

Article

NIKH-DS: A Network Provisioning Platform for Data Exchange in the Health Data Space [†]

Nikolaos Petroulakis ^{1,*}, Alexandros Kornilakis ¹, Panos Chatziadam ¹, Vasileios Theodorou ²,
Nicolas Louca ³, Stefanos Fafalios ⁴, Petros Zervoudakis ^{1,5,‡}, Dimitrios Laskaratos ^{2,6,§},
Maria Eleftheria Vlontzou ^{2,7,§} and Eleni Zarogianni ²

¹ Institute of Computer Science, Foundation for Research and Technology-Hellas (FORTH-ICS), 70013 Heraklion, Greece; kornilak@ics.forth.gr (A.K.); panosc@ics.forth.gr (P.C.); petros.zervoudakis@netcompany.com (P.Z.)

² Intracom Telecom, 19002 Peania, Greece; theovas@intracom-telecom.com (V.T.); laskaratosd@iconplatforms.com (D.L.); mvlontzou@mail.ntua.gr (M.E.V.); ezarog@intracom-telecom.com (E.Z.);

³ eBOS Technologies Limited, Nicosia 2322, Cyprus; nicolasl@ebos.com.cy

⁴ Sphynx Analytics Limited, Nicosia 2012, Cyprus; s.fafalios@sphynx.ch

⁵ Netcompany, 15125 Maroussi, Greece

⁶ Icon Platforms SA, 14235 Filothei, Greece

⁷ Faculty of Electrical and Computer Engineering, National Technical University of Athens, 10682 Athens, Greece

* Correspondence: npetro@ics.forth.gr

[†] This article is a revised and expanded version of a paper entitled “Towards the Development of a Network Provisioning Platform for Data Exchange in the Health Data Space,” which was presented at the IEEE Conference on Standards for Communications and Networking (CSCN), Belgrade, Serbia, 2024.

[‡] Contributed while affiliated with FORTH-ICS.

[§] Contributed while affiliated with Intracom Telecom.

Abstract

Secure and trustworthy data exchange across distributed data sources remains a major challenge in the health domain, where strict legal, regulatory, and privacy requirements must be satisfied. Data space technologies provide a promising approach to enabling interoperable and sovereign data sharing among diverse stakeholders while preserving data ownership and regulatory compliance. The NextGEM Innovation and Knowledge Hub (NIKH) was developed as a collaborative ecosystem for FAIR data access and evidence-based health risk assessment. This paper describes the NIKH Data Space (NIKH-DS), the underlying network provisioning platform within NIKH that enables secure data exchange in a health data space environment. The work outlines the key requirements, intended uses, and core implemented functionalities necessary for enabling secure network-provisioned data sharing among distributed data locations. Based on these requirements, a prototype architectural framework is proposed that integrates secure networking and interoperable services. The implementation of the individual components is described, including the data space controller, access control mechanisms, and a user-oriented dashboard that enables data visualization and interaction with distributed data sources. The NIKH-DS platform is validated through a set of case studies that demonstrate the feasibility and effectiveness of the platform in supporting secure, interoperable, and Findable, Accessible, Interoperable and Reusable (FAIR)-compliant health data sharing and risk assessment for the investigation of potential health effects of radio-frequency electromagnetic fields (EMF).

Keywords: data space; network provisioning; data sharing; security and sovereignty; health domain; distributed data systems; FAIR; EMF



Academic Editor: Pingyi Fan

Received: 31 March 2026

Revised: 16 June 2026

Accepted: 18 June 2026

Published: 29 June 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons](#)

[Attribution \(CC BY\)](#) license.

1. Introduction

The rapid expansion of digital technologies and the continuous growth in data generation have increased the need for secure and efficient mechanisms for data exchange, particularly in sensitive domains such as environmental health. As data volume and heterogeneity increase, robust frameworks are required to enable stakeholders to share, access, and utilize information while ensuring strong guarantees of security, privacy, and regulatory compliance. Data spaces have emerged as a key paradigm for addressing these challenges by enabling trusted collaboration between various actors, including data providers, research institutions, and technology developers. By supporting interoperability and the integration of heterogeneous systems, data space ecosystems facilitate seamless data exchange across organizational boundaries while preserving data ownership and control. Through well-defined governance mechanisms, data owners can specify and enforce access rights and usage conditions, ensuring data sovereignty and controlled data utilization.

In alignment with this vision, the European data strategy aims to establish a unified data market that improves global competitiveness and strengthens data sovereignty in Europe [1]. A central pillar of this strategy is the development of Common European Data Spaces, designed to enable reliable data exchange, access, and reuse across sectors and national boundaries [2]. These data spaces are based on principles of interoperability, standardization, and federated governance, supported by shared infrastructures and common semantic models. Their implementation is closely linked to emerging regulatory frameworks, including the Data Governance Act and the forthcoming Data Act, which promote secure and Findable, Accessible, Interoperable, and Reusable (FAIR) data sharing while ensuring compliance with the General Data Protection Regulation (GDPR). In this context, concepts such as data sovereignty and data stewardship are fundamental, emphasizing the ability of individuals and organizations to maintain control over their data. Within this ecosystem, the European Health Data Space (EHDS) represents a major sector-specific initiative aimed at enabling the secure and seamless exchange of health data throughout the European Union [3]. It supports both primary use, such as patient care, and secondary use, including research, innovation, and policy-making, with the potential to improve cross-border healthcare, enable large-scale data analytics, and accelerate data-driven and AI-based healthcare solutions. At the same time, it imposes strict requirements for privacy, security, and ethical data use, necessitating the adoption of advanced protection mechanisms such as anonymization, pseudonymization, and secure data processing environments.

In this context, the NextGEM project [4] provides a framework for the generation of scientific knowledge relevant to health in emerging scenarios of exposure to electromagnetic fields (EMF) across multiple frequency bands, with the aim of ensuring the safety of EU citizens by promoting a healthy living and working environment. One of its key outcomes is the NextGEM Innovation and Knowledge Hub (NIKH), which establishes a collaborative knowledge hub offering a standardized approach for European regulatory authorities, citizens and the scientific community to explore and assess project results and access FAIR data for evidence-based risk assessment. To achieve this objective, NIKH explores scalable and secure data sharing across distributed storage locations within the health data space through the development of the NIKH Data Space (NIKH-DS) mechanisms. Building on these developments, this article presents NIKH-DS, a network provisioning platform designed to support secure, interoperable, and scalable data exchange within the health data space for knowledge sharing and risk assessment based on distributed data sources. This work extends our previous study [5], which introduced the initial design of NIKH-DS, and presents the following main contributions:

- Design and development of a data space-enabled platform that supports reliable and secure data management and data exchange in the health domain across distributed storage locations through robust network provisioning and fine-grained access control mechanisms, while adhering to FAIR data principles.
- Provision of a user-oriented dashboard that facilitates data visualization, exploration, and analysis, enabling stakeholders to interact effectively with distributed data sources and derive actionable insights.
- Deployment and operational validation of the NIKH-DS platform through three realistic case studies on potential health effects related to electromagnetic field (EMF) exposure, as generated within the NextGEM project, demonstrating its applicability for data exchange and risk assessment tasks in a real-world health data-sharing environment.

The remainder of this paper is organized as follows. Section 2 reviews the background of data space paradigms, as well as existing initiatives and data-sharing architectures. Section 3 presents the design of the NIKH architectural framework and its services. Section 4 proposes a set of data space services to enhance flexibility and scalability for different user needs. Section 5 describes the development of NIKH-DS, a network provisioning platform for secure and interoperable data exchange in the health data space. Section 6 presents the development of the NIKH-DS dashboard as a user-friendly platform to incorporate robust access control and front-end mechanisms. Section 7 evaluates the platform through real-world case studies. Finally, Section 8 concludes the paper and outlines future directions.

2. Background of Data Space Paradigms

The design of efficient data management and sharing infrastructures has become a key research challenge in data-intensive domains. In particular, the need to handle heterogeneous data sources while ensuring secure and controlled access has driven the evolution of modern data architectures. This section reviews existing approaches that address these challenges, focusing on data lake architectures and data space paradigms.

