Data Exchange Agreements

Removing the barriers to consent-based, auditable and immutable data transactions

November 2022

An iGrant.io Whitepaper

Version 2.2

Acknowledgements

iGrant.io acknowledges the following organisations in the development of concepts outlined in this white paper:

NGI ONTO CHAIN

MyData

HUMAN COLOSSUS FOUNDATION

LINALTEC

Executive Summary

With the emergence of European data spaces and data markets, one of the fundamental issues to tackle is building trusted digital relationships between the parties in a data ecosystem.

In this white paper, we propose a suite of data exchange agreements as a means of establishing trust through transparency and auditability concerning the use of personal data. These data exchange agreements provide a legal, auditable construct for data transactions which benefit not only the individuals whose data is being transacted but also the organisations involved in the exchange of data . This ensures that the risk of non-compliance and contentious legal disputes is minimised. In case of a dispute, the agreements can be shared with a third-party auditor or used in a court of law. The data exchange agreements facilitate the governance of the ecosystem for actors such as data sources, data using services and data intermediaries.

This paper addresses how organisations can:

- build trust with individuals by being transparent about their personal data usage, empowering individuals to control the use of their data
- legally capture data beyond what is accessible within their own data sources
- ensure an auditable provenance trail that minimises the risk of non-compliance and data misuse

iGrant.io is a data intermediary for privacy-aware data exchange and verification services and stands at the forefront of developing and implementing data exchange agreements for a sustainable digital economy.

The organisations actively supporting this initiative include Human Colossus Foundation, MyData Sweden and Linaltec. The standardisation is being driven by the Decentralized Identity Foundation (DIF) and MyData communities.

Contents

Introduction

An exciting new trend is emerging: organisations are realising that there are ways and means to share and monetise the vast amount of valuable data assets in their possession with other organisations without breaking the law and without breaching their customers' trust. Many, if not most, large companies have been storing and sharing data collected from their customers and employees for years without having much regard for consumer rights or regulations. With the emergence of privacy-preserving technologies and, more importantly, cloud-based data exchanges and marketplaces, it is possible for companies to share data while preserving security and maintaining privacy.

According to Deloitte Insights[1]:

> *During the next 18-24 months we expect to see more organizations explore opportunities to create seamless, secure data-sharing capabilities that can help them monetize their own information assets and accomplish business goals using other people's data.*

According to Forrester Research[2], more than 70% of global data and analytics decision-makers are expanding their ability to use external data, and another 17% plan to so within the next 12 months.

Through the availability of innovative technologies and techniques, the data sharing revolution is making it possible for organisations to access more data more securely within their own ecosystems and from other organisations.

With the emergence of privacy- and security-preserving mechanisms, a crucial missing component was the involvement of the individuals whose data is to be processed and re-circulated. However, this has now been resolved. With immutable, automated and auditable data agreements, individuals can manage and follow who is consuming their data, when and why.

The data exchange agreement is a unique differentiator that provides any data ecosystem with the opportunity to engage in

1 Deloitte Insights: Tech Trends 2022 and 'Data-sharing made easy'
2 CDOs Wanted: Dedicated, Expanded Data Insights Leadership, Jennifer Belissent, 8 January 2021

trusted data exchange scenarios and directly involve individuals in a regulatory compliant and verifiable way.

Organisations, which could be either data sources or data using services, can leverage personal data and gain access to reliable data, provided they offer adequate transparency for individuals to trust them, and their data usage is compliant with the relevant data protection and privacy regulations which they can prove if requested.

In addition, because auditors can independently prove fair data usage via audit mechanisms, data exchange agreements give both organisations and individuals a means to verify the legitimacy of their claims in any legal dispute concerning the use or misuse of data.

Any organisation undergoing digital transformation needs to ensure that it 'follows the rules', so individuals continue to say "yes" to sharing their data, directly or through a data intermediary as proposed in the EU's Data Governance Act.

Data Intermediaries Enabling Data Exchange

A data intermediary helps organisations access and share personal data with the agreement or consent of the individuals involved. Using data exchange services, organisations gain access to verifiable and lawful data on a large scale. Every data exchange transaction has an associated data agreement that records conditions for an organisation to process personal data in accordance with data regulations, as illustrated in figure 1.

