

Data exchanges, data marketplaces and data intermediaries

An ethical approach to maximising the business use of personal data

David Goodman
iGrant.io Communications
7 October 2022



The burning business problems

Data exchanges benefit:

Organisations:

- 1 • sharing or exchanging verified personal and non-personal data with other organisations
• carrying out machine learning analyses on large data sets aggregated from multiple data sources
• establishing trust relationships with their sources of personal data
- 2 Businesses and individuals seeking to share data in compliance with both ethical/social norms and data-related regulations
- 3 Companies impacted by market and regulatory data sharing trends



Why this is worth knowing

- ① A confluence of new data-related regulations and fast emerging market trends point to next generation data exchanges and individual digital wallets
- ② A **data exchange platform** should be a scalable, zero integration, automated governance data intermediary solution ideally with a dApp/data wallet SDK that enables organisations to share verified personal and non-personal data aggregated from multiple sources with other organisations
- ③ A **data exchange** empowers both businesses and individuals to share data in compliance with both ethical/social norms and data-related regulations



Content

Why now

Introducing data exchanges

Data exchange transactions and agreements

Summary



Why now



Data is **not** oil - it is a renewable resource that can be pooled, shared, reused ... we want to enable businesses to make the most of data - while securing that we can trust that we are protected from misuse

Margrethe Vestager

Executive Vice-President European Commission

6 May 2021



Why now – the data sharing problem today

The process of personalising a service requiring even the most basic data set may not have either access to the relevant data or the requisite user consent – or both – and there are data elements that have to be obtained from a multiplicity of sources.

Most companies either:

- **collect data from their customers** or employees, which is then stored within the business; and/or
- **buy data from aggregators** with no involvement of the individuals whose data is being traded.

Neither situation is satisfactory and from a socio-economic, data economy and legal perspectives this process can be considered as broken.



Why now – regulatory imperatives

The [Data Governance Act](#) is the first of a set of measures announced in the 2020 [European Strategy for Data](#) and aims to create a framework with which to facilitate data sharing.

- The Data Governance Act covers the data of public bodies, private companies and citizens.
- Its main aims are to safely enable the sharing of sensitive data held by public bodies and to regulate data sharing by private actors.



Why now – data intermediaries

Although not mentioned explicitly, the [Data Governance Act](#) assumes the role of [data intermediaries](#) in facilitating data sharing

Data intermediaries:

- are the brokers in any data exchange between an organisation and an individual or between two or more organisations wishing to exchange data
- should not store any data and thereby maintain a separation between data storing sources
- are responsible for the safekeeping of the signed [data agreements](#) between all the parties involved in a data exchange transaction



Why now – regulatory imperatives

The 'eIDAS 2.0' proposal aims to provide, for cross-border use:

- access to highly secure and trustworthy electronic identity solutions
- trusted and secure digital identity solutions that public and private services can rely on
- digital identity solutions that natural and legal persons are empowered to use
- these solutions linked to a variety of attributes that allow for the targeted sharing of identity data limited to the needs of the specific service requested,
- acceptance of qualified trust services in the EU and equal conditions for their provision.



Why now – data wallets

The **eIDAS 2.0** proposal offers to any EU citizen the opportunity to obtain a digital identity wallet from a range of providers that can be used in any public or private transaction and that can be populated securely with verifiable attributes from multiple sources



Why now – GDPR and consent

Consent is a voluntary declaration of intent, which a person is free to withdraw at any time.

For **individuals**

- **Consent** should be freely given, informed and unambiguous
- Can opt-out anytime

For **organisations**

- **Consent is specific**: the provisions of consent are clearly distinguishable from terms and conditions
- **Demonstrating consent** is a responsibility of the data controller
- **Withdrawal of consent** should be as straightforward as granting of consent
- **Consent may not be conditional** on unnecessary processing: consent is tied to a usage purpose that the data subject can opt out of



Why now – other relevant instruments

The Data Act

The AI Act

The Cybersecurity Act

NIS Directive 2.0

The European Health Data Space



Why now – the drivers of consent

Data regulation

- GDPR Article 4 - 23
- Article 4: Definitions
- Article 6(1): Lawfulness of processing
- Article 7: Conditions for consents

Social and ethical norms

- MyData
- FAIR data principles

Standards and architectures

- Kantara Consent Receipt Specification v1.1
- ISO/IEC 29184: 2020: Information Technology - Online Privacy Notices and Consent
- ISO/IEC TS 27560: Privacy technologies - Consent record information structure
- Data model, lifecycle, schema and common vocabulary (DIF, ISO 27560, Kantara, W3C)



Why now – market trends

Post-pandemic, the world is awakening to new levels of awareness about the digital world and personal freedoms

- For companies and individuals, COVID-19 restrictions highlighted core **digital dependencies** and accelerated the pace of **digital transformation**
- **Data marketplaces** are emerging in different locations and industry sectors just as GDPR-like regulations are being adopted across multiple domains
- Access to more highly reliable, **quality data** is a requisite to offering new types of personalised services as well as building new AI-driven digital actionable insights
- The backlash against **corporate misuse of data** provides forward-looking businesses a great opening to differentiate their offerings and gain a competitive advantage



A new wave of human-centric data management is being promoted aligned with the behavioural shift of businesses and individuals

Data exchange platforms are trust-based solutions to the problem of business use of personal and sensitive data, enabling businesses to navigate the regulatory landscape with confidence while providing new highly valuable personalised services to their customers, based on existing and new technologies



Introducing data exchanges



The trusted data exchange

A **data exchange** provides access to as many data points as are needed to complete a data-oriented task or to fulfil a customer interaction or transaction.

