2026 European Conference on Computing in Construction
Corfu, Greece
July 12–15, 2026

USAGE POLICIES FOR FRAGMENTED DIGITAL PRODUCT PASSPORT DATA RETRIEVAL IN AECO DATA SPACES

Krista van Zandwijk, Ekaterina Petrova, Rik Eshuis and Pieter Pauwels
Eindhoven University of Technology, Eindhoven, The Netherlands

Abstract

Decentralized digital product passports (DPPs) retrieval via data spaces are emerging as a promising approach to enable material reuse in the Architecture, Engineering, Construction, and Operations (AECO) industry. Yet, no DPP-specific operational data space currently exists, and usage policy implementation remains unexplored. Building on Eclipse, this paper develops a proof-of-concept DPP data space, implementing asset registration, usage policy definition, contract negotiation, and authenticated data retrieval. Demonstrated through a suspended ceiling element, the research shows how multiple data providers can offer modular DPP data under differentiated usage policies, offering the first technical validation for decentralized DPP exchange in the AECO industry.

Introduction

To stimulate construction and demolition waste (CDW) reuse, European policies, such as the Construction Products Regulation (CPR) and the Ecodesign for Sustainable Products Regulation (ESPR), mandate the development of Digital Product Passports (DPPs) (European Parliament and European Union Council, 2024b; European Commission, 2025). DPPs are defined as *'a set of data specific to a product that includes information specified in the applicable delegated act and that is accessible via electronic means through a data carrier'* (European Parliament and European Union Council, 2024a, p.28) and aim to support the reuse of CDW by enabling more informed decision-making throughout the value chain (Kovacic et al., 2024). However, their current implementations fall short. In the absence of a common data standard, DPPs are developed as client-specific, non-interoperable formats, and are typically managed as static documents, resulting in incomplete and quickly outdated DPPs (Zhang et al., 2026).

Addressing these limitations requires DPPs to function as dynamic records that continuously reflect up-to-date lifecycle information (Çetin et al., 2023). This, in turn, calls for a shift from centralized data management toward decentralized frameworks, where data remains with the stakeholders who generate and maintain it (Bucher et al., 2025). A promising solution is the data space framework as proposed by the International Data Spaces Association (IDSA), which is *'a data integration concept which does not require common database schemas and physical data integration, but is rather based on distributed data stores and integration on an "as needed" basis on a semantic level'* (Nagel and Lycklama, 2021, p. 7). Data spaces enable federated, secure, and interoperable data retrieval while preserving data sovereignty (International Data Space Association, 2024).

A central mechanism for ensuring sovereignty in data spaces is the specification of usage policies, which define how, by whom, and under what conditions data may be used. Steinbuss et al. (2021, p.11) define usage control as *'specification and enforcement of restrictions regulating what must (not) happen to data'*. Usage control extends traditional access control by enforcing these policies continuously, regulating how data can be processed, aggregated, or shared even after access has been granted (Steinbuss et al., 2021). For DPPs, this would, for example, enable stakeholders to disclose only the information necessary for circular practices, such as material composition, demountability instructions, or maintenance history, while restricting the use of commercially sensitive data, preventing unauthorized redistribution.

However, no dedicated data space exists for DPP creation and management in the Architecture, Engineering, Construction, and Operations (AECO) industry, and consequently, no usage policies have been established to govern DPP data retrieval. Prior research has not investigated the implementation of these policies, leaving it unclear how an end-to-end technical pipeline can operationalize usage policies to allow multiple data providers with differing data types and related protection needs to share DPP data securely and effectively.

To address this, this paper explores the first domain-specific investigation of usage policy formulation for AECO DPP data retrieval. It demonstrates a proof-of-concept DPP data space that implements the full technical pipeline, including asset registration, access and usage policy definition, contract negotiation, and authenticated data retrieval. The approach is validated in a real construction case, where three distinct data providers, each with differentiated and stakeholder-motivated usage policies, offer their data and one data consumer retrieves it.

The remainder of the paper is structured as follows. The next Section presents a systematic literature review following the PRISMA methodology (Page et al., 2021), covering related work on data spaces, usage policies, and DPPs. The Methodology Section then describes the development of the end-to-end technical pipeline. The prototype is tested in a real construction environment, illustrating the data offering and retrieval process for a suspended ceiling component from a demonstrator project in the Netherlands, with the results presented in the Results Section. Finally, the last Section concludes with a discussion of the findings and outlines directions for future research.

