

## CONSTRUCTION DATA SPACE FOR BUILDING PERMIT MANAGEMENT

Gonzalo Gil<sup>1</sup>, Francisco Javier Diez<sup>1</sup>, Ricardo Romero<sup>1</sup>, Ignacio Lazaro<sup>1</sup> and Izaskun Fernandez<sup>1</sup>

<sup>1</sup>Tekniker, Basque Research and Technology Alliance (BRTA), Eibar, Spain

### Abstract

Building permit management involves complex compliance checking processes that today are mainly performed by sharing documents between stakeholders and reviewing them manually. This causes long delays in obtaining building permits. Based on the DigiPLACE Reference Architecture Framework for digital construction platform, this paper presents the DigiChecks Framework, a novel approach to digitize and automate building permit management based on the orchestration of compliance checks and a data space, a distributed and open infrastructure for interoperable, trusted, and sovereign data sharing between platforms of different stakeholders. The DigiChecks Framework reduces data sharing and compliance checking efforts, while it ensures strict compliance with existing regulations.

### Introduction

The management of building permits is a process that requires numerous compliance checks based on the information shared between different stakeholders, including architects, engineers, construction companies, subcontractors, designers, certification companies, suppliers, and public authorities. The current low level of digitization in the construction sector leads to resource-consuming compliance checks, based mainly in documents sharing and manual review. This causes considerable delays in obtaining building permits.

The challenges in digitizing and automating the management of building permits are significant (Beach et al., 2013). Among all of them, the following three stand out.

1. For different countries, but also regions or municipalities, there is a need to verify compliance with different regulations (Rezgui et al., 2011).
2. To check compliance, coordination issues should be tackled by combining building data stored in different proprietary formats (Rezgui et al., 2013).
3. The reluctance to share data needs to be avoided by providing control over the data (Jarke et al., 2019).

To address these challenges, based on the DigiPLACE Reference Architecture Framework (RAF) (David et al. 2021), this paper presents the DigiChecks Framework, a novel approach to digitize and automate compliance checks by combining an orchestration of compliance checks and a data space. The orchestration provides a modular and scalable approach to manage the different compliance checks to be performed based on current regulations. The data space, following the path for the digital transformation of the construction sector (Buhler et al., 2023), facilitates the necessary collaboration between stakeholders through an open and distributed

infrastructure for interoperable, trusted, and sovereign data sharing between their different platforms.

The rest of the paper is structured as follows. First, the related work is presented. Second, based on observed needs concerning building permit management, the main principles of the DigiChecks Framework are stated. Third, based on the related work and considering the main principles of the DigiChecks Framework, the conceptual architecture of the DigiChecks Framework is described. Fourth, the DigiChecks Data Space which, as part of the DigiChecks Framework, provides an open and distributed infrastructure to enable the collaboration between platforms based on interoperable, trusted, and sovereign data sharing, is detailed. Finally, conclusions about this work are drawn.

### Related Work

The DigiPLACE RAF sets common guidelines for building digital platforms for the construction sector. Considering them, the DigiChecks Framework proposes a novel approach to digitize and automate compliance checks by combining an orchestration of compliance checks and a data space. In what follows, the DigiPLACE RAF and the work carried out on the definition and design of data spaces is described.

### DigiPLACE Reference Architecture Framework

The RAF is based on two guidelines: “Interoperability and Common Processes” and “Data Control”. They are described below.

“Interoperability and Common Processes” is divided into data interoperability, data and process management and governance. Data interoperability establishes the definition of data vocabularies based on open standards, common data formats and models, and standardized data access. Data and processes management sets the collaboration between stakeholders through common data environments and data lifecycle management based on digital twins. Governance proposes open accessibility to standards and community engagement to improve them. Figure 1 represents this.

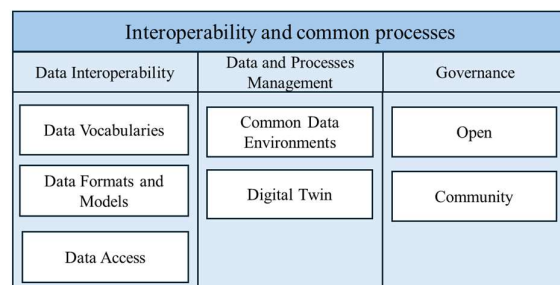


Figure 1: Interoperability and Common Processes

“Data Control” is divided into data security, data ownership, data trust and data availability and sustainability. Data security covers the security of the data, data sovereignty and data sharing within data spaces. Data ownership sets compliance with the GDPR, the ownership of the data and data transparency. Data trust encompasses data certification and value. Finally, data availability and sustainability establish compliance with FAIR principles as well as the sustainability of the data. Figure 2 represents this.