The benefits that **data exchanges** bring are in structuring, aggregating, and governing data that is shared through them by **consent** and subject to **legally-binding agreements** providing businesses with a greater degree of control as well as confidence than they have today.

A **trusted data exchange** is secure, privacy-centric, regulatory compliant and auditable: this is the differentiator from other data exchanges.



A data exchange platform

A data exchange platform:

- enables data to be **legally shared** between different organisations, reducing the risk of non-compliance to data protection regulations
- **automates data agreements** with individuals on the use of their data
- **empowers businesses** to engage with their customers in real time
- provides **access to data sources** outside companies to drive marketing activities and analytics based on tamper-proof data

A **trusted data exchange platform** is a **data intermediary** according to the Data Governance Act with GDPR compliance and enables **large data sets** through attribute aggregation from **multiple data sources** for more accurate **machine learning** analysis



Enabling new business opportunities

A data exchange platform enables companies to:

- Gain access to better quality data through a data marketplace with the freedom to use personal data for a range of marketing and analytical purposes
- Demonstrate regulatory compliant data use with auditable data agreements

- Use personal data to power customer engagement

For example:

- In marketing campaigns, using complex data-oriented activities without fear of breaking the law or compromising the trust of customers, suppliers or employees.

In short, access to business-essential data at low risk



Benefits and value for all stakeholders

Organisations

- **Operational efficiency** – zero code integration for all parties
- **Better care** – through access to high quality, verified and relevant data
- **Lawful processing of sensitive personal data** – through consent or data agreement

Individuals

- **Control of one's own data** – one-stop-shop data aggregation based on consents and permissions
- **Means to share data in real-time** – digital sharing of personal data for advanced personalised health-care or self-care. Data can also be “donated”

Ecosystem and society

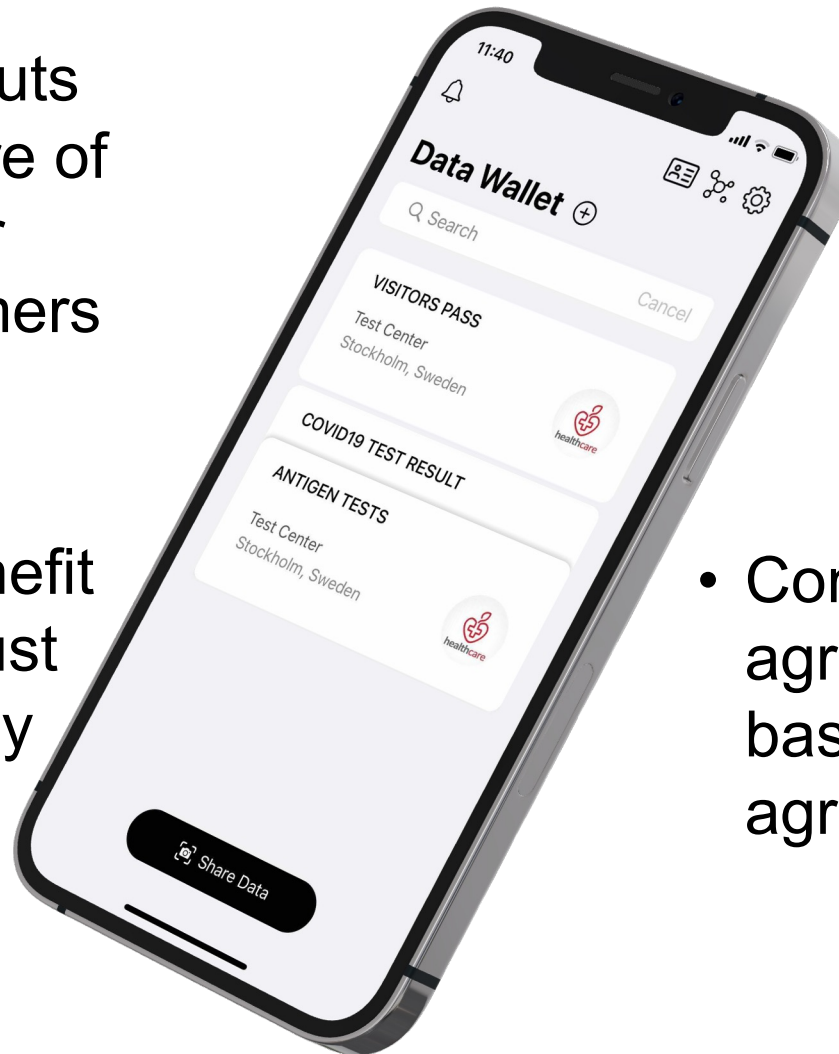
- **New services and innovation** – based on consented data exchange within an interoperable ecosystem
- **Means for actionable insights** – based on data re-use in the event of a pandemic or emergency
- **Sustainable ecosystem** – through the lawful reuse of data



Connect. Consent. Share.