2.1. Data-Driven Architectures and Platforms

Modern data-driven architectures and platforms have emerged to support the integration, sharing, governance, and analysis of heterogeneous data across domains. Among these approaches, data lakes have become one of the most widely adopted architectures for centralized data storage and processing. A data lake enables the storage of structured, semi-structured, and unstructured data in their native formats, following a schema-on-read paradigm that provides flexibility for future data exploration and analytics. Key principles of data lakes include scalable storage, metadata-driven discovery, data governance mechanisms, and support for heterogeneous data ingestion from multiple sources. These characteristics make data lakes particularly suitable for data-intensive environments where large volumes of diverse data must be collected, managed, and analyzed efficiently.

Data lake architectures have been proposed to facilitate the ingestion, storage, and sharing of heterogeneous data, allowing users to explore and analyze data [6]. The authors in [7] introduce a platform designed to address the need to share heterogeneous scientific data related to environmental research. The platform employs an on-premise solution based on the data lake concept to provide cloud services with both institutional authentication and open data access, deploying a catalog service to make data findable through metadata in accordance with data governance standards. In [8], the authors propose HEALER, a data lake architecture that performs data ingestion, storage, and access with the aim of providing a centralized repository for heterogeneous health data.

However, traditional data sharing platforms typically rely on centralized architectures that act as authoritative third parties for transactions and must therefore be trusted by all participants in the sharing process. To address trust and transparency concerns, some studies have proposed replacing centralized architectures with blockchain-based solutions that provide decentralization, immutability, and auditability. For example, the authors in [9] propose a blockchain-based solution that improves data access control by enabling data owners to specify access policies and achieve fine-grained control over data usage. Despite the promising features of blockchain and smart contract-based solutions for securing sensitive data, these technologies still face challenges that limit their extensive use in data sharing scenarios, particularly with respect to scalability [10]. Blockchain networks may struggle with throughput, storage, and networking constraints, and as the number of participants increases, the management overhead of the distributed ledger grows significantly. Nevertheless, the above solutions do not fully ensure a data-sharing model that simultaneously achieves security, interoperability, and sovereign data exchange while maintaining data ownership at the source.

2.2. Data Space-Related Works

To overcome the challenges of trust, interoperability, data sovereignty, and scalability in existing data-sharing solutions, the data space paradigm has emerged as a suitable structured and shared environment in which different organizations or systems can store, exchange, and access data across a network of users and platforms in a secure and interoperable manner. More specifically, data space acts as a decentralized framework for secure, sovereign and interoperable data sharing across organizations, allowing data owners to retain control while enabling trusted exchange under shared governance and standardized interfaces [11]. Unlike traditional centralized systems such as data lakes or warehouses, data spaces support discovering, negotiating, and using data without renegotiating ownership, making them particularly valuable for cross-sector collaboration in areas such as healthcare, manufacturing, mobility, and energy [12]. They rely on distributed architectures, semantic interoperability, usage policies, identity verification, and connectors that enforce the agreed-upon rules, focusing on data sovereignty, trust, and interoperability [13]. Recent research work on data space technologies has also explored digital platforms and governance frameworks to support controlled data sharing among multiple stakeholders. The authors in [14] propose a data management plan for a digital platform that integrates open and restricted data to allow data exchange between regional stakeholders, highlighting the lack of standardized concepts in data management and demonstrating how such platforms can support long-term data strategies and data-driven innovation. In [15], the authors conceptualize data spaces as distributed infrastructures supported by governance frameworks that allow trusted and sovereign data sharing between organizations. Therefore, a data space platform can serve as a key element in enabling accessible and interoperable data sharing across multiple domains, highlighting the need for further research and development efforts to design user-centric solutions that support secure, sovereign and efficient data utilization.

2.3. Core Principles and Enabling Services in Data Space Ecosystems

Data space ecosystems enable secure and trusted collaboration among distributed participants who retain control over their own data while adhering to common principles, rules, and standards. Within such environments, data or services are shared as assets through connectors, forming the fundamental units of data exchange that can be discovered by users along with their associated metadata, descriptions, providers, and data types. Access to these assets is governed by contract offers that define obligations and permissions,

which may lead to formal contract agreements following negotiation between participating parties. To ensure proper governance and operational management, data spaces incorporate mechanisms for participant management, premises monitoring and discovery, and policy definition and enforcement, allowing users to define and manage usage rules in compliance with data governance and data sovereignty requirements. Integration and data exchange across heterogeneous platforms are further enabled by dedicated data space connectors that enable seamless interaction between data providers, data consumers, and supporting services such as identity management components, including certificate authorities and participant information services, which ensure secure authentication and authorization. Widely adopted implementations include the International Data Spaces Connector (IDS) Connector [16], based on the IDS Information Model and standardized messaging services, and the Eclipse Data Space Connector (EDC) [17], an open-source and modular framework that supports sovereign inter-organizational data sharing through flexible protocols and a clear separation between control and data planes to enhance scalability and interoperability, while comprehensive surveys of available connector technologies are presented in [18].

2.4. Data Space Initiatives and Projects

Several initiatives, projects, and associations actively promote the adoption of data space principles and technologies across different sectors. The International Data Spaces Association (IDSA) [19] advocates the development of virtual data-sharing environments based on established standards, technologies, and governance models, which contribute to secure and reliable data exchange in digital transformation. Similarly, the GAIA-X European initiative focuses on building a federated and secure data infrastructure at the European level [20]. In the healthcare domain, the proposed EHDS framework defines mechanisms that allow citizens to access and share personal health data while enabling secondary use of data for research and innovation, emphasizing privacy, data sovereignty, and secure processing environments in accordance with regulatory requirements such as Article 50 of the EHDS proposal [21]. Recent projects such as Health-X dataLOFT [22] and HealthData@EU [23] further demonstrate the transition to federated and interoperable health data infrastructures, while IMPaCT-Data [24] identifies essential security measures to support compliant electronic health record exchange and data-driven precision healthcare under GDPR constraints. Beyond healthcare, sector-specific data space initiatives have also emerged, including Catena-X [25] for secure data exchange in the automotive industry, EONA-X [26] for mobility, transport and tourism, and the Omega-X project for the development of an energy data space based on GAIA-X and IDSA principles. Additionally, the Copernicus Data Space Ecosystem [27] has been established to manage and disseminate large-scale environmental data, illustrating the broad adoption of federated and interoperable data infrastructures in multiple domains. These initiatives collectively demonstrate the growing maturity of data space ecosystems and highlight the need for continued research and development of domain-specific data space platforms capable of ensuring trustworthy, sovereign, and user-accessible data exchange, particularly in sensitive sectors such as healthcare. In this context, projects such as NextGEM [4] highlight the growing role of data space technologies as key enablers of secure and interoperable health data exchange across domains, underscoring the need for continued research and development of scalable and user-accessible data space platforms, such as the proposed NIKH framework.

3. Design of NIKH Architectural Framework

NIKH is a collaborative framework designed to support knowledge and data exchange among relevant stakeholders. It acts as a central hub that facilitates research on exposure

to electromagnetic fields (EMF) and potential health effects while fostering collaboration and knowledge sharing between scientists, authorities, and policy makers involved in maintaining compliance with safety standards, performing risk assessments and increasing citizens awareness of EMF and health-related research [28]. As can be seen in Figure 1, the NIKH architecture is organized into three main layers, Application, Service, and Infrastructure, with a clear separation between them. The architecture also includes a Local Premises Layer, which represents a vertical layer responsible for managing infrastructure, storage, and application functionalities within local environments. In the following sections, an overview of the NIKH component architecture is provided by describing the functionalities envisioned for each layer and their interconnections with other architectural components, and outlines the procedures followed for the development of each component.

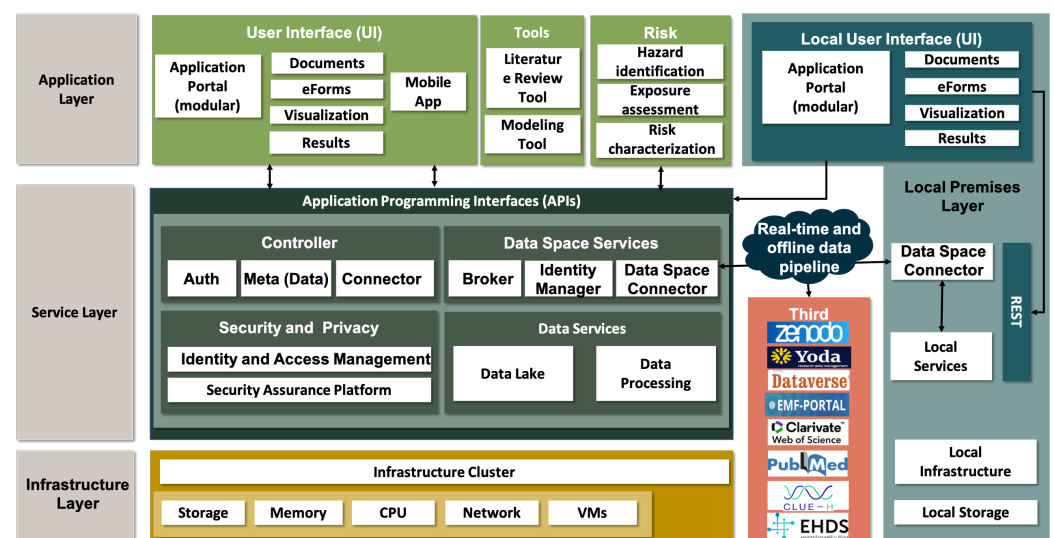


Figure 1. Conceptual architecture of the NIKH framework.