Data control			
Data Security	Data Ownership	Data Trust	Data Availability and Sustainability
Data Security	GDPR Compliance	Data Certification	FAIR Principles
Data Sovereignty	Data Ownership	Data Value	Data Sustainability
Data Spaces	Data Transparency		

Figure 2: Data Control

### Data Spaces

Nowadays, different initiatives are working worldwide on the definition and design of data spaces: The OPENDEI project, the Data Spaces Business Alliance (DSBA), GAIA-X and the International Data Spaces Association (IDSA) stand out. This large number of initiatives makes it difficult to clarify which building blocks are needed to build a data space and the technical components required to support them.

Recently, the design principles for data spaces resulting from the OPENDEI project (Nagel and Lycklama, 2021) and the common framework proposed subsequently by the DSBA (Gronlier et al., 2021) agree on the building blocks required to build a data space. These are detailed in Figure 3.



Figure 3: Data Space Building Blocks

In this context, GAIA-X and IDSA are positioned as the reference initiatives for the specification of the technical components that must be developed to support these building blocks. While GAIA-X defines the GAIA-X Technical Architecture 23.10 (GAIA-X European Association for Data and Cloud, 2023), a set of technical components for a governance framework for a federated infrastructure of services that complies with European standards and values of digital sovereignty, IDSA defines the IDSA Reference Architecture Model (RAM) 4.0

(International Data Spaces Association, 2023), a set of technical components for an interoperable, and sovereign data sharing framework between services.

On this basis and considering that the data space building blocks meet the DigiPLACE RAF core guidelines to build digital platforms in the construction sector, we consider the GAIA-X Technical Architecture 23.10 and the IDSA RAM 4.0 as the technical foundations to build the DigiChecks Data Space that acts as the core of the DigiChecks Framework.

### DigiChecks Framework Principles

For the design of the DigiChecks Framework, a review of the main needs concerning building permit management has been made. These needs are summarized below:

1. Automated compliance checking cannot be achieved with one-step solution, but by combining multiple tools in the form of services provided by different organizations that gradually makes compliance checking more mature.
2. The wide variety of existing processes, tools and contexts means that there will be no one-size-fits-all solution, but a solution that enables the interaction with multiple services.
3. Individual services communicating with each other need a common language so that they can understand each other. The common language should follow a formal, explicit specification of a shared conceptualization.

These needs lead to the following three principles of the DigiChecks Framework.

1. The framework is a distributed infrastructure, rather than a centralized, monolithic application.
2. The framework is an open infrastructure with a modular and scalable approach, where services can be included and swapped easily.
3. The framework uses a shared set of conceptual information models that align with existing domain ones. Information models are formalized based upon open and widely accepted standards.

### DigiChecks Framework Conceptual Architecture

Considering the three principles of the DigiChecks Framework, the DigiChecks Framework Conceptual Architecture is build based on the following four architecture principles:

1. The DigiChecks Framework Conceptual Architecture is a modular and distributed architecture in which the components have the flexibility to be deployed across multiple platforms managed by different stakeholders.