A **data exchange platform** puts customer consent at the core of a company data strategy for companies and their customers to share data

As a result of transparent interactions, companies benefit from increased customer trust and loyalty which in turn may grant access to greater volumes of personal data



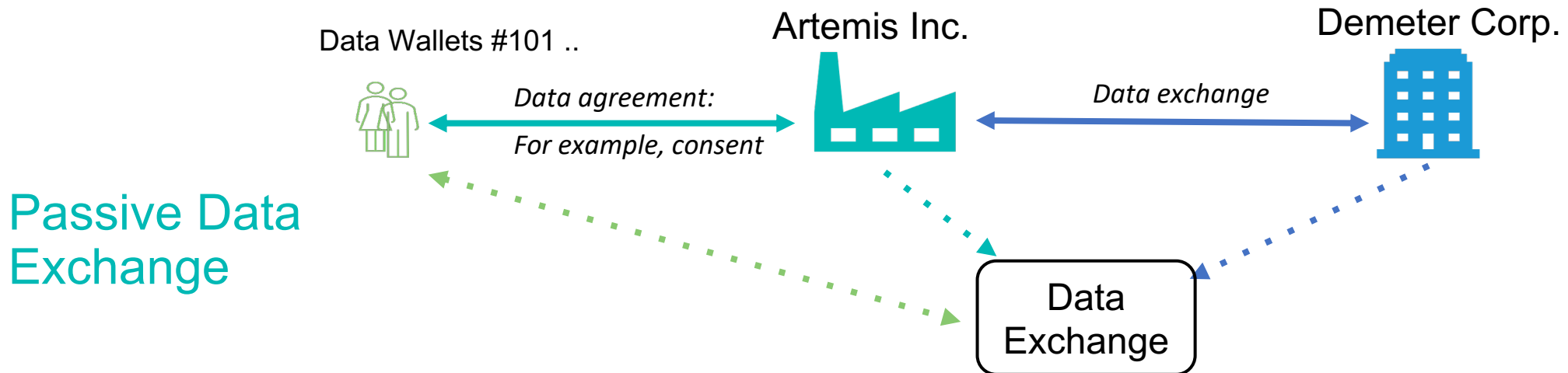
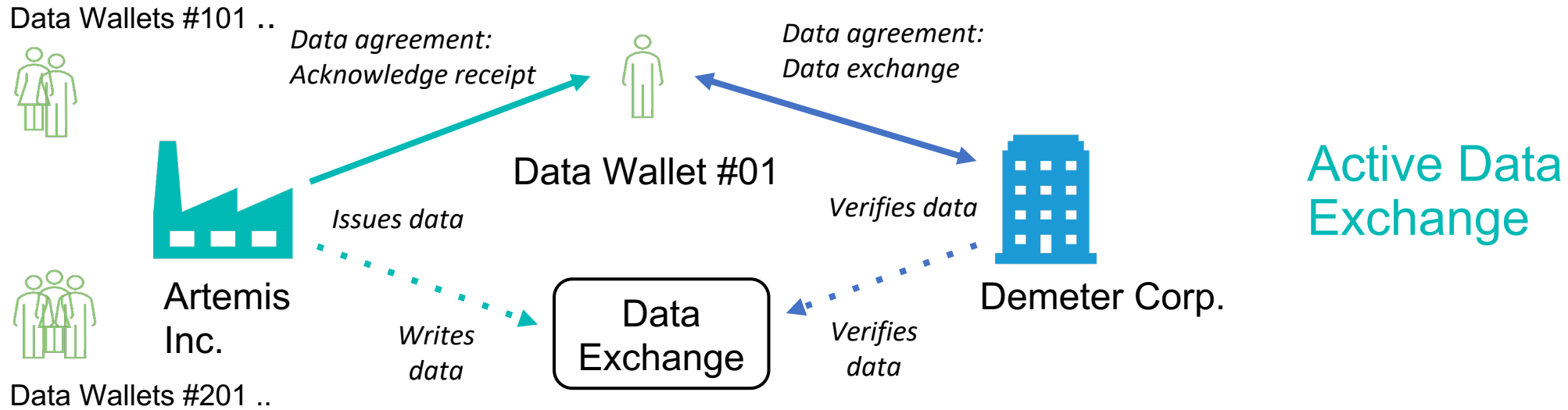
- Through a **mobile data wallet app**, users can make consent and preference decisions about how their data is used
- Companies can make agreements to share data based on existing data agreements with users