3.1. Application Layer

The Application Layer provides the interface through which users interact with NIKH and its components based on their access rights. It is the user-facing layer that offers direct access to services and tools through web and mobile interfaces, enabling intuitive interaction with the components of the platform. Users interact with the application portal via a graphical user interface (GUI), which functions as an access-controlled dynamic application connected to NIKH services. It provides a unified entry point into the data space ecosystem, supporting role-based access control, configurable dashboards, and visualization. Several applications are integrated into the NIKH architecture, including awareness hub, data exchange, literature search, risk assessment, and modeling functionalities, which leverage the underlying data space capabilities of the platform.

3.2. Service Layer

The Service Layer includes all services that enable the core functionalities of the NIKH framework, such as authentication and access control, data ingestion, data exchange, data storage, and efficient inter-component communication and workflow orchestration among system components. At the core of the Service Layer, the Controller acts as the central gateway, handling application programming interfaces (APIs), authentication, request routing, and secure communication while maintaining the metadata catalog. In addition, data space services enable secure and controlled data exchange by keeping data at the source and sharing it only upon authorized request. Data services can manage data ingestion, storage, processing, and analytics using a data lake as a scalable central repository.

Finally, security and privacy components include identity and access management for authentication and access control, along with a security assurance that continuously monitors risks and detects potential threats in compliance with security standards.

3.3. Infrastructure Layer

The Infrastructure Layer forms the foundation of the framework, comprising physical and virtual components that together deliver high performance, reliability, and security. The physical infrastructure has been designed to meet demanding technical requirements, including main servers, storage systems, and internal and external network connections selected to provide robust computing power, sufficient storage capacity, and high availability for platform applications and services. Complementing the physical infrastructure, the virtual infrastructure enables the platform to operate multiple fully isolated virtual machines (VMs) through a hypervisor layer that manages their creation and operation. This design ensures redundancy, minimized downtime, incremental backups, and built-in security through integrated firewalls, security groups, and IP management mechanisms. These VMs host key components such as the controller, data space services, application portal, risk assessment tool, security, and access control mechanisms. In addition, the infrastructure supports containerized services through virtualized environments, which abstracts the underlying virtual infrastructure and enables scalable, flexible, and efficient service orchestration.

4. Data Space Services in the NIKH-DS

NIKH supports several services and tools, where one of the most important is the NIKH Data Space (NIKH-DS) platform which includes configurations and deployment mechanisms for secure data exchange within the health data space. Through data space services and the integration of data space standards and protocols, NIKH-DS enables data to remain decentralized, transferring only upon request. It incorporates mechanisms for premises identity validation, data usage restrictions, and metadata cataloging. In this context, the decoupling of the connector from data storage within the data space architecture introduces a versatile approach that provides distinct solutions, called as as-a-Service (Figure 2). This conceptual separation is designed to offer organizations and stakeholders enhanced flexibility and scalability, allowing them to tailor data management strategies to their specific needs through four distinct services: Data-as-a-Service, Connector-as-a-Service, Premises-as-a-Service, and Data-Space-as-a-Service, as detailed below.

4.1. Data-as-a-Service (DaaS) for Data Space Members

Data-as-a-Service (DaaS) provides end-users and organizations with a comprehensive solution for accessing data resources within a data space ecosystem. A set of web interfaces allows users to seamlessly interact with data space functionalities through a secure, permission-based platform, supporting workflows for efficient data retrieval and metadata management. Robust authentication, authorization, and permission controls ensure secure access, keeping sensitive information protected while allowing users to customize and control access to their data. A Member is any registered and authorized user on the NIKH-DS platform, with access capabilities determined by predefined permissions. The DaaS model enables seamless data access for Members, eliminating the need for on-premises infrastructure or dedicated connectors. Members are registered via the access control mechanism to gain access to the available data through the NIKH controller. Access is granted through the central data space connector, which aggregates the requested data from all network participants in compliance with data space protocols. This setup provides streamlined access without requiring additional data storage while ensuring high availability, scalability, and reliable access for Members.

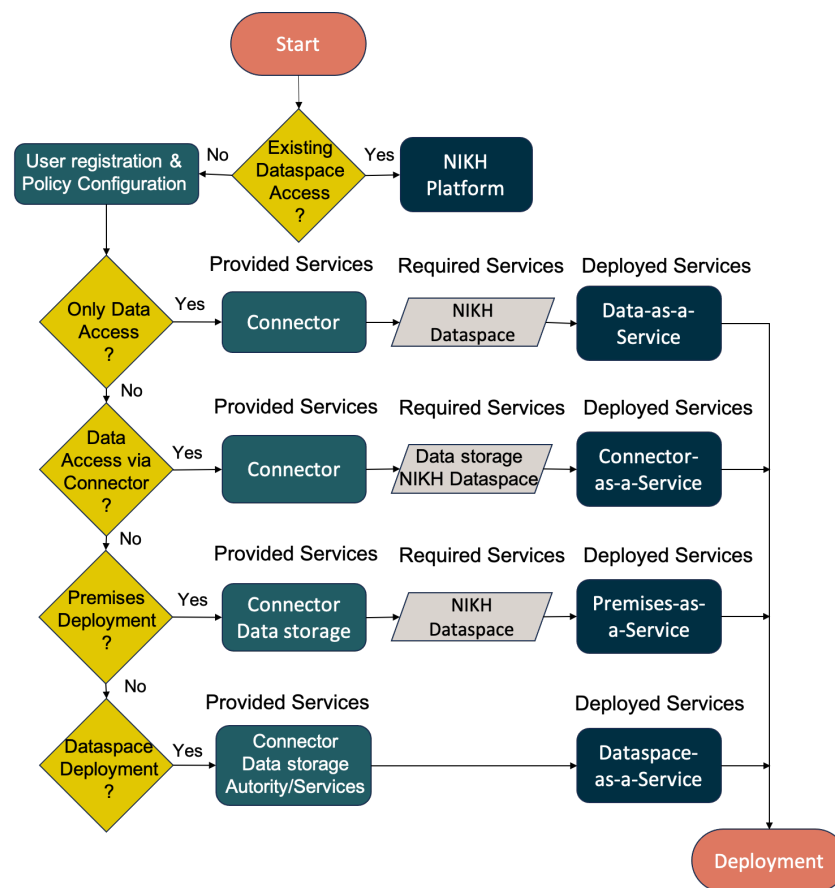


Figure 2. NIKH data space 'As-a-Service' usage scenarios.

4.2. Connector-as-a-Service (CaaS) for Local Premises

Connector-as-a-Service (CaaS) enables seamless data exchange capabilities among entities within the data space ecosystem. Using data space connectors, end-users can explore and retrieve heterogeneous data across the ecosystem. CaaS provides data space connectors to facilitate collaboration between users, allowing data sharing without switching between different tools or platforms. The local premises infrastructure ensures the protection of sensitive data, supporting secure data transfer and sharing among partners. Stakeholders maintain control over their data while fostering efficient collaboration. In alignment with the proposed architecture, the CaaS model deploys a dedicated container running the data space connector, along with additional containers running authority services pre-deployed to support local premises needs. A storage service within the local infrastructure enables persistent storage of scientific data. Consequently, this model requires sufficient storage capabilities on-premises, while data availability, scalability, and reliability depend on both the local infrastructure and the NIKH-DS platform. Data isolation ensures proper data governance, as organizations retain full control over their data.