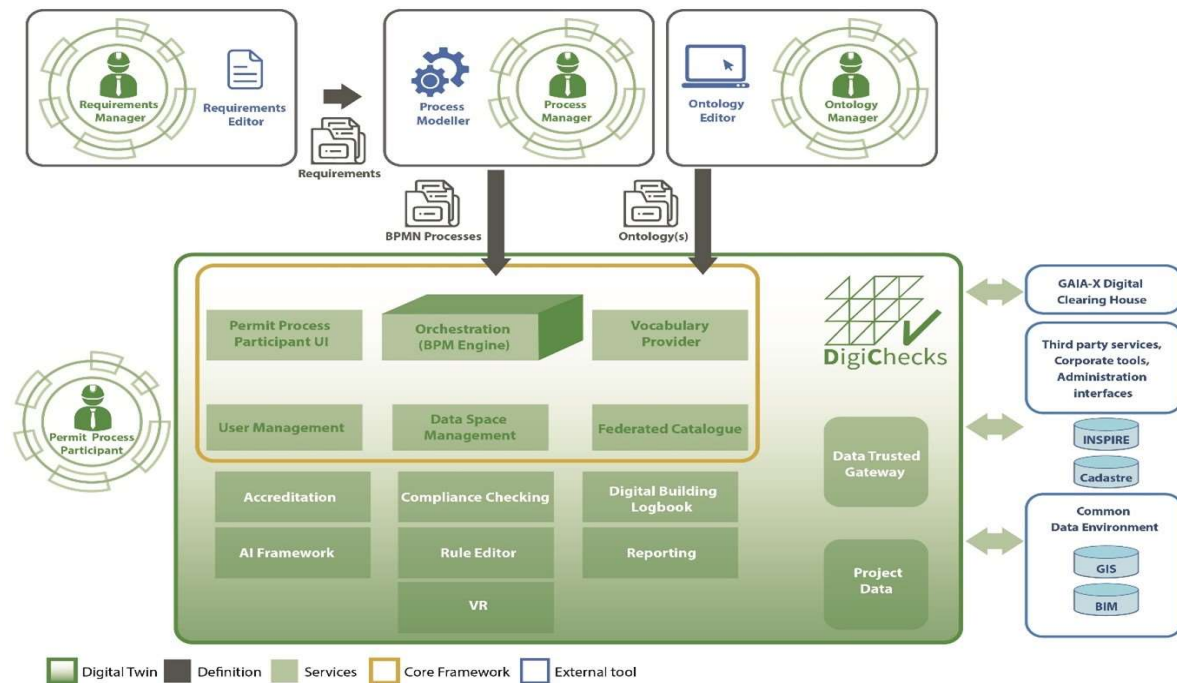


Figure 4: DigiChecks Framework Conceptual Architecture

- The DigiChecks Framework Conceptual Architecture is based on the DigiChecks Data Space to enable the collaboration between the platforms of different stakeholders based on interoperable, trusted, and sovereign data sharing.
- The DigiChecks Framework Conceptual Architecture provides Core Components that play an essential role in the orchestration of compliance checking processes and the management of the DigiChecks Data Space.
- The DigiChecks Framework Conceptual Architecture can be extended with new components that provide additional functionalities for specific use cases.

Considering these four architecture principles, Figure 4 represents the DigiChecks Framework Conceptual Architecture. It can be divided into three main blocks:

- **Design tools:** They are services that support the definition of the main elements involved in the building permit management.
- **Core Framework:** It consists of unique services that provide core functionalities to manage building permits.
- **Digital Twin:** It is composed of the Core Framework and additional services that provide specific functionalities that in conjunction with the Core Framework enable the performance of modular and scalable compliance checks.

All these main blocks and their components are further described below.

### Design Tools

The Design Tools are divided into the Requirements Editor, the Process Modeler, and the Ontology Editor.

The **Requirements Editor** assists the *Requirements Manager* in the definition of the requirements to be involved in compliance check processes. These requirements can be defined manually or extracted from structured documents and defined in a structured format.

The **Process Modeler** enables the *Process Manager* to define the processes in a Business Process Model and Annotation (BPMN) 2.0 standard format, defining who is responsible for the process, what requirements must be checked, and the data required to do so, what tasks and when must be performed and how they must be performed, either manually or automatically against and specific service.

The **Ontology Editor** supports the *Ontology Manager* to design the necessary semantic information model in form of ontology to represent the data to be shared in the DigiChecks Framework.

### Core Framework

The Core Framework is divided into the Orchestration, the User Interface, the User Management, the Data Space Management, the Vocabulary Provider, and the Federated Catalogue.

The **Orchestration**, which is a Business Process Model (BPM) Engine, is the core component in charge of managing the full process of turning a BPMN process in an executable version. It orchestrates and manages the state of the tasks required.

The **User Interface** offers to the *Permit Process Administrator* a user interface to manage and monitor the processes and workflows of the defined permitting processes. Also, provide specific forms and screens to enable the *Participant* to provide the necessary information for any step in the permitting process, be able to see at any time the status of the process, to provide manual inputs and get the final resolution approval or rejection.

The **User Management** enables administrators to manage the access of users to the different services that compose the DigiChecks framework.