Related Work

Data Space Architecture

The International Data Space (IDS) Reference Architecture Model (RAM) 4, developed by the International Data Spaces Association (IDSA), is the most widely adopted system architecture to develop data spaces (Gabellini et al., 2025). As shown in Figure 1, each data space participant has a verified digital identity and an IDS Connector, which form the core of the data space. The verified digital identity, authenticated and authorized by the identity provider, ensures trust and accountability, while the connector acts as a secure gateway, enabling controlled data access while keeping data stored at its source. Data providers define usage policies that specify how their data may be accessed and used. The data space itself does not store the actual data; it only exchanges metadata and enforces policies, while the real data flows directly between connectors once all requirements are met (International Data Space Association, 2024). Beyond these core components, the IDS framework includes several federated services that support data space operations. A Broker enables the publication and discovery of dataset metadata, while the Vocabulary Hub ensures semantic interoperability through shared ontologies. The App Store offers certified applications for data processing, transforming, or integration, and a Clearing House ensures accountability by monitoring, logging, and verifying data-sharing activities.

Few studies have examined the application of data spaces in the AECO industry. Cuno et al. (2019) proposed an urban data space model based on a German municipal case, while Gil et al. (2024) developed a regulatory framework that uses a building data space to automate and digitize building permit processes. Demonstrating its applicability in circular construction, Hagedorn et al. (2025) validated

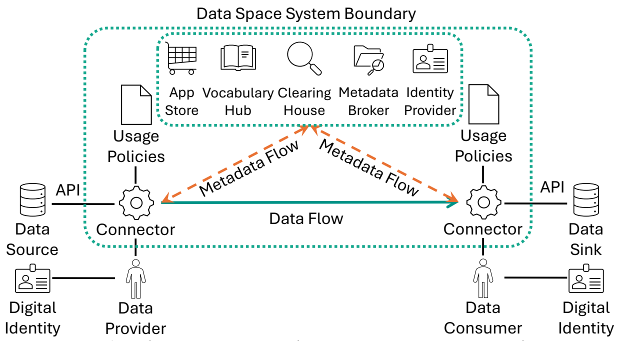

Figure 1: The International Data Spaces (IDS) Reference Architecture Model (RAM) 4 and its components, based on International Data Space Association (2024).

the integration of data space principles with Information container for linked document delivery (ICDD). Complementing these technical contributions, van Zandwijk et al. (2025) examined how data spaces should be designed at the User Interface (UI) level to meet user needs and align with existing AECO workflows.

Usage Policies

Usage policies and contract negotiation lie at the core of data offers and retrieval within a data space. When offering data, data providers attach a usage policy specifying what data consumers are allowed to do with the data once they have authorized access. In IDS, these policies are described in JSON-based contracts with a fixed structure, consisting of contract metadata and a set of usage control policy rules that define permissions, prohibitions, and obligations for data usage, as shown in Figure 2. Steinbuss et al. (2021) propose 21 classes of usage control rules, which can be combined to create tailored policies covering a wide range of mechanisms, including constraints on users, systems, locations, purposes, time, or security level, as well as rules for modification, logging, notifications, redistribution, encryption, and contractual conditions.

The usage control policy can be specified using the IDS Usage Control Language (UCL), a technology-independent, machine-readable language based on W3C's Open Digital Rights Language (ODRL) and represented in JSON-LD (Steinbuss et al., 2021). While ODRL can express usage rules, it lacks built-in enforcement capabilities, requiring external systems or additional machine-readable policy languages to implement and monitor compliance (Petrova-Antonova et al., 2026). Although enforcement is essential for a trusted data space where usage policies are effective, it is beyond the scope of this study and remains an important topic for future research. Existing research on usage control in data spaces focuses predominantly on the technical aspects of usage policy creation, negotiation, and enforcement. For example, Yang et al. (2022) propose a negotiation scheme for IDS usage policy generation, while Munoz-Arcentales et al. (2020) implement and validate a FIWARE-based architecture that enforces usage control across multi-organization environments. Similarly, Dam et al. (2023) formalize domain-specific usage-control patterns in ODRL for mobility data spaces.

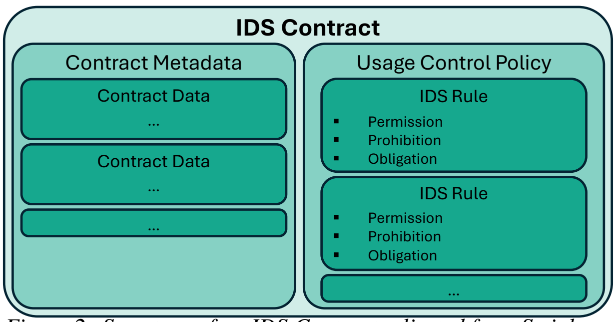

Figure 2: Structure of an IDS Contract adjusted from Steinbuss et al. (2021).