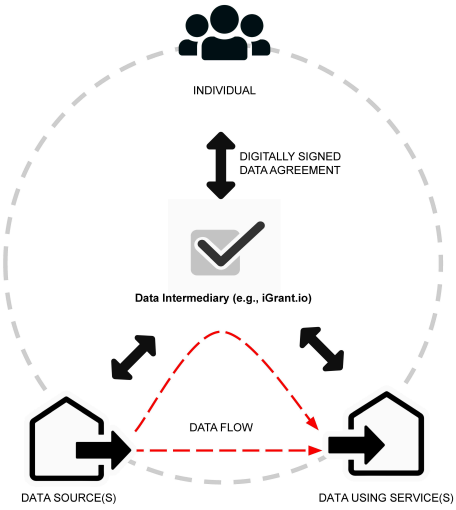


Figure 1. A data exchange ecosystem using a data intermediary

Data Exchange Agreements

In a data exchange ecosystem, there are several agreements that are required to legally endorse the actual data transactions. The various data exchange agreements contextualise the relationships that exist between organisations and individuals, depending on their roles in different usage scenarios involving personal data. The various agreements involved can be classified into four broad categories as shown in figure 2. These are agreements between:

- An individual and an organisation (**data agreement**)
- Two organisations (a data source and a data using service (**data disclosure agreement**)
- An organisation and its supplier (**data processing agreement**)
- Two individuals (**delegation agreement**)

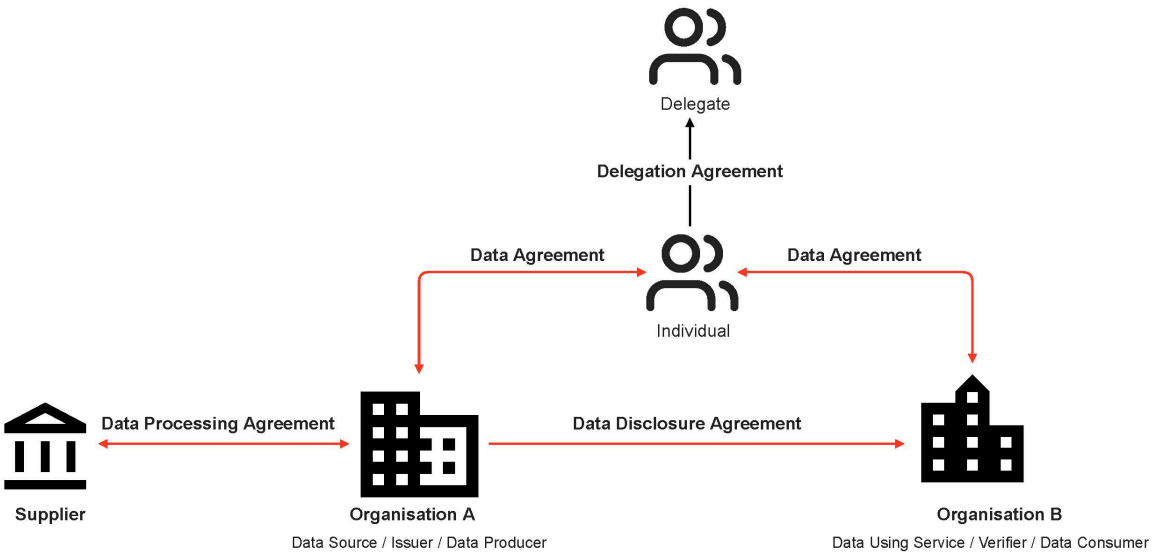


Figure 2. Data exchange agreements

Data Agreement

A data agreement, also referred to as a personal data agreement, exists between an organisation and an individual regarding the use and processing of personal data. A data agreement can have any legal basis as outlined by the relevant data protection regulation. The agreement can be between an individual and a data source (issuer) or a data using service (verifier).

Under the GDPR, there is a requisite for a policy to be in place for an organisation sharing personal data with third parties; the data agreement demonstrates that processing is performed in accordance with the regulation.

Today, a data agreement is implemented via a W3C-specified decentralised identifier (DID). It records the conditions for an organisation to process personal data in accordance with the relevant data protection regulations which could be data laws or norms such as the MyData principles.