The **Data Space Management** provides the services required to manage the DigiChecks Data Space. These are the Dynamic Attribute Provisioning Service (DAPS) and the Clearing House. The DAPS ensures trusted data sharing within the DigiChecks framework. The Clearing House provides a service to log data transactions. As they are part of the DigiChecks Data Space, they are further described in the following Section.

The **Vocabulary Provider** manages the semantic information model designed through the Ontology Editor to ensure interoperable data sharing within the DigiChecks Framework. As part of the DigiChecks Data Space, it is further described in the following Section.

The **Federated Catalogue** provisions a catalog of services that have been certified according to European guidelines of digital sovereignty. As part of the DigiChecks Data Space, it is further described in the following Section.

### **The Digital Twin**

The Digital Twin is composed of several services. Among others, the Compliance Checking, the Rule Editor, and the Interfaces with External Tools stand out. They are described below.

The **Compliance Checking** ensure the adherence of digital permitting processes to expert system rule-driven systems. It plays a crucial role in maintaining regulatory compliance and enforcing predefined rules and standards. By allowing operators to introduce and update rules, Compliance Checking empowers organizations to adapt their processes dynamically and stay aligned with evolving regulations.

The system leverages advanced algorithms and automation to evaluate the current state of the permitting process against the established rules. It constantly monitors and verifies whether the process complies with the required criteria, minimizing the risk of non-compliance and associated penalties. This automated approach significantly reduces the burden of manual

verification, enabling organizations to streamline their operations efficiently.

The **Rule Editor** enables *Rule Managers* to define, in an easy-to-use graphical interface, the rules to be executed by Compliance Checking services to validate compliance with specific requirements.

The **Interfaces with External Tools** integrate external third-party services, corporate tools, and data sources with the DigiChecks Framework through the DigiChecks Data Space. Within this category are the Data Trusted Gateway and Project Data. While the Data Trusted Gateway is a generic integration component, the Project Data is specific to manage the Common Data Environment (CDE) supporting the integration of Building Information Model (BIM) and Geographic Information System (GIS) data.

It should be mentioned that several external data sources are of interest for automating the management of building permits. Cadastre and Inspire Geoportal external databases are integrated in the DigiChecks Framework to provide Industry Foundation Classes (IFC) models and other relevant geographical information. Also, the Common Data Environment (CDE) is integrated into DigiChecks Framework to provide building data involved in the compliance checking services and to supply advanced visualization of the BIM models through external services and tools such as navigate on the building model pieces or parts, or by enriched 3D visualizations.

### **DigiChecks Data Space**

Based on the GAIA-X Technical Architecture 23.10 and the IDSA Reference Architecture Model 4.0, Figure 5 represents the DigiChecks Data Space. It can be divided into the technical components required for the role of the Core Participant and the role of the Intermediary that is provided in the DigiChecks Framework through the Data Space Management component within the Core Framework. These roles are described below.

#### **Intermediary**

Intermediaries act as trusted entities which assume a central role that creates benefit for Core Participants in the DigiChecks Data Space ensuring interoperability, providing trust, and creating new business models.

The technical components assigned to this category are the GAIA-X Digital Clearing House (GXDC), the Federated Catalogue, the DAPS, the Vocabulary Provider, and the Clearing House.

The **GXDC** operates and runs the services of the GAIA-X Framework. The GAIA-X Framework sets the rules that define whether organizations and the services they provide comply with European standards and values of digital sovereignty.

The services of the GXDC are operated by GAIA-X Federators. Therefore, they are not really provided within