However, to the best of the authors' knowledge, no prior work investigates the implementation and negotiation of usage policies for DPP data retrieval in the AECO industry. AECO data is often complex, multi-stakeholder related, and commercially sensitive, making dedicated data spaces and tailored usage policies particularly important for this domain. The absence of domain-specific studies shows the need to explore how usage policies can support trustworthy, compliant, and efficient DPP data retrieval in circular construction contexts.

Digital Passports

Digital passports, first mentioned in 1982, gained momentum after the 2017 Buildings as Material Banks (BAMB) report (van Capelleveen et al., 2023), with the ESPR and revised CPR establishing EU-wide frameworks and registries for construction products and materials. Despite this progress, the implementation of DPPs is still evolving due to two key challenges. First, the absence of a fully standardized regulatory framework creates uncertainty about what information a DPP should contain. Second, there is no standardized digital infrastructure to support the generation, retrieval, and maintenance of DPP data across stakeholders.

Several studies have investigated the information requirements for digital passports. For example, Çetin et al. (2023) investigate data needs and actual data availability in the existing building stock, identifying eight relevant categories, including building general information, product general information, product properties, product safety, health and environment, product operational aspects, and product end-of-life aspects. Similarly, Akbarieh (2023) conducts a literature review of 146 publications and groups information needs into six categories, ranging from general information to properties requirements for safe transformation, intervention, circular information, to structural considerations. Complementing these perspectives, Byers et al. (2024b) propose a taxonomy for information acquisition to support material reuse, distinguishing between material reuse actions, information properties, and information sources.

Next to that, a variety of infrastructures have been proposed to enable DPP data exchange and retrieval. Based on a cross-domain review of 186 publications, Zhang et al. (2026) identify Distributed Ledger Technologies (DLT), ontology and knowledge-graph–based approaches, Digital Twins, and sector-specific systems such as BIM and Digital Building Logbooks (DBLs) as the most common technologies used in the construction industry. Centralized platforms, as discussed in Kovacic et al. (2024), offer structured, updatable repositories but compromise data sovereignty and frequently yield incomplete datasets due to interoperability limitations between these platforms. DLT-based systems, as proposed by Byers et al. (2024a), support decentralized trust and immutable provenance, yet they do not provide fine-grained, dynamic, and enforceable usage policies without additional off-chain mechanisms (Rohrschneider et al., 2026). Linked Data and ontology-driven frameworks, such as the work of Kebede et al. (2024), offer machine-readable semantics and flexible querying, but similarly lack mechanisms for enforcing peer-to-peer usage rules during cross-organizational exchanges (Zhang et al., 2026). Emerging work on data-space based DPPs by Gallina et al. (2025) and Belova et al. (2025) illustrate the potential of data spaces to overcome these limitations. Gallina et al. (2025) developed a data space prototype for dynamic DPP management in an industrial case of a furniture dealer. They explores various possibilities enabled by data spaces and ontologies while identifying several challenges, such as missing standards and procedures concerning trust and data usage control. Belova et al. (2025) propose an initial architecture of a DPP system using data spaces and Knowledge Graphs, using carbon foot printing in the wood processing industry as context. Their focus lie in the proposal of a conceptual architecture, and the specific usage policies are outside the scope. Zhang et al. (2026) identify a persistent privacy–security trade-off in current DPP implementations, recognizing that additional technologies are often needed to achieve the needed privacy and security levels. However, this typically address only secure access control, not usage control. Data spaces address this gap by providing both fine-grained access control and enforceable usage control.

Methodology

To explore how usage policies can support DPP data retrieval in an AECO data space, this research simulates the retrieval of DPP information from a real-life demonstrator project using a suspended ceiling element. The simulation evaluates how modular DPPs can be shared while respecting data providers' data sharing constraints. This Section introduces the case study, the modular DPP structure, the data space prototype, and the simulation setup.

Case Introduction

The research builds on the Foppingadreef project, a renovation project of a Dutch bank's headquarters. Originally constructed in 1985, the building underwent renovation and expansion in 2022, unconsciously aligning with the three step process for reuse proposed by Bellini et al. (2024), which consists of collecting information, performing information-driven evaluations, and planning for reuse. Although the renovation comprises thousands of construction elements, this study specifically focuses on the reuse of a suspended ceiling. At the start of the renovation, the building contained an estimated 82,665 ceiling panels, which were in good condition and easily demountable. During the renovation, one-third of these panels were reused on-site, while the remaining two-thirds were repurposed in another building. This requires DPP data sharing in a complex multi-actor environment where well-defined usage policies are essential to enable secure and dynamic DPP data retrieval.

DPP creation

Since the Foppingadreef was built in 1985, no DPPs or BIM models existed at the start of renovation, an issue also identified by Çetin et al. (2023). Therefore, a material inventory was created listing all visible building elements and their properties, including suspended ceilings. For these elements, the collected data was converted into a modular DPP using the networked DPP ontology by Jansen et al. (2024). Modular DPPs are necessary to achieve scalable and cost-effective DPP solutions in complex, multi-actor environments, such as the AECO industry (Zhang et al., 2026).