Data agreements are characterised by being:

- Associated with any personal data usage including data sharing with third parties
- Reliant on an individual's consent or other lawful basis such as contract, legal obligation, vital interests, public tasks and legitimate interests by outlining the purpose for which personal data is to be processed
- Tied to, for example, a data protection impact assessment (DPIA) or similar that further strengthens an organisation's legal compliance. iGrant.io automates the conversion of the results of a DPIA to a machine-readable data agreement
- Standardised via ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection WG5: 27560 (working draft)

The key values enabled by a data agreement are:

- Risk reduction: A data agreement reduces the risk of non-compliance to data regulations. Based on a data protection impact assessment, a data agreement provides reassurance that an organisation has the intent to exchange data in compliance with a jurisdiction-appropriate data protection regulation.

- Transparency: A data agreement provides the requisite transparency to a data subject on how their personal data is to be used by an organisation, especially if exchanged with third parties.

- Auditability: With a data agreement, a data source can prove its legitimate right to collect and share data with a data using service via digital token-based verification system. Similarly, an individual can dispute data usage for which no legitimacy can be proven using the signed data agreement.

Data Disclosure Agreement

A data disclosure agreement exists between two organisations where one organisation acts as a data source and the other as a data using service. The term data sharing agreement is sometimes used synonymously in reference to 'good practice' in conformance with GDPR Article 28. The data disclosure agreement captures how data is shared between the two organisations and what roles and obligations each party has, either as a data processor and/or as a data controller. For any organisation involved in the data exchange, there is an associated data agreement that explains the purpose of processing personal data, what personal data is collected, what the rights of the data subject are, etc. Where both organisations are data controllers, the data subject has a signed data agreement with both.

Data Processing Agreement

The third form of agreement exists between an organisation and its suppliers, as illustrated in figure 2. where a vertical relationship exists between Organisation A as a data controller and its supplier as a data processor or sub-processor. For a higher level of accountability between these organisations and mandatory for the GDPR, a data processing agreement is set up, to lay out the routines required: for example, a data processor's obligations in case of a data breach or how the rights of the individual, such as access rights, are supported, among other policies and routines. An auditor should also be able to inspect the organisation and use the data processing agreement as reference material during the inspection. As depicted in figure 2, the data processing agreement is connected to the individual at the top of the hierarchy via the data controller organisation.

Delegation Agreement

A delegation agreement describes scenarios in which a delegate acts on behalf of an individual in signing off a data exchange. There are several scenarios where delegation is necessary. For example, in the case of:

- guardianship when an individual is incapable of signing off due to infirmity, incapacity or illness; or
- an individual is given temporary rights to sign off on behalf of another individual: for example, purchasing medicine at a pharmacy or collecting a parcel from a post office.

Data Provenance

Tangential but critical to the efficacy of the suite of data exchange agreements, it is vitally important for organisations to have confidence in the verifiable provenance of the personal data they are handling, in order for them to know that the data is 100% reliable.

W3C defines provenance as the information about entities, activities, and agents involved in "producing a piece of data or thing", which can be used to form assessments about its quality, reliability or trustworthiness.

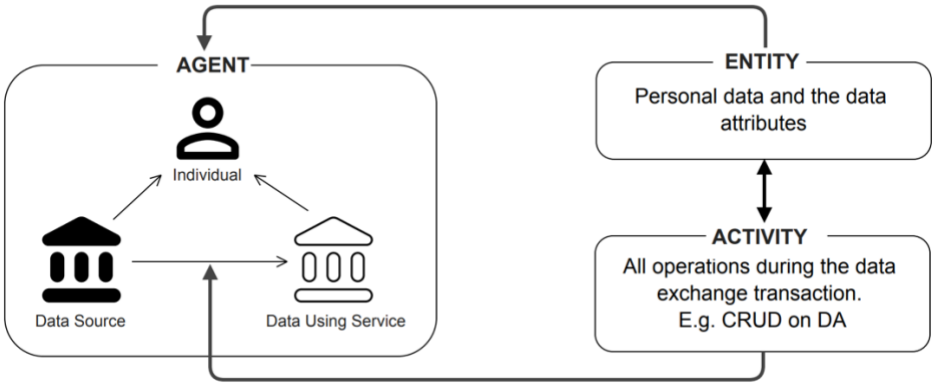


Figure 3. Data provenance terminology (from the W3C PROV Primer)

The different models used in data provenance include the Open Provenance Model (OPM) and W3C PROV, both of which have basic entity, activity and agent (people) components. They differ in that W3C PROV provides additional terms to help with explaining the details of activity

through the usage of “plans”, which set out the details of the execution of an activity.