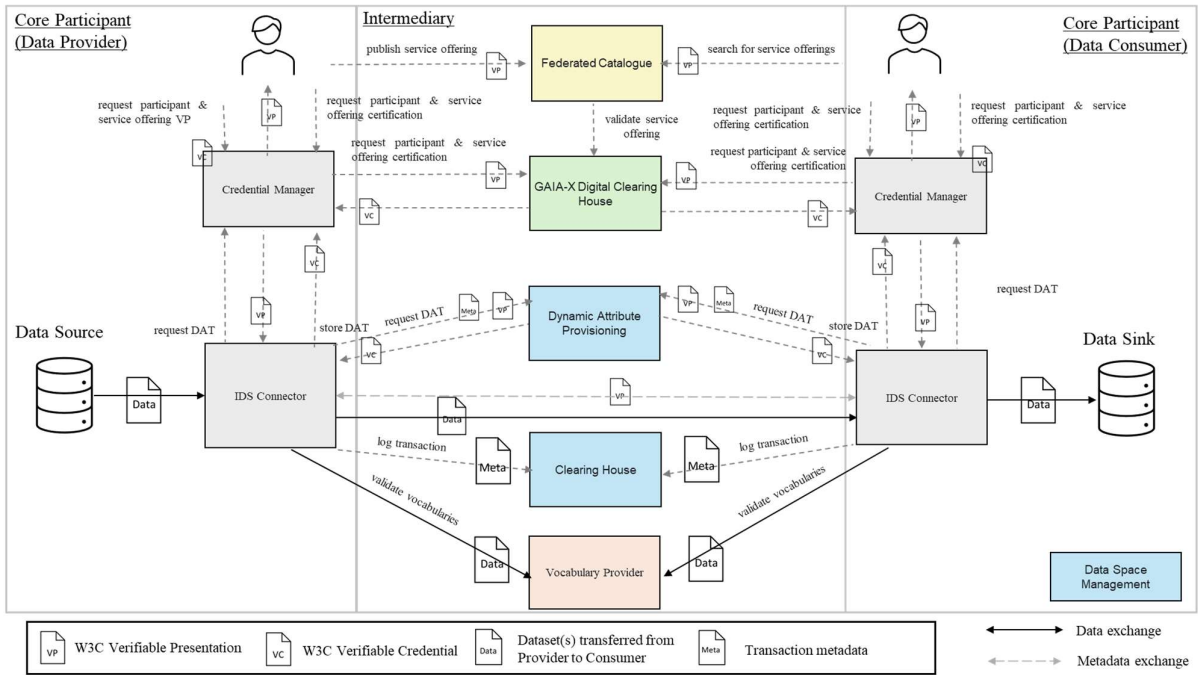


Figure 5: DigiChecks Data Space

the DigiChecks Data Space. These services are accessible to anyone to automatically verify compliance with the GAIA-X Trust Framework and obtain GAIA-X compliance attestations.

It is important to mention that the GXDCH relies on a user-centric and self-sovereign approach for identity management called Self-Sovereign Identity (Maier and Pohlmann, 2022) that is based on W3C recommendations of Decentralized Identifiers (DIDs)<sup>1</sup> and Verifiable Credentials (VC)<sup>2</sup>. Based on the information provided by Core Participants, the GXDCH verify compliance of either the organization or the services they provide with the GAIA-X Trust Framework. If satisfied, the GXDCH issues to the Core Participant a VC containing the GAIA-X compliance attestation. This VC is self-managed by the Core Participant. To enable other services to validate the integrity, the authenticity, and the validity of the issuer of the VC, the VC contains a cryptography proof.

The goal of the **Federated Catalogue** is to enable Core Participants within the DigiChecks Data Space to find best-matching service offerings, which comply with European standards and values of digital sovereignty.

To publish service offerings, the Federated Catalogue requests and validates VCs attesting compliance of the organization providing the service and the service itself with the GXDCH. To search for service offerings, it controls the access to the services available in the Federated Catalogue to organizations which comply with the GXDCH.

The **DAPS** sets the rules that define how an IDS Connector, the technical component of a Core Participant responsible for data sharing, manages data control. In other words, it states the level of trust of an IDS Connector. The IDS Connector is further described later.

As the trust level is higher, the requirements are higher, from a basic trust level where only interoperability is guaranteed, to higher levels that implement secure communication protocols, usage control etc.

As the level of trust can change in an operational environment over the time, once an IDS Connector is initially manually certified and deployed, the DAPS sets the operational trust level considering the one initially certified and operational environment data.

The DAPS, as the GXDCH, relies on DIDs and VCs. Therefore, it issues VCs that attest the trust level of an IDS Connector. This VC is self-managed by the Core Participant. It is used by the IDS Connector to access to other IDS Connectors.

The **Vocabulary Provider**, as part of the Data Space Management, hosts, maintains, and publishes the semantic information model that is designed using the Ontology Editor, describing the relevant concepts (e.g., “building”, “office space”, “toilet space” and “size”) shared by IDS Connectors in the DigiChecks Data Space to manage building permits in the construction domain. Furthermore, it implements Shapes Constraint Language

<sup>1</sup> [Decentralized Identifiers \(DIDs\) v1.0 \(w3.org\)](https://www.w3.org/TR/did-core/)

<sup>2</sup> [Verifiable Credentials Data Model v2.0 \(w3.org\)](https://www.w3.org/TR/2021/REC-vc-data-model-20210902/)

(SHACL)<sup>3</sup> validations that are required by the IDS Connector to verify whether the expected data is received. It is important to mention that the Vocabulary provider only includes the model. It does not include its instantiation (specific data) and therefore doesn't provide information about specific instances. The instances should be managed and provided by Core Participants through the IDS Connectors.