The DPP ontology network developed by Jansen et al. (2024) is sector-agnostic, meaning it is not tailored specifically to construction materials and may therefore be too generic to capture sector-specific nuances. Nevertheless, Jansen et al. (2024) aligned their ontology with the requirements of the ESPR, ensuring compliance with emerging regulatory requirements. Another suitable ontology is the modular DPP ontology proposed by Kebede et al. (2024), which is explicitly designed for products in the built environment. However, as this ontology is not published online, the present study adopts the published ontology of Jansen et al. (2024).

Although this study adopts the DPP ontology network for demonstration, data spaces support heterogeneous data models, as long as each dataset is accompanied by the appropriate documentation. In practice, various data standards can coexist within the same data space. The DPP ontology network is used in this research to illustrate how a complete end-to-end pipeline operates, but alternative data models or ontologies can also be used. Nevertheless, mapping different ontologies for an interoperable, scalable DPP system is beyond the scope of this research.

The DPP ontology network comprises five interconnected parts; The *DPP Ontology Design Pattern (ODP)*, which introduces the core concepts *Product* and *DPP* and their part–whole relations; The *DPP Core*, which refines the *Product* concept into subclasses such as components, materials, and substances in line with EU directives like the ESPR; The *DPP Information* module, which models the various types of information a DPP may contain through reified information objects, such as characteristics, product quality, and certification data; The *Product Composition* module, which represents detailed part–whole relationships, including substances of concern; And finally, the *DPP Provenance* module, which supports tracking of actors and temporal validity associated with the DPP data.

To create this modular DPP, the data from the material inventory is supplemented with mock-up data, as the inventory only contains information obtainable through visual inspection and therefore lacks essential elements such as certificates, repair instructions, and fire safety documentation. Since this research focuses on retrieving DPP data via usage policies rather than creating a complete and fully accurate DPP, the enriched, partially synthetic DPP is considered sufficiently robust to demonstrate and validate the proposed concept.

Data Space Environment

A small-scale data space is created using the Eclipse Minimum Data Space (MVDS) framework[1]. The MVDS code enables the creation of a small-scale demo data space compliant with current standards, including the IDS Dataspace Protocol and Gaia-X–aligned trust and identity mechanisms. The Eclipse MVDS is chosen over IDSA's MVDS[2] as it represents the state-of-the-art in open-source data space implementations (Gabellini et al., 2025).

As shown in Figure 3, the MVDS consists of only the core components required to establish a functional data space: a connector and an identity hub for both data providers and consumers. Each connector includes an internal catalog that describes the metadata of the provided data and the associated policies. The provider's connector has two catalogs: a private catalog, accessible only to the data provider, and a shared catalog, which is accessible to other participants who meet the access policies defined for the catalog. The identity hubs use decentralized identifiers (DIDs), but in this demo, identities and credentials are pre-created and manually seeded. The dynamic issuance of verifiable credentials by trusted authorities lies beyond the scope of this study.

The MVDS code is run locally on Linux via IntelliJ, which provides configurations for consumer and provider connectors, identity hubs, the provider catalog server, and a compound 'dataspace' setup to start all runtimes simultaneously. A NGINX instance hosts the issuer's DID document, with port mapping aligned to the expected DID. Once the runtimes are running, the data space is initialized using the provided seed.sh script to set up the Participant Contexts and enable connector-to-connector communication. REST API interactions can then be executed via the included Postman collection.

Scenario simulation & Policy formulation

To demonstrate the full technical pipeline, the research build upon a scenario in which multiple data providers offer different parts of a modular DPP with a single data consumer, conceptually shown in Figure 4. Three actors

[1] https://github.com/eclipse-edc/MinimumViableDataspace

[2] https://github.com/International-Data-Spaces-Association/IDS-testbed

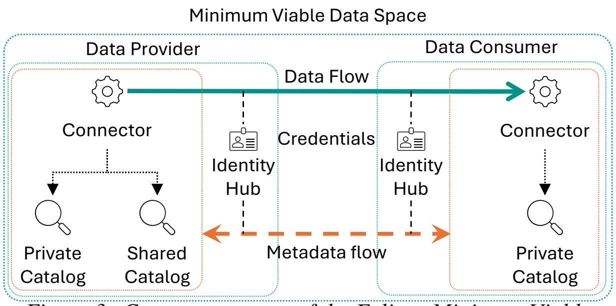

Figure 3: Core components of the Eclipse Minimum Viable Data Space.