In the context of a personal data exchange transaction as illustrated in figure 3:

- the agents are the actors involved in the transaction such as the individuals (or data subjects) and the organisations (data source and data using service),
- the entities are the data and the data attributes being exchanged,
- the activities include create/read/update/delete (CRUD) operations on these agreements.

In a personal data transaction, provenance provides a critical foundation for assessing authenticity, enabling trust, allowing reproducibility and the re-use of personal data. When this is achieved, assertions can be made about the use of contextual metadata: for example, events in data agreements and data disclosure agreements. These can themselves become important records with their own provenance. Once provenance metadata is collected it is possible to check claims that are being made in the records.

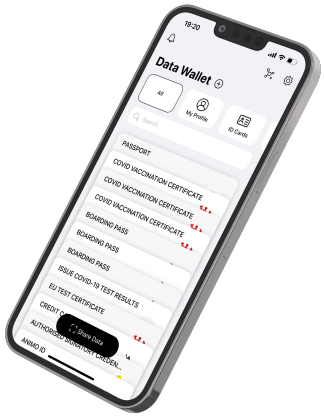
Use Case

Charlotte wants to travel to a country with an outbreak of a dangerous virus and is required to show a valid medical certificate (valid test - or vaccination certificate). Charlotte gets a test from a recognised Test Centre to prove that she is virus free and allowed to travel. The Test Centre issues its test results in the form of digital certificates which Charlotte can store in her iGrant.io data wallet and share with the travel company.

Connecting to the data issuer

Charlotte visits the Test Centre to test for the virus. Using her data wallet, Charlotte registers by seeking an organisation connection, scanning the QR code provided and then connecting to the Test Centre. The Test Centre is now listed as a connected organisation.

Data issue



Charlotte identifies herself and after this is verified by the Test Centre, she gets tested for the virus. Once available, the test results are issued by *filling out* a simple form. The fields included in the form are optimised based on the purpose, such as medical passport, visitor registration and access.

- A notification is sent to Charlotte's data wallet.
- She sees there is a notification and pushes the notification icon.
- The test results appear on the screen in the form of a certificate, which Charlotte accepts and holds in her data wallet.

Data using service

Charlotte presents herself at the airport check-in desk and is requested to produce her valid medical test results.

- By *scanning* the QR code, Charlotte is asked first to connect to the Travel Company, and then to share the test result data by *clicking* on the exchange data button

The Travel Company receives Charlotte's test results, verifies its authenticity and checks its compliance with the airline's travel requirements.

Data exchange agreements

The use case process described above is dependent on the underlying processes involving data exchange agreements and demonstrates an active data exchange *(see figure 4).* For a comparison with a passive data exchange, see below.

- In order for Charlotte to set up a *personal data exchange agreement* with the Test Centre, her identity is verified using the iGrant.io *verification service.* Once the agreement is in place, Charlotte's Test Results are shared with the Test Centre.

- Charlotte then sets up another *personal data exchange agreement* with the Travel Company, which verifies the agreement made with the Test Centre, in order to access the Test Results.

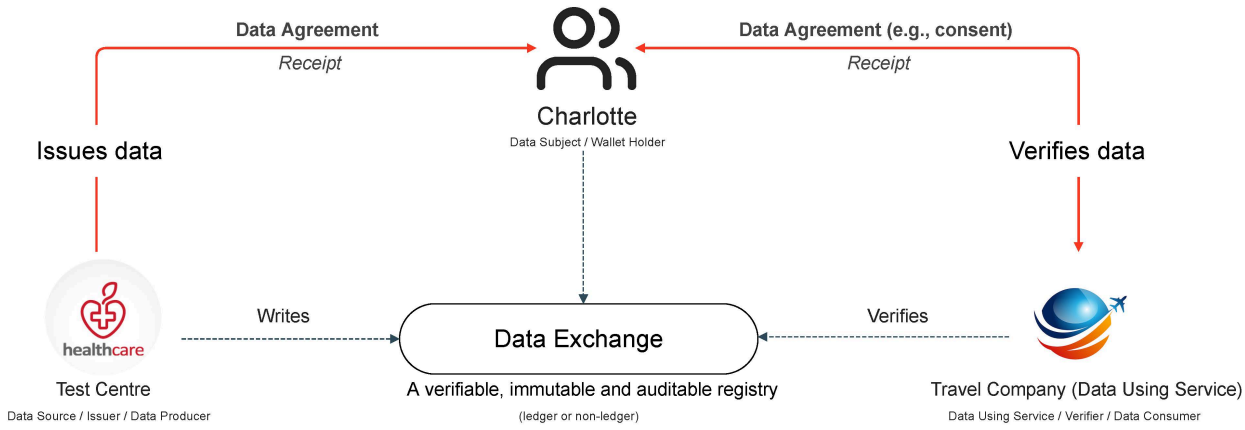


Figure 4. An SSI-enabled active data exchange

Active and passive data exchanges

A data exchange can be of two types:

(1) **Active Data Exchange:** an individual is actively involved in the data exchange flow. This can be of two types:

A. Using a data wallet, the individual holds the data and shares the data with any data using service, in real-time.

B. Using notifications, the individual is notified of a request to use their data by the data using service and the individual agrees to a data exchange from a given data source.

(2) **Passive Data Exchange:** data is exchanged between a data source and a data using service based on a data agreement that was mutually endorsed between the individual and the organisations involved.

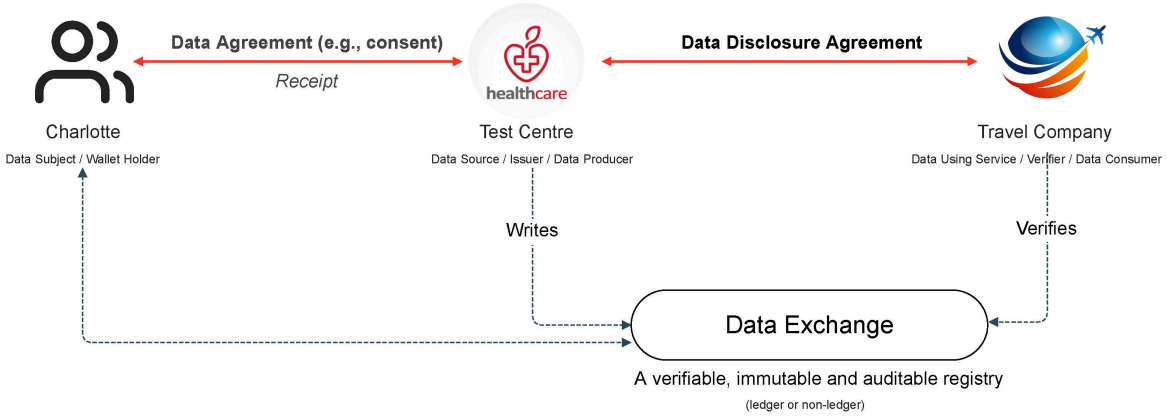


Figure 5. An SSI-enabled passive data exchange

Summary

With the introduction of data exchange agreements, new avenues are opening up for individuals and organisations to discover ways in which to collaborate confidently and efficiently in making the most of the personal data generated in different online transactions. Data exchanges are scalable ecosystems for data sharing, powered by data intermediaries that provide the underlying infrastructure, whilst enabling both individuals and organisations to choose which data intermediaries to work with.

Data exchange agreements provide the fundamental basis for creating a trusted and dynamic data space or marketplace that facilitate the use and re-use of data across an ecosystem.

This is a revolution in the making.

Through the emergence of new technologies and standards (from SSI and W3C) and governance mechanisms (ledger-based, data exchange agreements), it will be possible to exchange data cross-company and cross-border without breaking the law or invading people's privacy.

iGrant.io is at the forefront of this technological evolution that gets to the heart of the trust and accountability issues associated with data sharing.

Annex

Data Exchange Overview

Figure 6 illustrates how an organisation, Org. A, uses a data agreement to share data externally to Org B and Org C. Individual instances of the data agreement are signed by individuals X and Y. A data disclosure agreement is used to govern the data exchange between Org A and Orgs B and C.