The **Clearing House**, as part of the Data Space Management, records all the relevant information related to data sharing between the IDS Connectors of Core Participants. This includes contract agreements and data usage information for clearing, settlement and billing services.

### Core Participant

A Core Participant can be assumed by any organization that provides or consumes data within the DigiChecks Data Space. Roles assigned to this category are the Data Provider and the Data Consumer.

To share data between the Data Provider and the Data Consumer, both uses a software component that is compliant with the IDSA RAM. This is the IDS Connector. To manage the VCs issued by the GXDCH and the DAPS, the Data Provider and the Data Consumer use a software component called Credential Manager.

The **IDS Connector** is the technical component responsible for interoperable, trusted, and sovereign data sharing between Core Participants within the DigiChecks Data Space.

To enable a modular and scalable development of the services, the DigiChecks framework is based on a microservices approach (De Lauretis, 2021). For a system that provides a specific service, while the user interface layer enables participants to manage the service itself, the IDS Connector provides those layers to share data within the DigiChecks Framework in an interoperable, trusted, and sovereign way. Figure 6 represents these system layers.

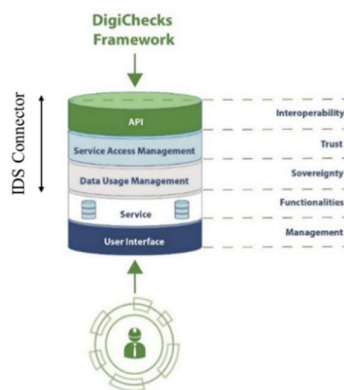


Figure 6: DigiChecks Framework Microservices System Layers

The Application Programming Interface (API), the Service Access Management and Data Usage Management layers are described below.

The API ensures interoperable data sharing. To this end, it implements the Dataspace protocol v1.0 (International Data Spaces Association, 2024) and several Data transfer protocols.

The Dataspace protocol is a set of specifications that define the interfaces, protocols, and schemas to expose a data catalog, to negotiate contracts and access negotiated data. To describe the data catalog, the Dataspace protocol proposes the Data Catalog Vocabulary (DCAT)<sup>4</sup>. It is a vocabulary designed to facilitate interoperability between data catalogs. It should be noted that DCAT is domain-agnostic. To provide a domain-specific description of the data, DCAT is extended with domain-specific vocabularies, which are provided by the Vocabulary Provider. Once negotiated data is accessed, data sharing is delegated to data transfer protocols.

Data transfer protocols are traditional protocols, such as HTTP or MQTT, that will be used for data transfer after data access. They are also integrated with the Vocabulary Provider. As the Vocabulary Provider implements SHACL validations, it can be ensured that the expected data is received.

The Service Access Management ensures trusted data sharing. It controls the access to the IDS Connector based on the VC that attests the level of trust of a requesting IDS Connector. For authentication purposes, it validates the integrity, the authenticity, and the validity of the issuer of the VC. For authorization purposes, it analyses the attributes of the VC.

The Data Usage Management ensures sovereign data sharing. Data sovereignty is referred as the self-determination of organizations regarding the usage of their data (Jarke et al., 2019). To grant data sovereignty, the IDS Connector implements Distributed Usage Control (Gil et al., 2023). It is a particularization of Usage Control for data sharing scenarios that extends Access Control to control what must happen to data through its life cycle (Jung and Dorr., 2022).

The **Credential Manager** abstracts Core Participants from the complexity of managing VCs.

On the one hand, it provides Core Participants with the interfaces to request the certification of the organization itself and the services it provides to the GXDCH, store the VC attesting the result and retrieve them.

On the other hand, it provides the IDS Connector with the interfaces to store retrieved VC from the DAPS and retrieve them for authentication purposes.