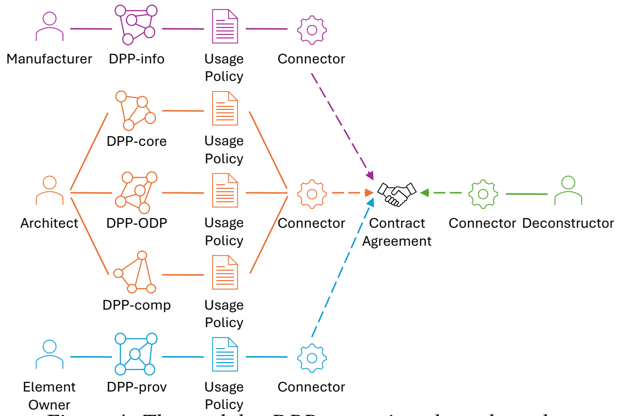

Figure 4: The modular DPP scenario, where three data providers contribute distinct DPP modules with specific usage policies, all accessed by a single data consumer.

act as data providers: the manufacturer, the architect, and the element owner. Each contributes specific DPP modules: the manufacturer supplies DPP-info; the architect provides DPP-core, DPP-ODP, and DPP-comp, and the element owner supplies DPP-prov. Verstraete et al. (2025) argues that data providers are reluctant to share data with other stakeholders, and Dam et al. (2023) argues that different data providers may have different data sharing constraints depending on their role and data offer. Hence, each data offer has its own sharing constraints and therefore usage policy. The manufacturer protects competitive information and limits liability by allowing DPP-info access only for safety, planning, and compliance during the deconstruction project. The architect safeguards intellectual property by permitting read-only access while prohibiting modification, redistribution, and printing. The element owner prioritizes privacy, requiring one-time read access, mandatory deletion within 24 hours, and notifications upon access. The usage policy for the architect is shown in Listing 1. This IDS contract permits the data consumer to read and display the specified dataset, while prohibiting modification, distribution, or printing.

These policies and constraints are hypothetical mock-up scenarios designed to demonstrate the proof of concept. However, the specific differences in usage policies per stakeholder group and data type for DPP data in the AECO industry is unexplored. Therefore, this research builds upon these fictitious scenarios to illustrate the modular DPP approach, but future work should explore specific differences in usage policies per stakeholder groups and data

Listing 1 Example of an IDS Usage Policy describing permitted and prohibited actions for using the DPP-core asset.

```
{  "@context": [
     "https://w3id.org/edc/connector/management/v0.0.1"
   ],
   "@type": "ContractRequest",
   "counterPartyAddress": "{{PROVIDER_DSP_URL}}/api/dsp",
   "counterPartyId": "{{PROVIDER_ID}}",
   "protocol": "dataspace-protocol-http",
   "policy": {
     "@type": "Offer",
     "@id": "{{POLICY_ID_DPP-core}}",
     "assigner": "{{PROVIDER_ID}}",
     "permission": [
       {"action": "use",
         "constraint": [
           {"leftOperand": "idsc:ALLOWED_ACTION",
             "operator": "eq",
             "rightOperand": ["idsc:READ", "idsc:DISPLAY"] }
         ]
       }],
     "prohibition": [
       {"action": "use",
         "constraint": [
           { "leftOperand": "idsc:PROHIBITED_ACTION",
             "operator": "eq",
             "rightOperand": ["idsc:MODIFY", "idsc:DISTRIBUTE", "idsc:PRINT"] }
         ]
       }],
     "obligation": [],
     "target": "DPP-core"},
   "callbackAddresses": []
}
```

types.

Results

The Eclipse MVDS provides a small-scale data space where participants can offer and retrieve data through a six-step process, as illustrated in Figure 5. This Section describes each step of this process in detail. Sequence diagrams for all steps are available on GitHub[3], but are not shown here due to space constraints.

Creating the Asset and the Usage Policies

First, the data offer must be registered in the connector by the data provider. This registration should include a short description of the dataset and the base URL that can be used to access the data. Next, several policies need to be defined. The first is an access policy, which ensures that only participants with an active membership credential are allowed to use the asset. The second is a data usage policy, which specifies how the data can be processed and allows the data provider to enforce different usage rules

[3] https://github.com/KristavanZandwijk/MVDS

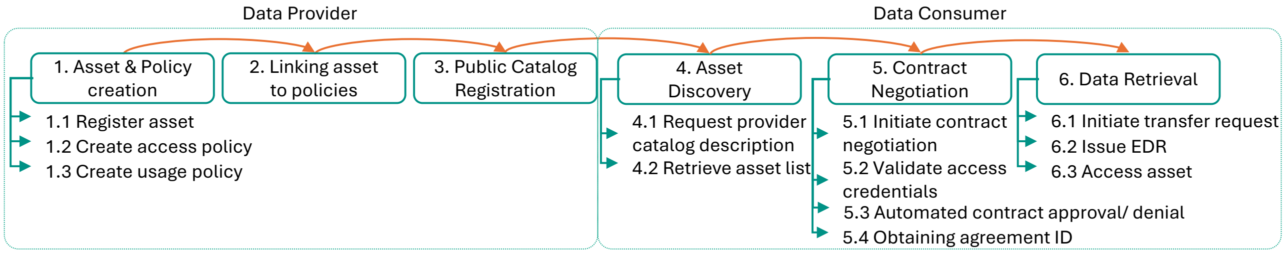

Figure 5: Six-step process outlining how data providers and consumers offer and retrieve DPP data within the data space.

