this vein, personal data spaces can also be described as that end-user service layer which caters specifically to individuals (as opposed to companies and other organisations), and which operates on top of the infrastructure layer provided (at least in part) by sectoral data spaces like health, mobility, public administration, and so on.

Multiple natural and/or legal persons can and most often do hold different kinds of rights over the same personal data. The same data can be relevant for two or more individuals (for example, the energy consumption of a household of two or more people) or for individuals and organisations (for example, the location data generated by ride-sharing service use). As a result, the data

controllable by an individual via personal a data space can be, and usually will be, also in some way controllable or processable via one or more personal and/or sectoral data spaces according to the rights (and restrictions) relevant for the natural and legal persons involved.

Collective personal data spaces are also conceptually possible for formal and informal groups and communities. Collective data governance such as would be required for collective personal data spaces have been explored especially by and in the context of indigenous peoples and in connection with variously defined collectivist concepts like data trusts, commons, cooperatives. However, individualist models continue to dominate in the EU and collective personal data governance remains at present underexplored especially outside research institutions.

Features of personal data space design and implementations

Because they are always specific to an individual, personal data spaces can be described as always being *human-centric* and *decentralised* in the specific sense that control over personal data is situated with each individual.

Personal data spaces can be implemented in a variety of ways which need to be *interoperable*. Interoperability is necessary for these varieties of implementations to be functional collectively, in a way that serves their purpose of empowering individuals, and in a way that does not lead to unwanted (market) phenomena and vendor lock-in effects.

This requirement of interoperability, in turn, strongly recommends *modularity* in the design of personal data spaces. Modular design must allow for both centralised and decentralised implementations for specific elements.

A definition, not the only nor an entirely uncontroversial one, of the *necessary* and *optional* elements that make up the functional stack of personal data spaces is included next.

Personal data spaces will always include the following core functionalities:

- Identity management,
- Permissions management (access control),
- Activity logging & support for auditing,
- Interfaces for individuals,
- Interface for data sources,
- Interface for data using services,
- Cybersecurity.

Personal data space offerings may or may not include additional functionalities such as:

- Data storage or hosting,
- Data transfer,
- Data source or using service discovery,
- Value exchange,
- Data model management,

- Identity wallet (storage for attributes, claims, etc.)
- Data visualisation.

Implementations of these functionalities are interoperable within their categories and these functionalities may also be provided as add-on services independently of a core personal data space service.

Organisational and individual perspectives on personal data spaces

An organisation providing personal data space services to individuals will need to provide (independently or in conjunction with partners) at least: Customer interface and UX for individuals; Legal compliance and means for lawful operations for the regulator; Technical capacity for the core functionalities and possible additional services.

For the individual, a personal data space can appear as an app they use on their device, through a browser log-in, or through other services where they see who is using what data about themselves and for what purpose. They can add data sources like online services they use. They can also accept incoming requests by services or products to access and use data from the data sources added.