4.3. Premises-as-a-Service (PaaS) for Local Premises with Limited Resources

Premises-as-a-Service (PaaS) provides stakeholders and organizations with virtual premises, including reliable storage connected to the data space ecosystem. The PaaS solution offers participants benefits such as seamless scalability, high availability, and secure storage, eliminating the need for local resources. Participants can confidently store, manage, and access data assets, assured that their data is securely hosted by a trusted service provider. The limited local premises utilize a shared pool of resources to deploy a dedicated connector and necessary services for data collection and transfer, including an object storage service. This approach ensures secure data storage within NIKH-DS. In

line with the proposed architecture, the PaaS model deploys a dedicated container running the data space connector and essential services, such as authority services and shared object storage, already hosted on NIKH-DS. This model does not require individual storage capabilities, as the platform ensures high availability, scalability, and reliable data access. However, centralized data storage affects data governance, as organizations do not retain full control over their data.

4.4. Data-Space-as-a-Service (DSaaS) for External Data Space Ecosystems

Data-Space-as-a-Service (DSaaS) leverages the advantages of the data space ecosystem by providing a fully managed environment tailored to specific needs, with a centralized authority maintaining control over the data space. DSaaS streamlines the setup, enabling innovation and collaboration within the newly created ecosystem. The authority ensures compliance with local regulations, transparency standards, and cybersecurity protocols. DSaaS allows for the creation of an external data space ecosystem according to the needs of participating entities. The service provider can replicate the proposed platform, including the Kubernetes cluster, controller, authority services, premises, storage, and connectors based on stakeholder requirements. This approach enables NIKH-DS to be deployed centrally or remotely, supporting a fully functional data space ecosystem. Finally, Table 1 summarizes and compares the capabilities and functionalities of the various services, highlighting the operational readiness and adaptability of the proposed solution. The reported characteristics provide a qualitative comparison of the deployment models and reflect relative operational characteristics rather than quantitative performance metrics.

Table 1. NIKH data space services.

Service	Description	Storage	Availability/ Reliability	Scalability	Data Governance	Isolation
Data as a service	Members	-	High	High	No	-
Connector as a service	Local premises	Moderate *	Moderate *	Moderate *	No	Physical
Premises as a service	Limited local premises	Limited	High	High	No	Virtual
Data Space as a service	External data space	Moderate **	High **	High **	Yes	Virtual/ Physical

* Depends on local premises capabilities. ** Depends on external data space capabilities. Availability/Reliability: High indicates that the functionality is primarily supported by centrally managed NIKH-DS infrastructure; Moderate indicates dependence on both NIKH-DS and local premises capabilities. Scalability follows the same qualitative interpretation. The reported characteristics provide a relative qualitative comparison of the deployment models and are not intended as quantitative performance metrics.

5. Development of the NIKH-DS Platform

The NIKH-DS platform establishes a comprehensive framework that enables secure and sovereign information exchange between participants through well-defined data ownership and distribution policies. To support this, a range of components and applications have been implemented to integrate the various services and data required for a unified prototype platform where multiple standards and protocols are applied. Specifically, to establish a functional data space ecosystem, NIKH-DS incorporates the following functionalities: (i) data space connectors, (ii) service orchestration, (iii) access control, and (iv) reliable data lake services. All main components are encapsulated within a container orchestration system and deployed independently as Docker containers. The containerized NIKH-DS components are orchestrated using Kubernetes with appropriate configuration files (Kubernetes deployment YAMLS). Figure 3 illustrates the workflow of data space components within the NIKH-DS platform under the different as-a-Service

models, as described in Section 4. More specifically, as shown in the figure, DaaS provides registered users with access to data through the controller's DS connector. CaaS enables data exchange for users hosting a DS connector on their local premises. PaaS offers a virtual environment for storing and exchanging data within the same DS. Finally, DSaaS delivers a complete dataspace ecosystem by replicating the proposed platform, including all required services and functionalities, according to users' needs.

In the following subsections, the implementation details of the individual data space functionalities are presented.

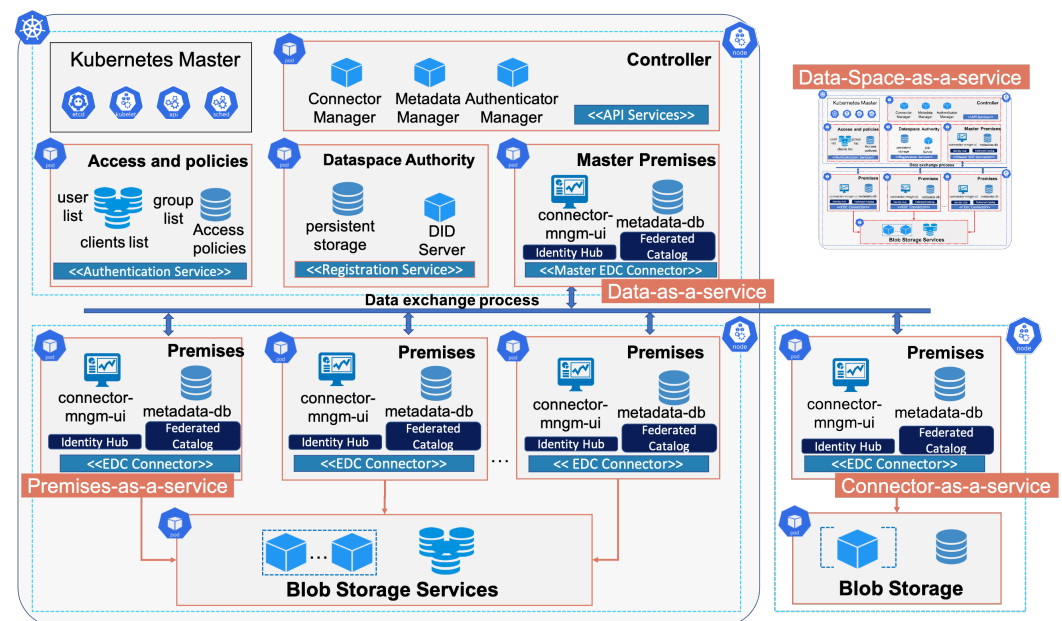


Figure 3. Deployment of the NIKH-DS platform.

5.1. Data Space Connectors and Services Deployment

Data space services in NIKH-DS enable controlled, sovereign, and secure data exchange through the deployment and registration of Data Space Connectors. The setup includes several supporting services and interoperable components such as a connector runtime, identity and trust services, a federated catalog for data discovery, and policy/contract negotiation mechanisms. These components enable secure and efficient data exchange between participants in the NIKH-DS. The implementation is based on the open-source EDC deployed with the Eclipse Minimum Viable Data Space (MVD) [29], which serves as reference connectors demonstrating interoperable data exchange in a minimal standards-compliant data space. The EDC provides a RESTful API interface that allows applications to interact with the data space, enabling interoperability, resource management, and exchange between connectors (e.g., assets, contracts, policies, and data transfers). A Federated Catalog Service in the EDC provides data catalog functions while ensuring data sovereignty, availability, and scalability by listing all participants' contract offers. It consists of the Federated Catalog Node, which handles catalog cache requests, and the Federated Catalog Crawler, which periodically crawls and caches catalogs in trusted relationships. This allows for the retrieval of all contract offers from participating provider connectors, enabling decentralized catalog configuration. The Data Space Authority Services include a registration service for managing participants, facilitating onboarding, and providing a catalog of all participants. The interface supports adding new participants and listing existing ones stored in the registration service database. Additionally, an Identity Hub acts as a credential repository, enabling secure delivery of verifiable credentials from a data space issuer to participants. Each participant's self-description document, including

information about their data space connector, can be retrieved using the Identity Hub API. Finally, object storage is provided through Azurite [30], an Azure Storage Emulator that supports blob and file storage for local development. Azurite ensures that data remains under the control of the data owner while replicating Azure Blob Storage functionalities for reliable object storage. Finally, the NIKH-DS architecture follows a federated data-sharing model in which data remain under the control of participating premises and are not centralized within the Controller, while selected coordination and management services are centrally deployed to simplify administration and governance.