depending on the type of data or the requirements of the data provider. The usage policy for the architect is already shown in Listing 1. Finally, these policies are linked to the specific asset through a contract definition, ensuring that the rules apply whenever the asset is accessed.

Public Catalog Registration

The data now has a dedicated policy but is not yet discoverable in the data space. To make it visible, the asset must be registered in the shared catalog of the provider's connector and linked with its access and usage policies. Only participants who satisfy the access policy can discover the asset, and those meeting the usage policy can access and use it under the defined conditions.

Asset Discovery

Next, the data consumer can explore available data offers. Assuming that they meet the access policy, they request the catalog from the data provider's connector, retrieving the list of exposed assets. The data consumer then queries the cached catalogs to identify the applicable policies for contract negotiation, enabling an informed decision on which data to request.

Contract Negotiation

Based on this information, the consumer initiates a contract negotiation, of which the process is shown in Figure 6. The data provider's connector verifies the data consumer's DID against the access policies. If the data consumer complies with the predefined terms, the negotiation is automatically accepted, and rejected otherwise. For now, this means that the negotiation process functions as a contract validation mechanism rather than an interactive bilateral negotiation, which is something that should be explored in future research. Once approved, the consumer receives a contract agreement ID to initiate the data transfer.

Data Retrieval

Using the agreement ID, the data consumer initiate the data transfer. The transfer is tracked via transfer processes, and the consumer retrieves the corresponding Endpoint Data Reference (EDR) to get the data address and authorization token. Finally, the data consumer uses this information to access the data from the data provider.

Following this process, the manufacturer, architect, and element owner each provide their respective DPP modules for the suspended ceiling element. The deconstructor retrieves each module in accordance with the corresponding usage policies, ensuring compliance with each provider's constraints. By repeating this process for all relevant assets, the deconstructor obtains access to the modular DPP data for the ceiling element.

Conclusion

This paper demonstrates how usage policies can enable modular and decentralized DPP data provision and retrieval within an AECO data space, using a suspended ceiling element as example. The research shows how building-product data supplied by multiple data providers can be offered and retrieved using differentiated usage policies. In doing so, the study contributes an exploratory proof-of-concept DPP data space that implements the complete technical workflow, including asset registration, access and usage policy definition, contract negotiation, and authenticated data retrieval. Because this research is based on hypothetical scenarios and a limited set of generic policy templates, it should be considered as an initial exploration rather than a mature implementation of usage poli-