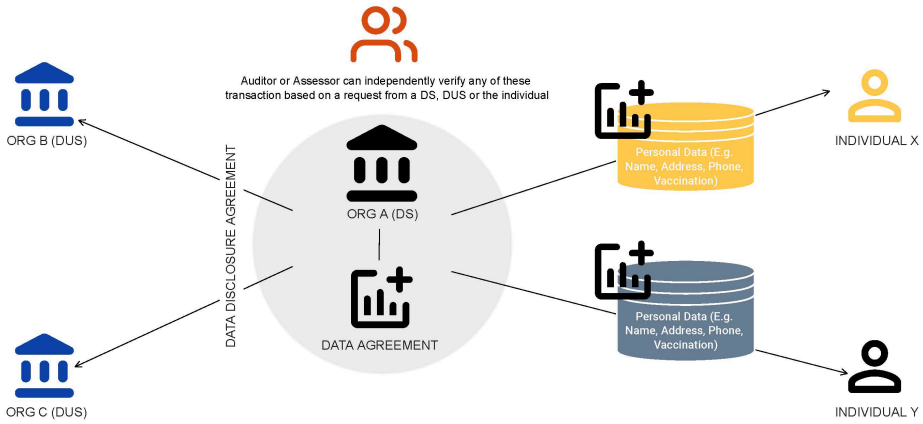


Figure 6. Data exchange and provenance scenarios

Data Exchange High-Level Workflow

Figure 7 illustrates the different phases of a decentralised data exchange service workflow based on self-sovereign identity (SSI), OpenID Connect and OAuth protocols. The service enables organisations to exchange data in a transparent, secure and privacy-centric manner using verifiable data exchange agreements. The received data can be verified using SSI and X.509-based signatures.

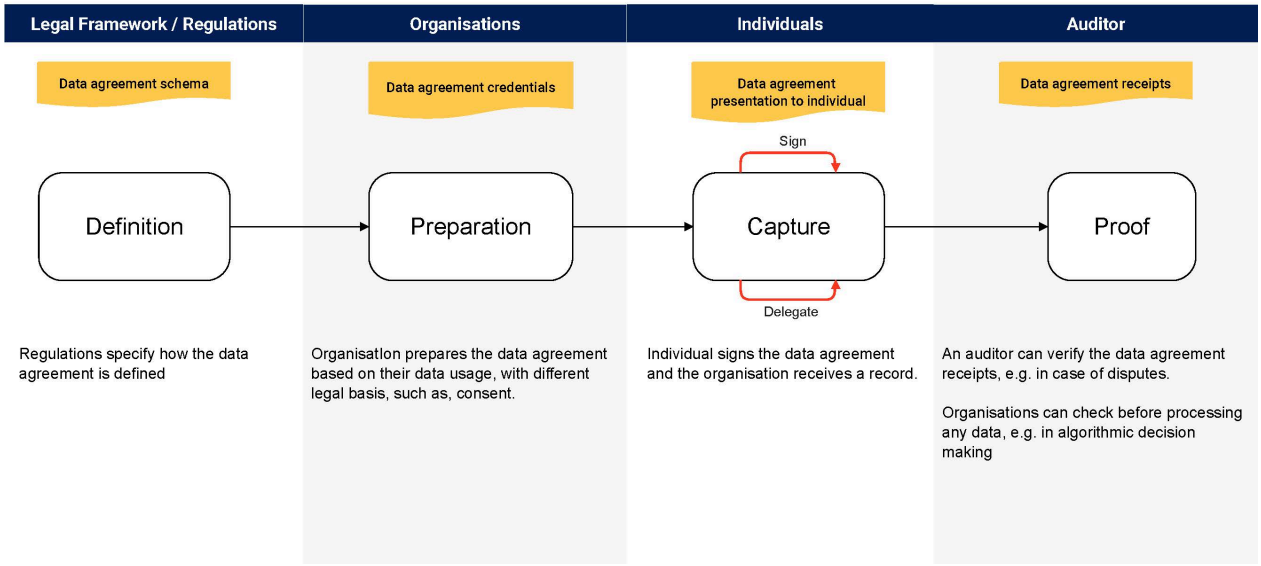


Figure 7. A data agreement and data disclosure agreement workflow

These different phases are:

- Definition: An existing agreement template is adopted as-is or a new one is formulated. The template could be based on a particular industry and/or sector-specific practice, which can then be used by any organisation (a data source or data using service) for a particular data usage purpose. In this example, it is for enabling a third-party data exchange.
- Preparation: An organisation creates an agreement based on a data protection impact assessment or similar and shares it with relevant parties. For a data agreement, the relevant counterparty is the individual while, for the data disclosure agreement, it is a data using service.
- Capture: The counterparty signs the agreement. For a data disclosure agreement, it is countersigned by the data using service while, for a data agreement, it is the individual.
- Proof: Any organisation or individual can demonstrate that an agreement exists between the parties. Independent auditors can also check that records are in place proving that the individual's personal data may be processed (e.g., as per GDPR Article 30).