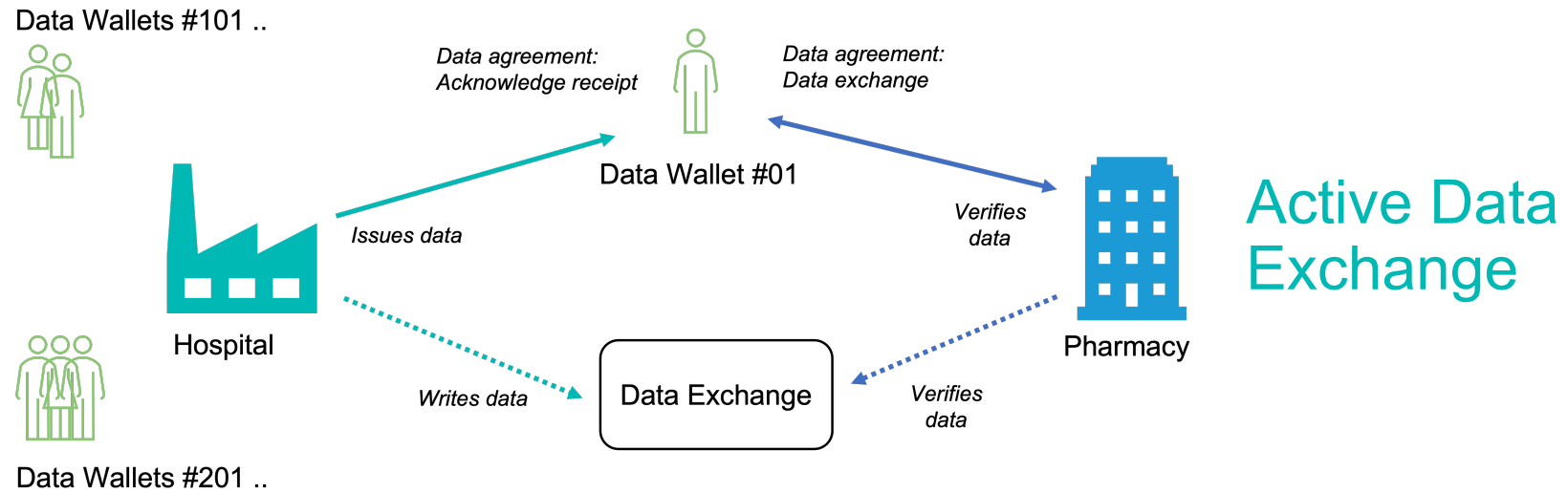
Data exchange transactions and agreements