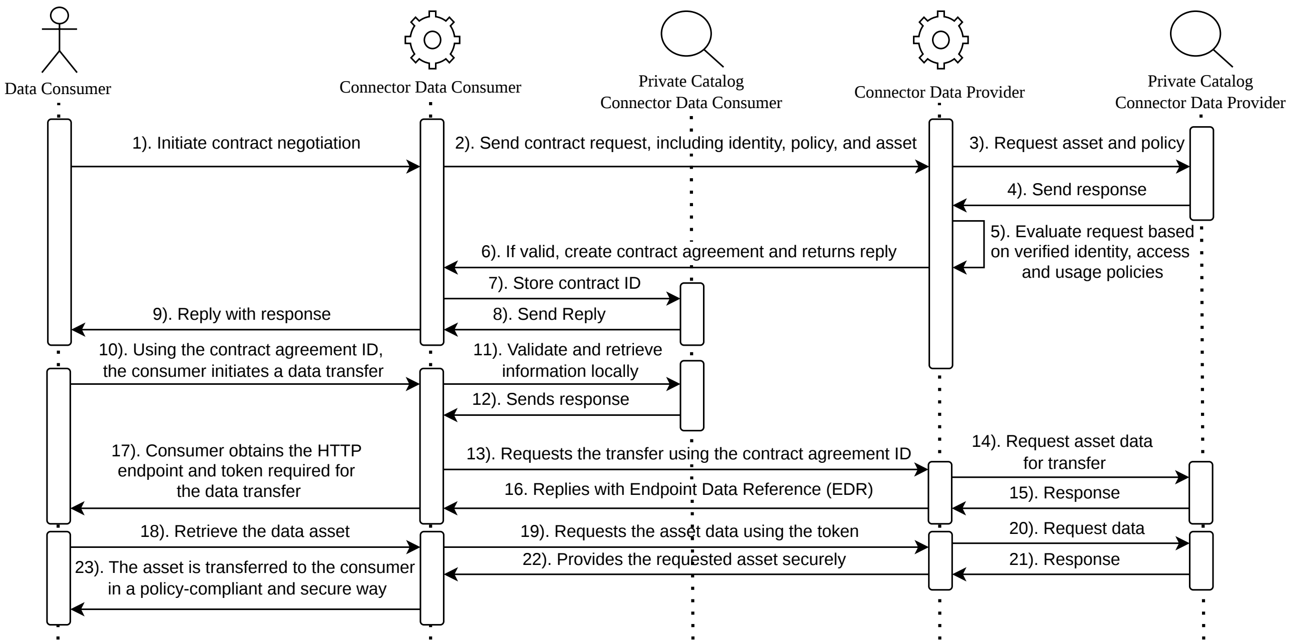

Figure 6: Sequence diagram showing contract negotiation and data retrieval between data provider and consumer.

cies in the AECO domain. Advancing toward operational deployment will require future research in several directions.

First, further work is needed to understand which specific usage-policy requirements AECO stakeholders have when sharing product-related data. Real-world needs must be validated to determine whether existing IDS policy templates are sufficient or require domain-specific extensions. As also highlighted by Bastiaansen et al. (2020), future research should therefore examine stakeholder- and data-specific policy needs while also developing more efficient negotiation mechanisms that prevent repetitive, module-by-module contracting and thus support both scalable and flexible DPP retrieval for data consumers.

Second, defining a usage policy is only one part of effective data governance; enforcing and monitoring compliance is another issue, as demonstrated in Cimmino et al. (2025). Future research should investigate mechanisms to verify policy adherence both within and beyond the boundaries the data space.

Third, as also highlighted by Sołtysiński et al. (2025), usage policies rely on the trustworthiness of digital identities associated with both data providers and consumers. Future work should explore how self-sovereign decentralized identities and trust frameworks interact with usage control and how they can be integrated into AECO data spaces.

Acknowledgments

This work is supported by the UPSCALE project, funded by Dutch Organization for Scientific Research (NWO).

Declaration of AI-generated text

During the preparation of this work, the authors used generative AI to improve the grammar and readability of the text. After using this, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

Akbarieh, A. (2023). Information Modelling for Circular Transformation of Built Assets' End-Of-Life. PhD thesis, Unilu - Université du Luxembourg, Luxembourg.

Bastiaansen, H., Dalmolen, S., Kollenstart, M., and Engers, T. (2020). User-Centric Network-Model for Data Control with Interoperable Legal Data Sharing Artefacts. In PACIS 2020 Proceedings.

Bellini, A., Andersen, B., Klungseth, N. J., and Tadayon, A. (2024). Achieving a circular economy through the effective reuse of construction products: A case study of a residential building. Journal of Cleaner Production, 450:141753.

Belova, A., Gallina, V., Revenko, A., and Ahmeti, A. (2025). Digital Product Passport: Initial System Architecture with Knowledge Graphs and Data Spaces. In CEUR Workshop Proceedings, Portorož, Slovenia.

Bucher, D. F., Hunhevicz, J. J., Byers, B. S., Honic, M., De Wolf, C., and Hall, D. M. (2025). Decentralized Data Networks for Lifecycle Management in the Built Environment. ITcon, 30:826–851.

Byers, B., Hunhevicz, J. J., Honic-Eser, M., and De Wolf, C. (2024a). Exploring Tokenized Product Passport for Circular Construction Supply Chains. In 2024 European Conference on Computing in Construction. ETH Zurich.

Byers, B. S., Raghu, D., Olumo, A., De Wolf, C., and Haas, C. (2024b). From research to practice: A review on technologies for addressing the information gap for building material reuse in circular construction. Sustainable Production and Consumption, 45:177–191.

Çetin, S., Raghu, D., Honic, M., Straub, A., and Gruis, V. (2023). Data requirements and availabilities for material passports: A digitally enabled framework for improving the circularity of existing buildings. Sustainable Production and Consumption, 40:422–437.

Cimmino, A., Cano-Benito, J., and García-Castro, R. (2025). Open Digital Rights Enforcement framework (ODRE): From descriptive to enforceable policies. Computers & Security, 150:104282.

Cuno, S., Bruns, L., Tcholtchev, N., Lämmel, P., and Schieferdecker, I. (2019). Data Governance and Sovereignty in Urban Data Spaces Based on Standardized ICT Reference Architectures. Data, 4(1):16.