5.2. Implementation of the NIKH-DS Controller and Interconnection with the Data Space Ecosystem

The Controller is developed to orchestrate and manage incoming requests through three core services: Authentication Manager, Metadata Manager, and Connector Manager. The Authentication Manager handles user management, authentication, authorization, resource access based on user tokens, secure communication with external data providers, and metadata catalog maintenance. The Metadata Manager oversees the full lifecycle of resource metadata, including creation, modification, deletion, and retrieval, while enabling extraction and registration via APIs for internal and external sources. The Connector Manager acts as a middleware layer, enabling integration and interaction between data storage environments and the platform. It supports file sharing, policy, contract, and asset management through RESTful APIs that interact with EDC APIs, initiate asset and contract negotiations, and manage data transfers once a participant's connector is registered. All controller services are containerized and managed within Kubernetes, with external access provided via NGINX as a reverse proxy. Container images are automatically built using GitLab CI based on Dockerfiles and Docker Compose files provided by component owners. Although the Controller acts as a central coordination component, the underlying data assets remain distributed across participating premises and connectors. Consequently, the Controller does not constitute a single point of failure for stored data.

5.3. Access Control Management

To enforce access control policies in NIKH-DS, a unified Identity and Access Management (IAM) system manages user registration, login, and role-based access. Keycloak [31] is deployed to enhance EDC access policies, providing authentication, authorization, and user management with customizable roles, groups, and permissions. It runs as a container within the Kubernetes cluster and communicates with platform services via RESTful APIs. Keycloak uses a PostgreSQL database to store user, role, and group information, with resources defined within specific realms. New users register through a defined process, gaining access to the platform with assigned roles: simple members (search/view data), full members (create/edit assets, policies, contracts), administrators (full operational rights including registration approvals), and super admins (Keycloak-specific platform-wide configuration). Authentication of platform components is handled via client resources, ensuring that only trusted applications can interact with Keycloak using client secrets embedded in their Spring Boot configurations. This deployment provides a centralized and secure authentication and authorization framework for NIKH-DS services. While EDC supports decentralized trust mechanisms through verifiable credentials and Identity Hub services for participant-level trust establishment (data space connectors), end-user authentication and authorization are centrally administered through Keycloak, enabling controlled access to the platform, user interface, and associated services.

5.4. Data Lake Services of the Controller

Data lake services in NIKH-DS handle data ingestion, storage, and processing, serving as a central repository capable of storing structured, semi-structured, and unstructured data at any scale. Each dataset is associated with identifiers and metadata to enable fast retrieval. Following a schema-on-read approach and automated workflows, transformations are deferred until analysis, supporting analytics, database queries, big data processing, full-text search, real-time analytics, and machine learning. MongoDB was chosen for the data lake due to its flexible JSON-based storage, which is more versatile than traditional RDBMS (Relational Database Management System). The database stores metadata describing assets (research files, datasets, etc.) and administrative data such as registration requests. Metadata fields are centrally stored, while raw data may undergo basic preprocessing. MongoDB organizes data into four collections (Metadata, Connector, Registration, and Field), analogous to tables in relational databases. It also stores backend data essential for platform operation, such as registration requests and connector access information. MongoDB is deployed as a container within the Kubernetes cluster using a deployment descriptor specifying the necessary fields for successful deployment.

5.5. Reliability of the Data Space Ecosystem

To improve service availability and prevent data loss, the controller implements a backup and recovery mechanism for assets, policies, and contracts. During testing, the absence of permanent storage in the connectors revealed potential data loss after failure. A dual storage approach was implemented using MongoDB and native file storage (NFS). Controller metadata are persistently stored in MongoDB, while daily backups are maintained for both the Controller container and its associated data to support service recovery and continuity. MongoDB stores assets, policies, and contracts in the original format to avoid transformation errors during recovery. Simultaneously, an NFS volume mounted on the Connector Manager pod stores copies of files attached to assets, ensuring a backup of files normally stored in Azurite. Recovery can be triggered through the data space connector-recover interface, either for a specific organization or for all organizations. The process sequentially recreates assets, restores files from NFS to Azurite, and reinstates contracts and policies from MongoDB. After completion, the Connector Manager generates a recovery report, where a 409 code indicates that all assets, contracts and policies are recovered in the connector.

6. NIKH-DS Dashboard

The large number of available data sources and users required the development of a module capable of integrating, accessing, and acquiring data from these sources. In this context, the NIKH-DS dashboard (Figure 4a) is developed as a robust data management system, allowing users to view metadata and upload new data assets to the platform, thereby providing access to the data space ecosystem (Figure 4b). The dashboard provides a user-friendly interface that enables users to explore and analyze data from different providers in a unified manner, facilitating seamless data exploration for a holistic view. This section presents the implementation of the NIKH-DS dashboard for accessing and managing distributed premises and data exchanged.

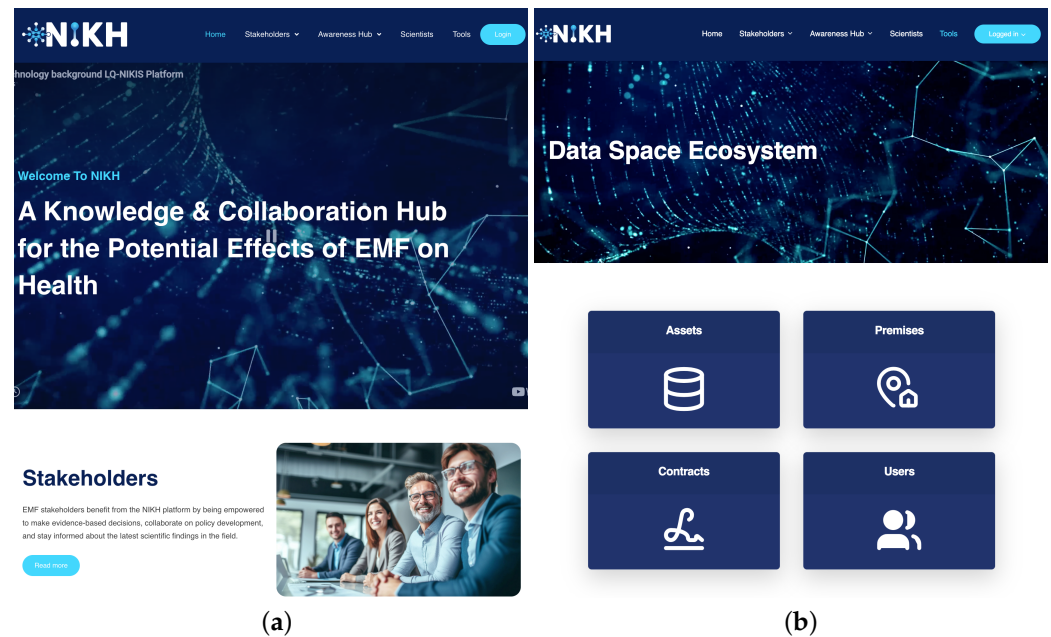


Figure 4. NIKH-DS dashboard: (a) welcome page; (b) data space functions.

6.1. Development of the Graphical User Interface of NIKH-DS

The NIKH-DS dashboard provides a flexible and efficient interface to connect diverse digital infrastructures across physical and virtual remote locations, enabling multiple systems to interconnect within a tightly integrated data space ecosystem. It is built as a custom web application using React.js (v19.2.4) for the front end and Node.js (v24.13.0) for server-side execution. The dashboard comprises a variety of React components, some representing pages through file-based routing in the Next.js (v16.2.2) framework, and others forming elements of the graphical interface. Next.js is leveraged to enable Server-Side Rendering for seamless component rendering on the server and Static Site Generation for faster page loads and improved performance. Although the graphical interface does not expose APIs directly, it communicates with the Controller's APIs through the relevant controller managers, providing a unified interface that transforms collected data into intuitive and presentable structures. The dashboard is available to authorized NIKH-DS subscribers, including organization members within the data space ecosystem and external consumers seeking posted data. It enforces strict authentication and authorization to ensure data security, access control, personalization, accountability, and confidentiality. Users log in through a single sign-on system managed by Keycloak, allowing one login to access all related services, with access granted based on registered permissions for tasks such as uploading data or retrieving internal resources.

6.2. Development of Data Space Functions

The dashboard provides four main functions: Assets and federated catalog, Contracts and policies, Premises and users (Figure 4). These functionalities allow registered members to upload data as assets, edit records, and initiate data-sharing procedures within the NIKH-DS ecosystem.

Assets and federated catalog: The Assets tab allows members to manage data resources that facilitate collaboration and innovation through secure sharing. Users can view a list of owned assets and key details and create new assets by filling out required metadata fields. The dashboard supports uploading a wide range of file types, including research data, datasets, processed data, reports, images, and videos. For each asset, users can: (i) add required metadata, (ii) upload or link to external data sources, and (iii) provide additional

domain-specific metadata. Once submitted, the Connector Manager triggers a RESTful API endpoint to securely store the files within the NIKH-DS knowledge base. The Federated Catalog aggregates all assets in the ecosystem, allowing members to download or request assets provided by other premises according to existing policies and contracts.