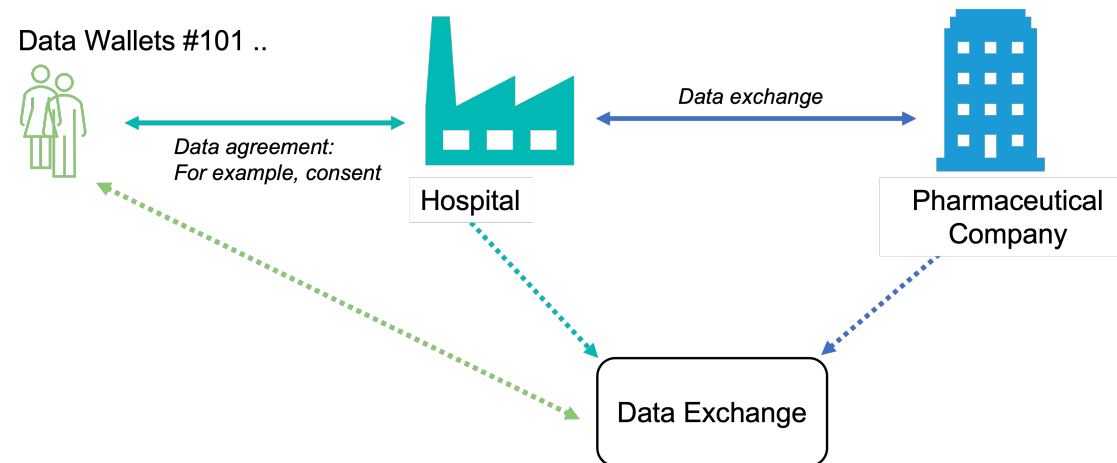
Data exchange transactions



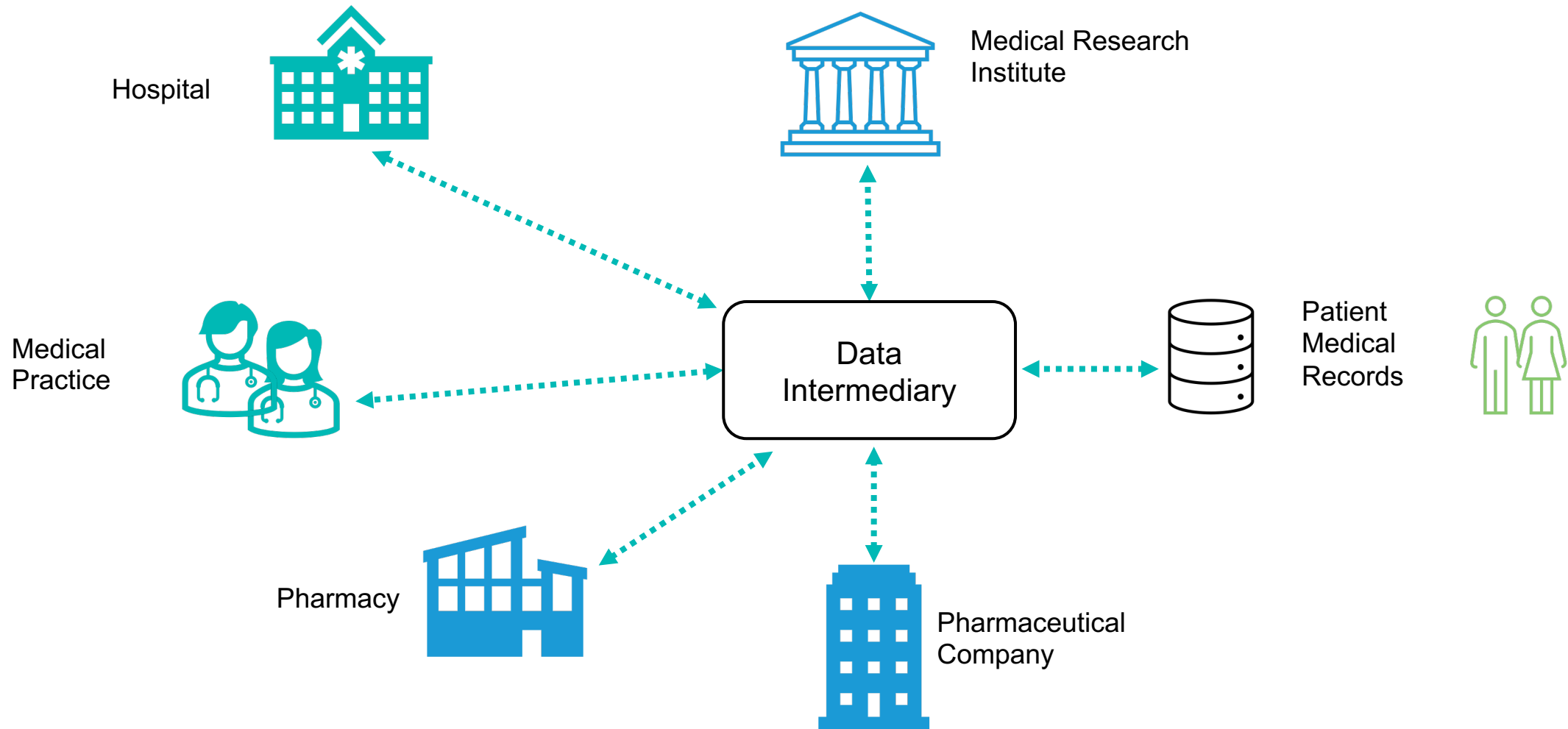
Medical data exchange examples



Passive Data Exchange



A medical data intermediary example

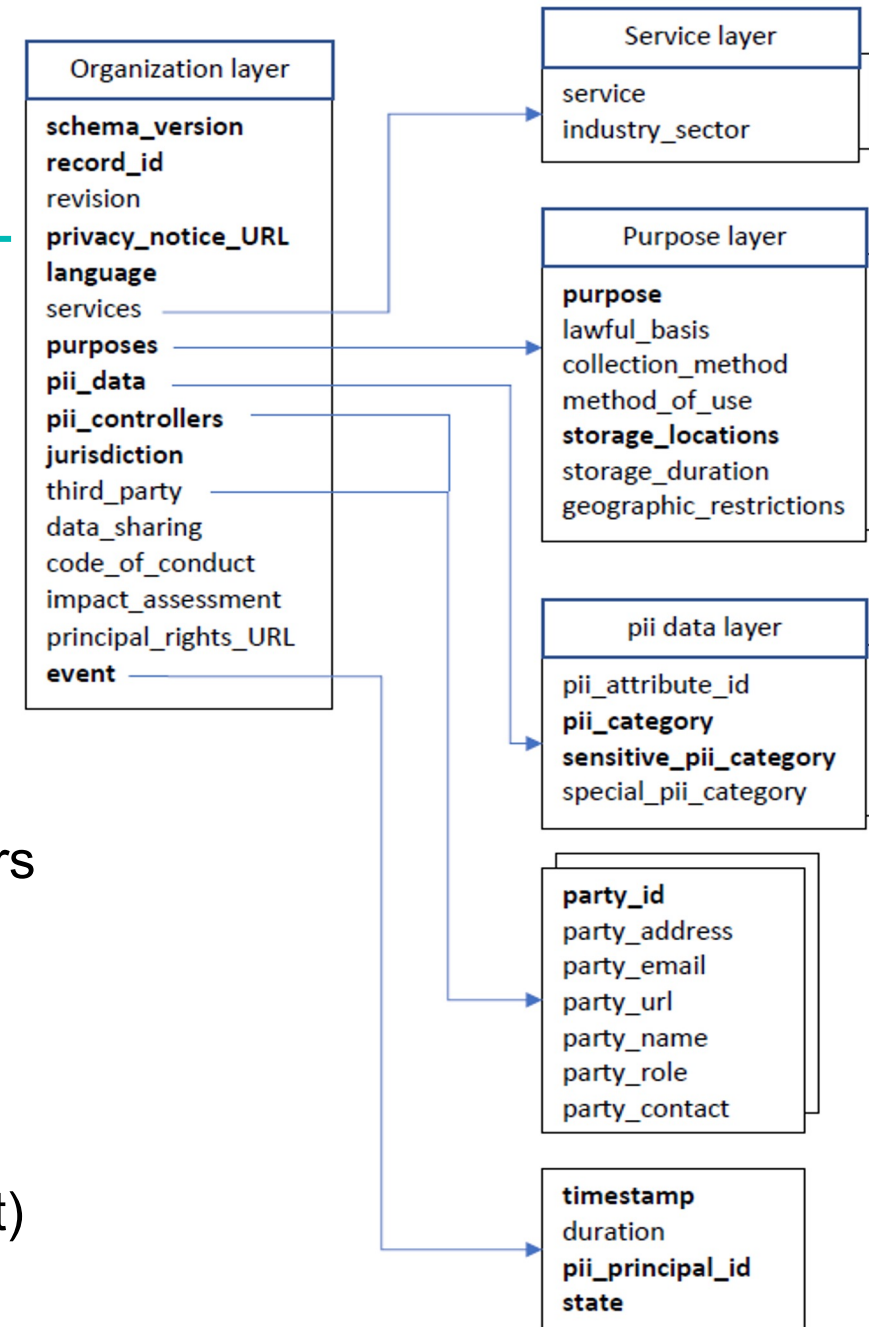


What is a data agreement

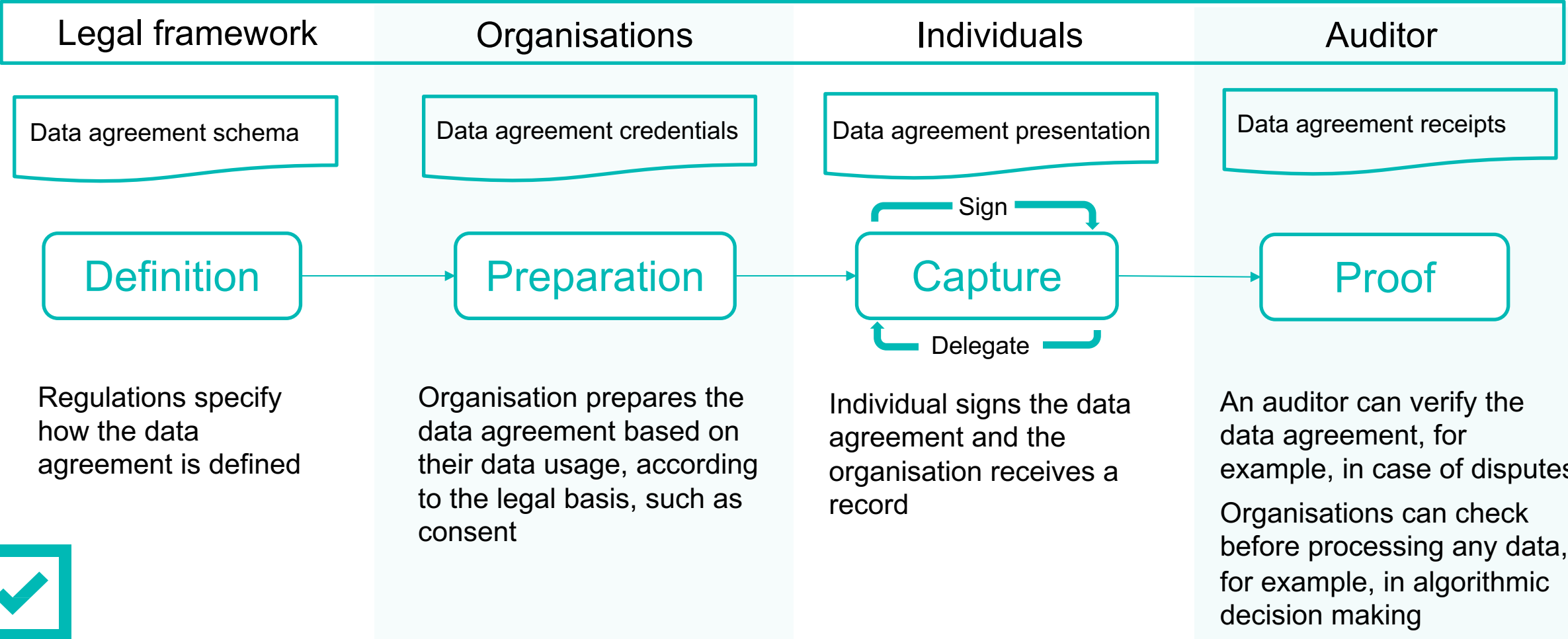
A **data agreement** records the conditions for an organisation to process personal data in accordance with data regulations (e.g. GDPR).

The characteristics of a data agreement are:

- Associated with any personal data usage including data sharing
- Could be of any legal basis: for example, consent or others defined by the law
- Could be formulated as a results of a DPIA (data protection impact assessment) that ensures data compliance
- Standardisation via ISO SC27 WG5: 27560 (working draft)



