# Sharing Agreement (request- perspective)

## What is it.

The customer journey is developed from the standpoint of the data consumer. The data consumer goes through a discovery phase, either interactively (via a search and discovery front-end) or by automation on the connector. Discovery includes exploratory data analysis that is implemented with test data products or mock data.

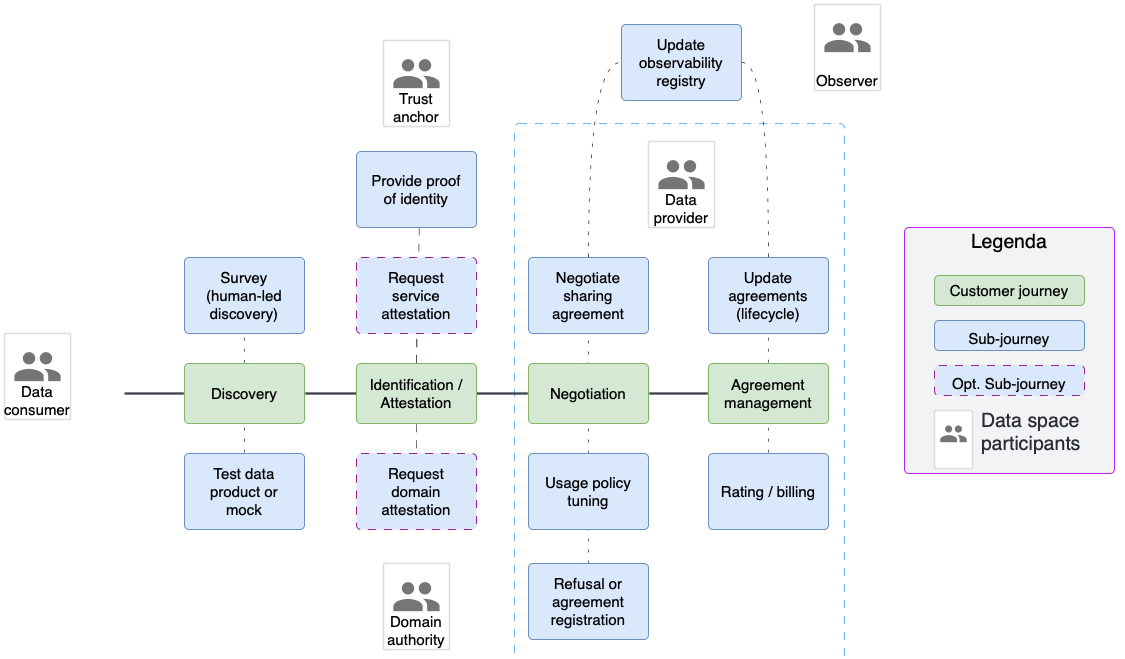
There might be a case where the consumer is required to give proof of trust or compliance, the attestation phase is such a process where the data producer or a trusted entity grant the attestation to the consumer.

The data consumer enters in negotiation with the data product provider, the resulting data sharing agreement is either refused or put in force. In the latter case, the sharing agreement is registered, for governance purposes, in an observability registry.

Data sharing agreements undergo a business lifecycle of updates, renewal, revocation, and rating updates in case a value-transfer offering is involved.

## Detailed overview

### Graphical representation



### Actors

|  |  |  |
| --- | --- | --- |
| Actor | Description | Notes |
| Data consumer | A participant engaged in data sharing in the International Data Spaces requesting and using data provided by a Data Provider. | Participants can assume different roles (e.g., consumer, producer, intermediary, etc.) |
| Data provider | Participant exposing Data Sources via a Connector; a Data Provider may be an enterprise or other organisation, a data marketplace, an individual, or a “smart thing”. |
| Observer | A participant that implements a business observability function across the entire data space. There might be more than one observer in a data space. | Business observability is the pillar for governance enforcement. |
| Domain authority | A domain authority maintains a  governance framework that is specific to an industry or part of it. To simplify the customer journeys, we assume that the domain authority is also able to certify an entity to be compliant with the domain governance. | GAIA-X, is an example of domain authority supporting a framework to verify trust compliance.  ISO institutes |

### ~~Customer journey: Discovery~~

### Customer journey: Attestation

|  |  |  |  |
| --- | --- | --- | --- |
| Sub-customer journeys | Description | Examples of ISO 25010 Qualities | Review/tests |
| Request service attestation | The provider might request a consumer to self-produce proof that it complies with the producer’s governance. The producer defines the behaviour it expects from the consumer, the producer can measure such behaviour without intermediaries. | 1. Functional appropriateness: The system provides building blocks to create an attestation, notably: a language to express the attestation, a way to present an attestation, mechanisms to define the measurement of the attestation. 2. The system allows a data producer to define the attestation. For instance: “The consumer’s connector runs on a trusted execution environment”. 3. The system allows the consumer to deploy a status function, for instance: “A cryptographically signed hash that certifies that my connector runs on a trusted execution environment.! 4. The system allows the consumer to present the measurable status, for instance: “Verifiable presentation on VCs”. 5. The system allows the producer to validate the above-mentioned verifiable presentation. | **1: Assessment and coverage tests: Create a mock scenario where a participant is attested as being based in EU. Measurement based on GeoIP library…**  2: Prove that the system has the capability to delegate a data producer to attest a participant.  3: Emulate a TEE (<https://github.com/Open-TEE> ) and provide a TEE attribute as a service.  4: The signed TEE certification is included in a Verifiable Presentation. |
| Request domain attestation | The producer might demand that the consumer present proof of compliance from an industry authority that defines a domain governance. | As above, but the issuer is the domain authority, while the appraiser remains the producer. |  |