Contracts and policies: The Contracts tab provides a structured approach for managing agreements and collaborations, ensuring trust and reliable data sharing while maintaining ownership and control. Users can create and manage contracts for selected assets through a form that includes essential fields such as asset name (selected from the user's assets) and access policy name (selected from available policies). Policy types include: (i) Public—data fully accessible with no restrictions; (ii) Public after embargo—data becomes publicly available after a specified embargo period; (iii) Restricted access—access may require negotiation; and (iv) Closed—both data and metadata are inaccessible to other participants. **Premises and users:** The Premises tab lists all registered premises in the data space ecosystem. Each entry indicates the presence of a Data Space Connector, confirming that the organization is an active participant. The premises are created by administrators or developers through the installation of new connectors, either locally or centrally. The Users tab displays all registered members in the NIKH-DS ecosystem. Users are created by administrators or developers according to access control mechanisms, and relevant information about each registered member is presented for transparency and management purposes.

7. Application of NIKH-DS in the NextGEM Case Studies

NIKH-DS has been designed, developed, and deployed to meet the requirements of the NextGEM project by enabling controlled access to sensitive and public data. The platform incorporates secure storage and data exchange mechanisms for both raw and processed data within the NextGEM data space ecosystem, ensuring compliance with FAIR principles and data protection standards. Data access and interoperability are facilitated via data space connectors deployed within NIKH-DS. The following subsections describe the applicability of NIKH-DS for data exchange and for using the ingested data to conduct risk assessments.

7.1. NextGEM Case Studies

NIKH-DS serves as the central repository for background information and research results generated within NextGEM, supporting the project's case studies. It enables organizations to manage collected results among authorized users and provides the basis for assessing the potential health effects of exposure to EMF. Through the NIKH-DS dashboard, affiliated users can manage organizational data, explore data from other participants according to access policies, register new entries, and maintain data ownership. Upon successful login, users access data governed by NIKH-DS across the different interface tabs (Assets, Contracts, Premises, and Users). The platform has been validated in the following three case studies to demonstrate the platform's capability to manage distributed data collection, provide secure storage and exchange in diverse real-world settings, and support health risk assessment workflows.

- Case Study 1: Potential effects of indoor RF exposure on vulnerable populations, focusing on reproduction and development.
- Case Study 2: Optimized outdoor urban planning and 5G architecture design, including investigations into public awareness of cancer-related health hazards.
- Case Study 3: Health effects of exposure to mmWave EMF in indoor and outdoor environments.

7.2. Deployment of the NextGEM Data Space Ecosystem Within NIKH-DS

NextGEM partner organizations have established their own premises within the NIKH-DS ecosystem, as shown in the Premises tab (Figure 5). Currently, 20 premises corresponding to project partners are registered, each running a separate container with an individual NIKH-DS connector. Access is restricted to authorized subscribers based on permissions associated with NextGEM members, protecting sensitive and public data. Each premises can register multiple users with predefined roles (e.g., supervisor, full member, member) to manage datasets, access data, and configure permissions. Users include both project partners (providers and consumers) and external consumers. The platform displays the list of members within the NextGEM data space ecosystem along with their organizational affiliations and contact information. Based on the allocation, the partners involved in the case studies are:

- CIMNE, CSIC, and CNR lead the activities of Case Study 1;
- UCAS, CNR, SC, TIM, and FIBER are the principal contributors to Case Study 2;
- THUAS, TUD, SC, HUJI, and UZH play a key role in Case Study 3;
- SPi, IMBEI, IARC, RIVM, and FORTH participate primarily as consumers.

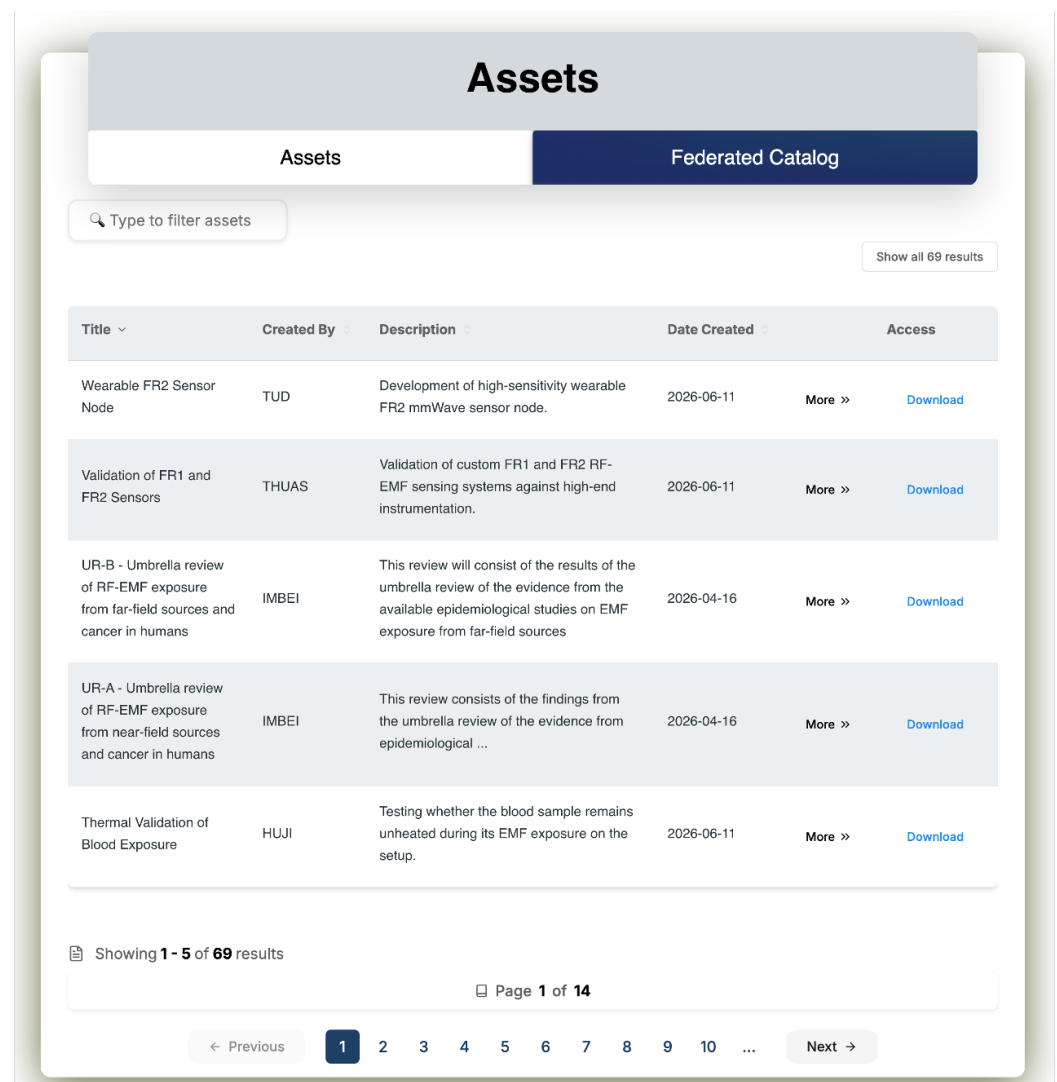
Full Name	Organization
Universita degli studi di Cassino e del Lazio Meridionale	UCAS
Consiglio Nazionale Delle Ricerche	CNR
Foundation for Research & Technology – Hellas	FORTH
Centro Internacional de Métodos Numéricos en la Ingeniería	CIMNE
The Hague University of Applied Sciences	THUAS
Hebrew University of Jerusalem	HUJI
Technische Universiteit Delft	TUD
University of Zurich	UZH
Sciensano	SC
Agencia Estatal Consejo Superior de Investigaciones Científicas	CSIC
eBOS Technologies Limited	eBOS
SciProof International AB	SPi
Sphynx Analytics Limited	SANL
Intracom SA Telecom Solutions	ICOM
Istituto Superiore di Sanità	ISS
Telecom Italia S.p.A.	TIM
Rijksinstituut voor Volksgezondheid en Milieu	RIVM
Universitätsmedizin der Johannes Gutenberg-Universität Mainz	IMBEI
Centre International de Recherche sur le Cancer	IARC
FiberCop S.p.A.	FIBER

Figure 5. All deployed premises in the NextGEM data space ecosystem.