Dam, T., Krimbacher, A., and Neumaier, S. (2023). Policy Patterns for Usage Control in Data Spaces. In SEMANTiCS Workshops Proceedings, volume 3510, Leipzig, Germany.

European Commission (2025). (First) CPR Working Plan for 2026-2029. Technical report, European Union, Brussels.

European Parliament and European Union Council (2024a). Establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC. Technical report, European Union, Brussels.

European Parliament and European Union Council (2024b). Regulation (EU) 2024/1781 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC. Technical report, European Union.

Gabellini, M., Civolani, L., Ronchi, M., and et al. (2025). Data Spaces in Manufacturing and Supply Chains: A Review and Insights from European Initiatives. Applied Sciences, 15(11).

Gallina, V., Lanbach, E., Ahmeti, A., and et al. (2025). Creating a Digital Product Passport Using Data Spaces and Ontologies: A Case Study at a Furniture Dealer. IFAC-PapersOnLine, 59(10):643–648.

Gil, G., Diez, F., Romero, R., Lazaro, I., and Fernandez, I. (2024). Construction Data Space for Building Permit Management. In Proceedings of the European Conference on Computing in Construction, volume 2024, pages 191–197.

Hagedorn, P., Donkers, A. J., Petrova, E., and König, M. (2025). Decentralised Data Exchange in Construction Data Spaces using Information Containers. In Proceedings of the 2025 European Conference on Computing in Construction and the 42nd CIB W78 Conference on IT in Construction, pages 566–573, Porto, Portugal.

International Data Space Association (2024). IDS RAM 4. https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0?tab=readme-ov-file.

Jansen, M., Blomqvist, E., Keskisärkkä, R., and et al. (2024). Modelling Digital Product Passports for the Circular Economy. In Proceedings of the The 2nd International Workshop on Knowledge Graphs for Sustainability (KG4S 2024) Colocated with the 21st Extended Semantic Web Conference (ESWC 2024), pages 14–28, Hersonissos, Greece.

Kebede, R., Moscati, A., Tan, H., and Johansson, P. (2024). A modular ontology modeling approach to developing digital product passports to promote circular economy in the built environment. Sustainable Production and Consumption, 48:248–268.

Kovacic, I., Honic, M., and Sreckovic, M. (2024). Digital Platform for Circular Economy in AEC Industry. EPOJ, 9(1):16.

Munoz-Arcentales, A., López-Pernas, S., Pozo, A., and et al. (2020). Data Usage and Access Control in Industrial Data Spaces: Implementation Using FIWARE. Sustainability, 12(9).

Nagel, L. and Lycklama, D. (2021). Design Principles for Data Spaces. Technical report, Zenodo.

Page, M. J., Moher, D., Bossuyt, P. M., and et al. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. BMJ, 372:n160.

Petrova-Antonova, D., Pareti, P., Tomov, P., and et al. (2026). Knowledge graph-driven policy enforcement in urban dataspace. In Knowledge Graphs, pages 406–421, Singapore. Springer Nature Singapore.

Rohrschneider, D., Pehlke, M., Handmann, U., and Jansen, M. (2026). LLM-based JSON Mapping and Blockchain Integration for Digital Product Passports. Digital Business, 6(1):100167.

Sołtysiński, T., Niederhausen, J., and Eichstädt, S. (2025). Digital Calibration Certificate in a trusted quality infrastructure federated data space: A proof of concept. Measurement: Sensors, 38:101484.

Steinbuss, S., Eitel, A., Jung, C., and et al. (2021). Usage Control in the International Data Spaces. Technical report, International Data Space Association.

van Capelleveen, G., Vegter, D., Olthaar, M., and van Hillegersberg, J. (2023). The anatomy of a passport for the circular economy: A conceptual definition, vision and structured literature review. Resources, Conservation & Recycling Advances, 17:200131.

van Zandwijk, K., Donkers, A. J., Petrova, E., and Pauwels, P. (2025). From Siloed Centralized Information Systems Towards Federated Data Ecosystems: Developing AECO Data Spaces. In Proceedings of the 2025 European Conference on Computing in Construction and the 42nd CIB W78 Conference on IT in Construction.

Verstraete, M., D'Hauwers, R., de Mildt, M., Colle, D., and Verbrugge, S. (2025). Assessing the value of decentralized and interoperable data storage for service providers. Inf Syst E-Bus Manage, 23(2):467–488.

Yang, C., Guo, Y., Yu, M., and Zhang, L. (2022). Truthfully Negotiating Usage Policy for Data Sovereignty. In 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pages 20–27.

Zhang, Z., Gu, J., Li, R., Lian, W., Ma, C., and Tian, J. (2026). Bridging digital and green transitions: A literature review of digital product passport systems. Renewable and Sustainable Energy Reviews, 228:116600.