Data agreement lifecycle



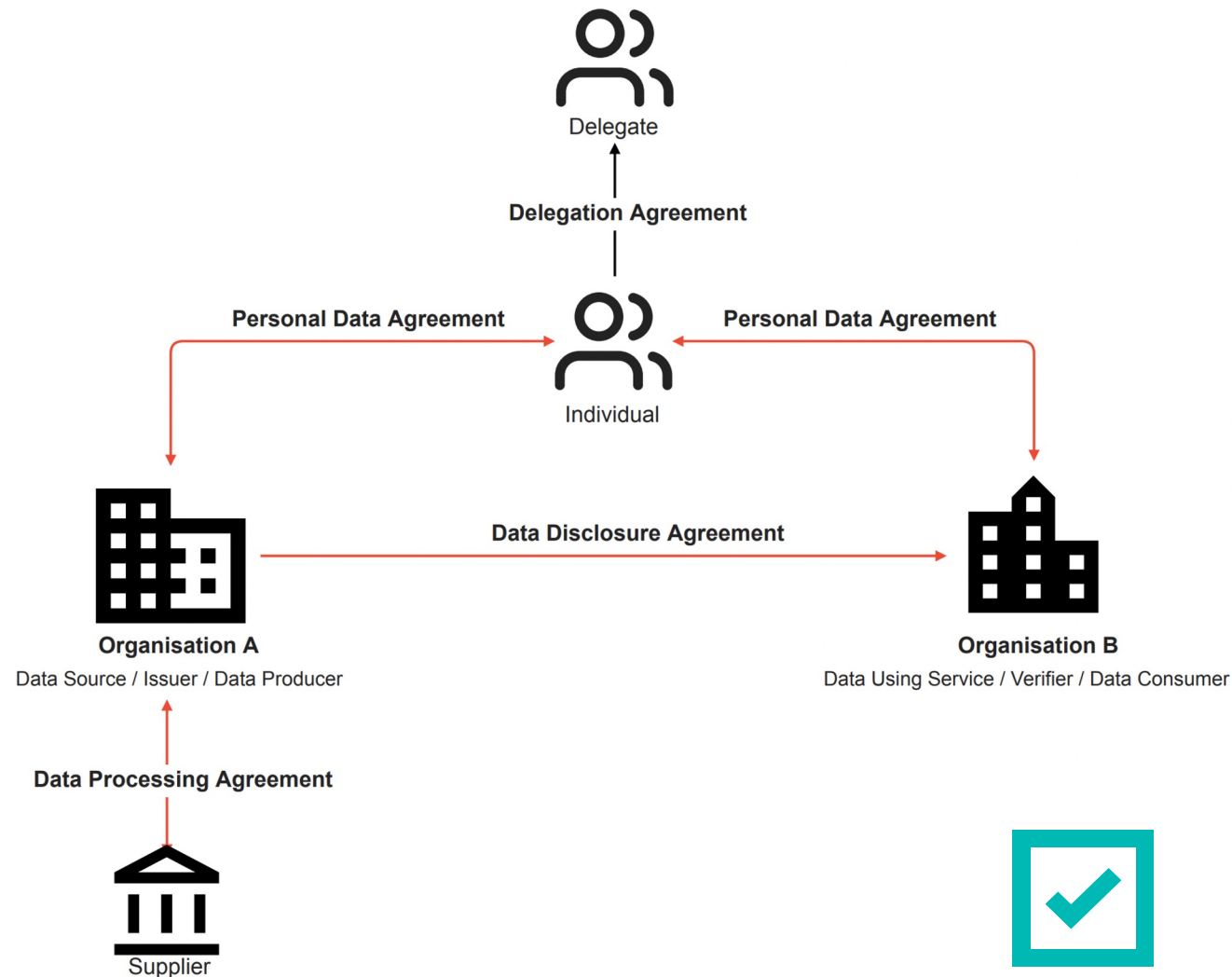
Data exchange agreements

Lawful data usage secured through data exchange agreements based on a data protection impact assessment (DPIA)

- Personal Data Agreement
- Data Disclosure Agreement
- Data Processing Agreement
- Delegation Agreement

Open sourced (Apache 2.0) via NGI-Trust specifications

Service endpoints as RESTful APIs



Data exchange agreements

Personal data agreements exist between *organisations* and *individuals* in the use of personal data and can have any legal basis according to any data protection regulation.

Data Processing Agreements are legally binding contracts in the context of any data protection regulation, either in written or electronic form, entered into between *data processors* and *data controllers* that state the rights and obligations of each party concerning the protection of personal data.

Data disclosure agreements are formal contracts that detail what data is being shared and the conditions for the appropriate use for the data between *data sources* and *data using services*. DDAs could contain both personal and non-personal data.

Delegation agreements are a means to formalise delegation from a *delegator* to a *delegate* to act on their behalf in the enactment of one or many data agreements



iGrant.io as data intermediary



iGrant.io solution

iGrant.io is a **data intermediary** and offers a a **B2B data exchange platform** and **verification service** that enable access to as many personal or non-personal data points as are needed to complete a data-oriented task or to fulfil a customer interaction or transaction.



iGrant.io characteristics

- Automated data governance, based on Hyperledger and including a range of B2B and B2C data agreements
- Protocol-based with zero integration rather than API based integration which is more costly, complex and less efficient
- Cloud-based scalability
- dApp / data wallet SDK with end user consent management capabilities
- Data provenance verification providing data authenticity and quality assurance



Summary



Work on data exchanges, marketplaces and intermediaries as well as automated data exchange agreements are pioneering the ground-breaking technologies that are transforming the way that businesses and their customers interact over personal data, realising a clear and sustainable way forward.