7.3. Case Study Assets in the NextGEM Data Space Ecosystem

NextGEM assets include research outputs, experimental studies, and exposure assessments related to EMF and health investigations. Users belonging to NextGEM premises can upload assets via the Assets tab on the NIKH-DS dashboard in standardized formats, following predefined policies and contracts. This enables secure collaboration and data sharing across the ecosystem. Dedicated connectors allow contributors to link local datasets to the federated NextGEM ecosystem. For each asset, participants provide

metadata, including title, authors, organizations, description, keywords, study type (e.g., exposure assessment, human studies, in vitro, in vivo, in silico) and domain-specific details such as study parameters. Some assets are stored locally in connectors' Azurite databases, while others are linked to external storage platforms, such as Zenodo, to ensure interoperability, archival continuity, and public sharing. However, both metadata are inserted as assets in the data space. In addition, the Federated Catalog (Figure 6) includes the assets designated for the different case studies according to policies and contracts. Each asset is associated with a contract that defines access rules: publicly shareable, organization-restricted, or embargoed. Members can download assets based on policy permissions or request access for restricted assets. Currently, the federated catalog contains 69 assets from all case studies. Although file size uploads are limited at the current stage to 100 MB, there is no restriction on the number of assets per organization within allocated storage. As NIKH-DS is fully operational, the number of assets will increase as the project progresses.



Title	Created By	Description	Date Created	Access
Wearable FR2 Sensor Node	TUD	Development of high-sensitivity wearable FR2 mmWave sensor node.	2026-06-11	More » Download
Validation of FR1 and FR2 Sensors	THUAS	Validation of custom FR1 and FR2 RF-EMF sensing systems against high-end instrumentation.	2026-06-11	More » Download
UR-B - Umbrella review of RF-EMF exposure from far-field sources and cancer in humans	IMBEI	This review will consist of the results of the umbrella review of the evidence from the available epidemiological studies on EMF exposure from far-field sources	2026-04-16	More » Download
UR-A - Umbrella review of RF-EMF exposure from near-field sources and cancer in humans	IMBEI	This review consists of the findings from the umbrella review of the evidence from epidemiological ...	2026-04-16	More » Download
Thermal Validation of Blood Exposure	HUJI	Testing whether the blood sample remains unheated during its EMF exposure on the setup.	2026-06-11	More » Download

Showing 1 - 5 of 69 results

Page 1 of 14

← Previous 1 2 3 4 5 6 7 8 9 10 ... Next →

Figure 6. Federated catalog of shared assets in NextGEM.

7.4. Applicability of Data Space Assets for Risk Assessment

A key validation step is the integration of NIKH-DS assets with the Risk Assessment (RA) tool developed within NextGEM. The RA tool provides an interactive environment for the human health risk assessment related to EMF exposure, following a workflow of hazard identification, exposure assessment, and risk characterization (Figure 7a): Hazard identification considers EMF parameters with potential health risks; exposure assessment

quantifies these parameters in real-world scenarios using sensor data and computational models; and risk characterization synthesizes the information to evaluate potential adverse effects. All generated data and metadata have been incorporated into NIKH-DS, ensuring FAIR compliance and enabling structured data management, literature review, and risk assessment workflows. For Case Study 1, related literature is first imported into the RA tool using the Add Literature by DOI function to form the evidence base. The data assets of the NIKH-DS ecosystem are then imported using the Add from Dataspace function (Figure 7b), with each asset marked by an icon indicating its source: DOI for publications or NextGEM icon for the data space assets of the project (Figure 7c). These assets are incorporated into the hazards identification and exposure assessment tabs. Finally, the same workflow is applied for Case Studies 2 and 3, demonstrating the interoperability of NIKH-DS modules and showing how the literature and project data assets together can be applied for effective risk assessments within a consistent and traceable framework. Overall, this integration demonstrates how NIKH-DS assets support interoperable, FAIR-compliant, and traceable workflows for comprehensive EMF risk assessment across multiple case studies.

7.5. Discussion

The results presented in this work demonstrate that the NIKH-DS platform provides a functional implementation of data space principles in a real-world research environment. Its deployment within the NextGEM ecosystem and its validation in multiple case studies confirm the platform's capability to support secure, interoperable, and policy-driven data exchange between distributed stakeholders. A key strength of the proposed approach lies in the implementation of standardized metadata management, federated catalog services, and controlled access mechanisms that preserve data sovereignty while enabling collaborative data sharing. The platform supports multiple data governance configurations, including differentiated access policies and secure authentication workflows, ensuring compliance with organizational and regulatory requirements. These capabilities directly contribute to the implementation of FAIR data principles by enabling structured data discovery, controlled reuse, and transparent provenance tracking throughout the data lifecycle. In addition, the integration of the NIKH-DS with the RA tool illustrates the practical value of combining heterogeneous datasets and scientific literature within a unified workflow, allowing reproducible and traceable analytical processes across organizational boundaries. This end-to-end integration highlights the operational applicability of the platform beyond a conceptual architecture and demonstrates its suitability for realistic scientific and regulatory use cases.

Nevertheless, certain limitations remain. The current deployment reflects infrastructure-level constraints, such as containerized DS connectors with a limited number of datasets and restricted data sizes, which may affect performance in large-scale or high-throughput data ingestion scenarios. Additionally, while the platform has been validated within the scope of the NextGEM project, broader adoption across external domains will require further evaluation of interoperability with additional data space ecosystems, and long-term operational sustainability. Addressing these aspects represents an important direction for future platform evolution and large-scale deployment.

It should also be noted that the objective of the current work was to design, implement, deploy, and validate the NIKH-DS platform within a real-world health data-sharing environment. Consequently, the evaluation focused on demonstrating the successful integration of distributed data providers, deployment of federated data space services, enforcement of access control policies, and support of data sharing and risk assessment workflows. Quantitative measurements of latency, throughput, connector overhead, catalog lookup performance, concurrent workload handling, scalability, reliability, and fault

tolerance were outside the scope of this study. Therefore, the presented results should be interpreted as evidence of the feasibility and operational applicability of the proposed architecture rather than as a quantitative assessment of system performance.