### Customer journey: Negotiation

|  |  |  |  |
| --- | --- | --- | --- |
| Sub-customer journeys | Description | Examples of ISO 25010 Qualities | Review/tests |
| Negotiating sharing agreement | The data producer and consumer engage in matching respective requirements for the use of the data product offering. The producer might define data usage policies or demand a attestation. The negotiation can take different steps and channels, even engage parties through off-band channels (e.g., e-mail or phone calls). | 1. Interoperability: The system provides components that negotiate a data sharing agreement through a common protocol. 2. Interoperability: The data sharing protocol implements requests, responses, and states that produce an iterative data sharing negotiation which is semantically interpretable by an observer. 3. Functional completeness: The protocol implements negotiation based on claims, usage policies, and business service descriptors. 4. The sharing agreement protocol supports automated and manual negotiation. 5. The sharing agreement protocol supports notifications if either party must be informed of the outcome of a transaction or if the system is awaiting a response (asynchronous negotiation). 6. Security confidentiality: The data sharing agreement exchanges use an encrypted channel, the two parties have mutually authenticated, and the information of the negotiation is only visible to authorized users of the data producer and data consumer connectors. 7. Security integrity: The system provides observability records of the sharing agreement states (privacy terms of observability are out of scope here). | **1,2: Test completeness: Two connectors can negotiate a data sharing agreement that supports a defined minimal state machine (the definition of the minimal state machine must be agreed beforehand).**  2: Assessment: states, transactions and outcomes are semantically defined and can be described in a vocabulary.  3: **Tests: prove that the negotiation can use the following assets and parameters to define a contract:**   * **Claim verification** * **Usage policy rules** * **Service Agreements**   **The larger the coverage, the higher the rank.**  4: Test: create a sharing agreement that always lands in a “hold state” waiting for manual or external service input.  5: **Assessment / test that the system provides a working feedback to notify participants of the status and holding of a sharing agreement.**  **6: Test that the data sharing protocol is compatible with channel encryption (e.g. TLS), that a connector authentication has taken place exclusively for the data sharing negotiation.**  7: Verify that the system outputs logs detailing the sharing agreement process. Rank higher if the logs provide business information under a standard format. |
| Adjusting usage policies | If an initial contract agreement is not found, the data producer might decide to relinquish some usage policies, or introduce different ones as a result of the negotiation with the data consumer. | * Functional completeness: The system supports the making of a counterproposal in data sharing negotiation. | Skip tests: The feature is either unfinished (EDC) or absent (Fiware). |
| Refusal or registration of sharing agreement | The data consumer is updated on the result of the negotiation, eventually the data sharing agreement comes in force and is stored in the consumer’s connector. | 1. Security Confidentiality: The system ensures that confidential details of the agreement are only shared between authorized participants. 2. Security integrity: The system provides a observability trace of the sharing agreement (privacy terms of observability are out of scope here). 3. Integrity: A negotiated sharing agreement trace is persisted on a tamper-proof storage / DB. | 1**: Assessment: either the negotiation API, or the status messages, or the negotiation logs, are not accessible to entities other than the negotiating participants and the system admin (privileged role).**  **2: Assessment: See p7 of Sharing agreement negotiation.**  3: Assessment: determine if the logging system is protected against intrusion. |
| Update observability registry | When a data sharing agreement comes in force, the logs of the transaction are (optionally) shipped to the data space observability registry for governance controls. | * Security Accountability: The traces generated during the sharing agreement phases are bound to involved participants. * Security confidentiality: Participant’s identifiers in observability traces are obfuscated. * Security integrity: The updating and persistence of the observability registry implement tamper-proof mechanisms. | 1: Assessment: determine that a privileged user can link the records related to the sharing agreement to identifiable participants.  2: Assessment: determine that none other than a privileged admistrator.  3: Identify who is the tamperer and identify all feasible methods of unauthorized access. Check if tamper-evident mechanisms are implemented. |

### Customer journey: Agreement management

|  |  |  |  |
| --- | --- | --- | --- |
| Sub-customer journeys | Description | Examples of ISO 25010 Qualities | Review/tests |
| Update agreements | A data sharing agreement is updated for business reasons (renewal, revocation, etc) or because governance, attestations are subject to change. The consumer must be notified of these changes that could lead to re-negotiation. | 1. Security Integrity: The update system is secured (AAA), and it is designed to provide tampering detection. 2. Functional appropriateness: the system implements communication channels to notify participants of required updates. 3. Integrity: a change to a sharing agreement leads to a re-negotiation. | 1:See NIST 800-53 controls for other tests.  2: Check that the producer connector can notify the contact point of the contract on the consumer side about the upcoming contract change.  3: Verify that changes to a sharing agreement are not allowed or invalidate the a gremenet, |
| Rating billing | Rating and billing are constantly updated following the value-exchange model that characterizes the data product offering. As above, a feedback loop must inform the consumer of relevant updates. | * Functional appropriateness: The system provides a rating/billing management interface. * Modifiability: The system allows a data producer to define the rating model, tiering and conditional rating parameters. * Functional Security Integrity: The system secures the management interface for rating and billing. * Functional appropriateness: The system notifies every data consumer that rating is activated, or rating params are changed. | **Assessment: verify the existence of a rating and billing capability**. |
| ~~Update observability registry (as above)~~ | ~~Same as in Negotiation customer journey.~~ | * ~~Same KPI as in Negotiation customer journey.~~ |  |