### Conclusions

This paper addresses the main challenges regarding the automated management of building permits. These are the lack of standards between regulations in different

<sup>3</sup> [Shapes Constraint Language \(SHACL\) \(w3.org\)](https://www.w3.org/)

<sup>4</sup> [Data Catalog Vocabulary \(DCAT\) - Version 3 \(w3.org\)](https://www.w3.org/)

countries and regions and municipalities, interoperability between data in different formats and the control of the data.

Considering the DigiPLACE RAF, which sets the common guidelines for building digital platforms for the construction sector, and with the aim of addressing the challenges identified, this paper presents the DigiChecks Framework, a novel approach to digitalize and automate building permit management that combines an orchestration of compliance checks and a data space. While the orchestration provides a modular and scalable approach to verify different compliance checks depending on existing regulations, the data space facilitates the collaboration between stakeholders through interoperable, trusted, and sovereign data sharing between their different platforms. Thus, the DigiChecks Framework reduces data sharing and compliance checking efforts, while it ensures strict compliance with existing regulations.

### Future Work

The conceptual architecture of the DigiChecks Data Space, which is the main development within the DigiChecks Framework and the focus of this paper, is based on existing standards defined by GAIA-X and IDSA. In this regard, the defined technical components are built from open-source tools that have already been developed following these standards or from new tools developed from scratch. The application of these tools to real-world scenarios presents two major challenges. First, as data spaces is a novel concept, these standards are continuously evolving. As the piloting stage approaches in the DigiChecks project, there is a need to make decisions on the versions of the standards to be used for two main purposes. For those tools already developed, to select the version to be used. For those new tools required, to select the version to be followed in the development. Second, different pilots lead to different requirements. Although existing tools are developed to be 100% agnostic to the use case requirements, the truth is that they should be adapted in about a 10% to the use case. This may lead to weaknesses in our approach that should be addressed by providing extensions to existing tools. For example, in the case of the IDS Connector, specific data transfer protocols may be required for the different pilots. If they are not implemented on existing tools, they must be implemented on top of an existing tool.

Having said that, at the end of the piloting phase, with the tools already selected and adapted, the DigiChecks Data Space technical architecture is expected to be published considering the version of the standards followed, the tools selected, the specific challenges addressed for their application in real-world scenarios and how they have been addressed.

### Acknowledgments

This work has received support from Horizon Europe project DigiChecks (Digital environment for management

of permits and compliance in building and construction) with grant agreement number 101058541.

### References

- Beach, T.H., Kasim, T., Li, H., Nisbet, N., Rezgui, Y. (2013). Towards Automated Compliance Checking in the Construction Industry.
- Bühler, M., Nübel, K., Jelinek, T., Riechert, D., Bauer, T., Schmid, T., and Schneider, M. (2023). Data cooperatives as catalyst for collaboration, data sharing and the digital transformation of the construction sector.
- David, A., Zarli, A., Mirarchi, C., Naville, N., Perisich, L. (2021). DigiPLACE: Towards a reference architecture framework for digital platforms in the EU construction, pages: 511-518
- De Lauretis, L. (2019). From monolithic architecture to microservices architecture. 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), pages 93–96.
- GAIA-X European Association for Data and Cloud (2023). GAIA-X Architecture Document 23.10.
- Gil, G., Arnaiz, A., Higuero, M. (2023). Advances in Sovereign Data Sharing: Identification and Assessment of the Main Features of Distributed Usage Control Solutions and Improvements in the Policy Quality.
- Gronlier, P., Hierro, J., and Steinbuss, S. (2021). Data Spaces Technical Convergence v2.0.
- International Data Spaces Association (2023). IDS Reference Architecture Model 4.0.
- International Data Spaces Association (2024): Dataspace protocol v1.0.
- Jarke, M., Otto, B., and Ram, S. (2019). Data sovereignty and data space ecosystems. *Bus Inf Syst Eng*, 61:549–550.
- Jung, C. and Dörr, J. (2022). *Data Usage Control*, pages 129–146. Springer International Publishing, Cham.
- Maier, B., Pohlmann, N. (2022). GAIA-X secure and trustworthy ecosystems with Self Sovereign Identity
- Nagel, L. and Lycklama, D. (2021). *Design Principles for Data Spaces*
- Rezgui, Y., Miles, J. (2011). *Harvesting and Managing Knowledge in Construction*.
- Rezgui, Y., Beach, T., & Rana, O. (2013). A governance approach for bim management across lifecycle and supply chains using mixed modes of information delivery.