Data Provenance Enabling Workflow

The four phases described above are further elaborated in figure 8 and explain how the data agreements and data disclosure agreements are interlinked in the data exchange

workflow. To ensure their compliance with data regulations, each organisation is encouraged to perform a privacy risk assessment or data protection impact assessment and ensure that risk mitigation measures are in place before collecting and processing personal data.

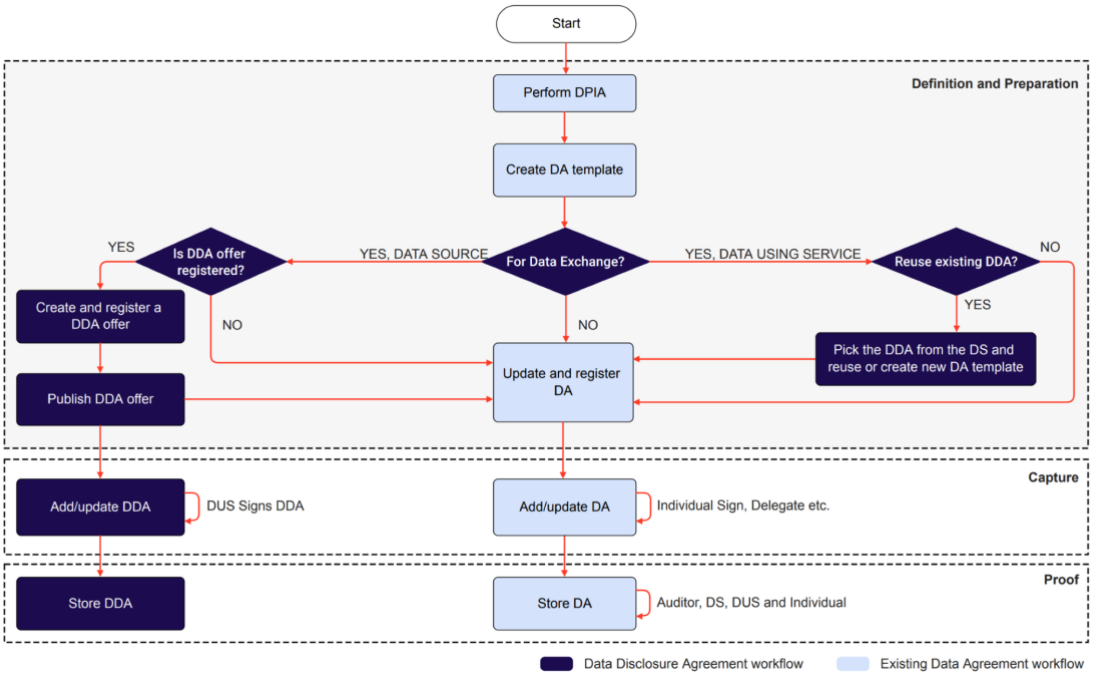


Figure 8: Data agreement and data disclosure agreement interlink within a data exchange workflow

When a data disclosure agreement is signed and personal data has been exchanged, the data source is not liable for the data using service's use of personal data. However, the obligation to monitor the individual's consent to share data with a third party, in this case, the data using service, remains with the data source. The data using service is obliged to adhere to the terms laid out in the data disclosure agreement. If the data using service does not adhere to the data disclosure agreement, the data source can, upon finding out about the infringement, withdraw the data disclosure agreement and consequently revoke all the data agreements associated with the data disclosure agreement.

Throughout the data agreement lifecycle, cryptographic proofs are generated detailing who created the data agreement during the preparation phase and who signed it during the capture phase. This is based on a W3C specification and realised via a data agreement protocol implementation.

iGrant.io is a Swedish cloud-based data intermediary for privacy-aware data exchange and verification services. The solutions are based on self-sovereign identity technology (SSI) and follow the MyData principles based on open standards such as W3C, DIF and ToIP.

Using a data wallet, the iGrant.io infrastructure lets individuals control and share their personal data for the purposes they choose, enabling a new level of scalable interoperability and automating compliance with data protection and privacy regulations.

With the iGrant.io solution, organisations can access verifiable personal data to support their digitalisation efforts within a B2B/B2G ecosystem

Bössvägen 28
Sollentuna - 192 55
Sweden

info@igrant. Io

www.igrant.io