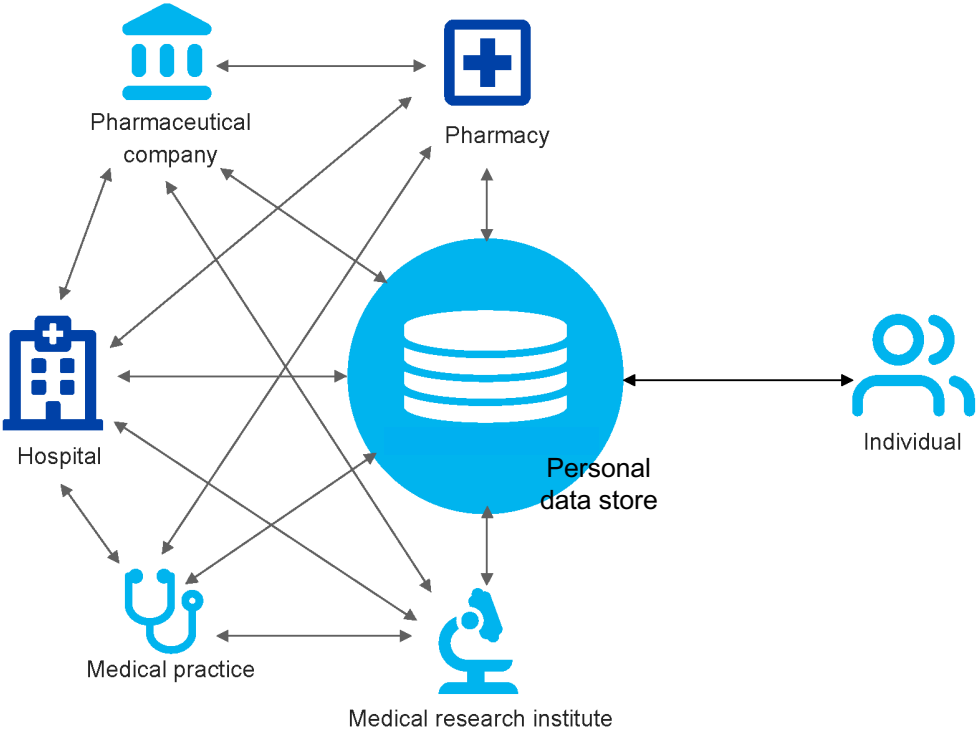


Thank you!

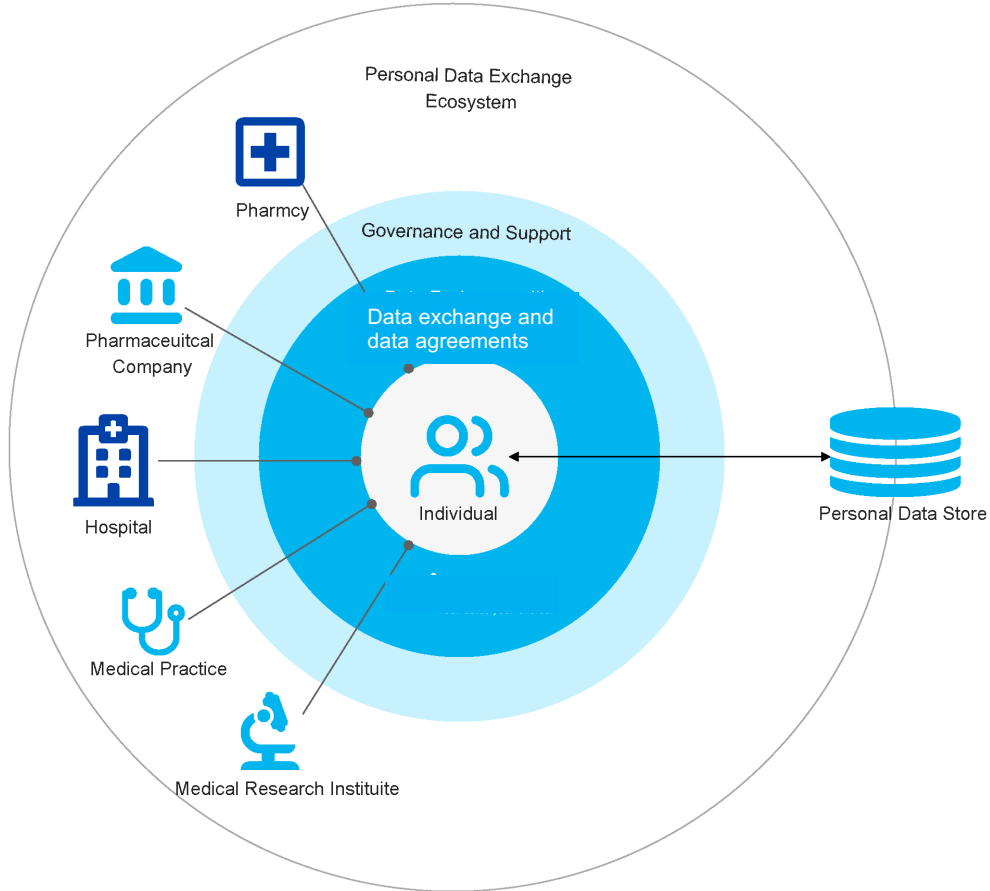
David Goodman
david@igrant.io



A medical data exchange example



A data sharing environment for patient medical records which is neither sustainable nor human-centric



A data sharing of patient medical records with a data exchange