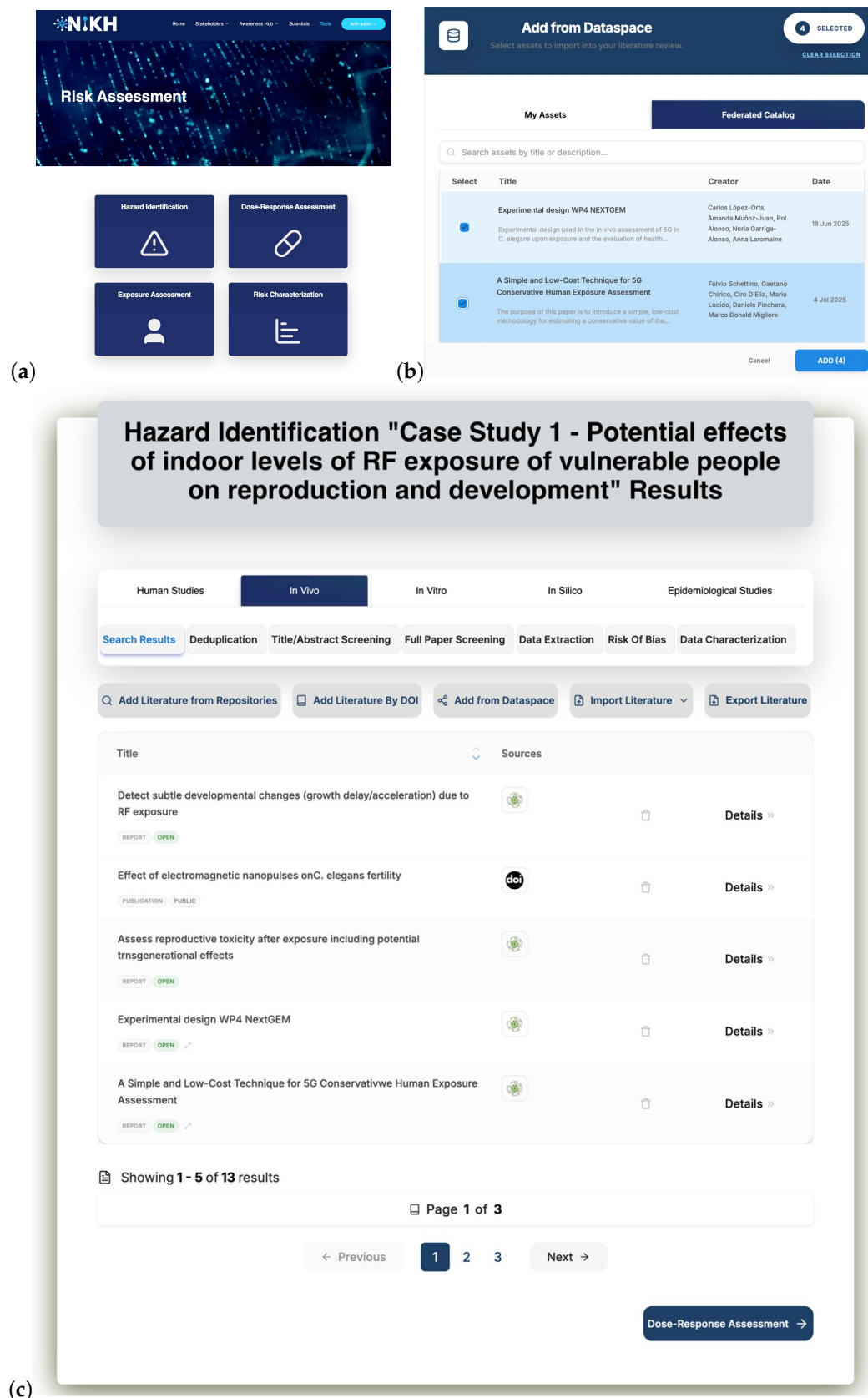


Figure 7. Risk Assessment tool: (a) interface; (b) addition of data space assets; (c) integration of literature and data space assets.

8. Conclusions

This paper presented the design and validation of the NIKH-DS platform as a secure and interoperable infrastructure for distributed data management and exchange in collaborative research environments. The deployment of the platform within the NextGEM project and its application across multiple case studies demonstrated the practical feasibility of implementing data space services to support controlled data sharing, reproducible workflows, and policy-driven governance among distributed stakeholders. By enabling structured data discovery, secure access control, and transparent data provenance, the NIKH-DS supports FAIR data exchange and strengthens the reliability and traceability of scientific analysis and risk assessment. Future work will focus on improving scalability, enhancing interoperability with external data space ecosystems, and further automating governance and policy enforcement mechanisms to support large-scale operational deployment.

Author Contributions: Conceptualization, all authors; methodology, all authors; software, all authors; validation, all authors; investigation, all authors; writing—original draft preparation, N.P.; writing—review and editing, all authors; visualization, all authors; supervision, N.P.; project administration, N.P.; funding acquisition, all authors as contributors to the funded Horizon Europe Project NextGEM. All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of the European Union’s Horizon Europe research and innovation program under grant agreement No 101057527 (NextGEM). Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: Authors V.T., M.E.V. and E.Z. were employed by the company Intracom Telecom. Author D.L. was employed by the company Intracom Telecom and Icon Platforms SA. Author N.L. was employed by the company eBOS Technologies Limited. Author S.F. was employed by the company Sphynx Analytics Limited. Author P.Z. was employed by the company Netcompany. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. European Commission. A European Strategy for Data. Available online: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> (accessed on 17 June 2026).
2. European Commission. Common European Data Spaces. Available online: <https://digital-strategy.ec.europa.eu/en/policies/data-spaces> (accessed on 17 June 2026).
3. European Health Data Space. Available online: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en (accessed on 17 June 2026).
4. Petroulakis, N.; Mattsson, M.O.; Chatziadam, P.; Simko, M.; Gavrielides, A.; Yiorkas, A.; Zeni, O.; Scarfi, M.R.; Soudah, E.; Otin, R.; et al. NextGEM: Next-generation integrated sensing and analytical system for monitoring and assessing radiofrequency EMF exposure and health. *Int. J. Environ. Res. Public Health* **2023**, *20*, 6085. [CrossRef] [PubMed]
5. Petroulakis, N.; Zervoudakis, P.; Nomikos, G.; Kornilakis, A.; Chatziadam, P.; Laskaratos, D.; Eleftheria, V.M.; Eleni, Z.; Theodorou, V. Towards the development of a network provisioning platform for data exchange in the health data space. In Proceedings of the 2024 IEEE Conference on Standards for Communications and Networking (CSCN), Belgrade, Serbia, 25–27 November 2024.
6. Sawadogo, P.; Darmont, J. On data lake architectures and metadata management. *J. Intell. Inf. Syst.* **2020**, *56*, 97–120. [CrossRef]
7. Sarramia, D.; Claude, A.; Ogereau, F.; Mezhoud, J.; Mailhot, G. CEBA: A Data Lake for Data Sharing and Environmental Monitoring. *Sensors* **2022**, *22*, 2733. [CrossRef] [PubMed]
8. Manco, C.; Dolci, T.; Azzalini, F.; Barbierato, E.; Gribaudo, M.; Tanca, L. HEALER: A Data Lake Architecture for Healthcare. In Proceedings of the EDBT/ICDT Workshops, Ioannina, Greece, 28–31 March 2023.

9. Wang, S.; Zhang, Y.; Zhang, Y. A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems. *IEEE Access* **2018**, *6*, 38437–38450. [CrossRef]
10. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A Survey on the Scalability of Blockchain Systems. *IEEE Netw.* **2019**, *33*, 166–173. [CrossRef]
11. Curry, E.; Scerri, S.; Tuikka, T. Data spaces: Design, deployment, and future directions. In *Data Spaces: Design, Deployment and Future Directions*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 1–17.
12. Kovach, A.; Montalvillo, L.; Lanza, J.; Sotres, P.; Urbieto, A. Understanding data spaces: A Systematic Mapping Study of foundations, technical building blocks, and sectoral adoption. *Comput. Sci. Rev.* **2026**, *59*, 100819. [CrossRef]
13. Dam, T.; Klausner, L.D.; Neumaier, S.; Priebe, T. A survey of dataspace connector implementations. *arXiv* **2023**, arXiv:2309.11282.
14. Beckmann, S.; Klemm, S.; Krüger, T.; Trojahn, S. Data management plan for a digital platform with open and restricted data. *IFAC-PapersOnLine* **2025**, *59*, 548–553. [CrossRef]
15. Guggenberger, T.M.; Schlueter Langdon, C.; Otto, B. Data spaces as meta-organisations. *Eur. J. Inf. Syst.* **2025**, *34*, 822–842. [CrossRef]
16. Pampus, J.; Brian-Frederik, J.; Ronja, Q. Evolving data space technologies: Lessons learned from an IDS connector reference implementation. In *Proceedings of the ISOLA*; Springer: Cham, Switzerland, 2022.
17. Eclipse Data Space Components (EDC). Available online: <https://projects.eclipse.org/projects/technology.edc> (accessed on 17 June 2026).
18. International Data Spaces Association. Data Connector Report. Available online: <https://internationaldataspaces.org/data-space-connector-report/> (accessed on 17 June 2026).
19. International Data Space Association (IDSA). Available online: <https://internationaldataspaces.org> (accessed on 17 June 2026).
20. Gaia-X: A Federated Secure Data Infrastructure. Available online: <https://gaia-x.eu> (accessed on 17 June 2026).
21. Raab, R.; Küderle, A.; Zakreuskaya, A.; Stern, A.; Klucken, J.; Kaissis, G.; Rueckert, D.; Boll, S.; Eils, R.; Wagener, H.; et al. Federated electronic health records for the European Health Data Space. *Lancet Digit. Health* **2023**, *5*, e840–e847. [CrossRef] [PubMed]
22. HEALTH—X dataLOFT Platform. Available online: <https://www.health-x.org/en/platform> (accessed on 17 June 2026).
23. HealthData@EU Pilot. Available online: <https://health-data-hub.fr/page/healthdataeu-pilot/> (accessed on 17 June 2026).
24. Rodríguez-Mejías, S.; Degli-Esposti, S.; González-García, S.; Parra-Calderón, C. Toward the European Health Data Space: The IMPaCT-Data secure infrastructure for EHR-based precision medicine research. *J. Biomed. Inform.* **2024**, *156*, 104670. [CrossRef] [PubMed]
25. Catena-X Automotive Network. Available online: <https://catena-x.net/> (accessed on 17 June 2026).
26. EONA-X: Data-Sharing on Mobility in Europe. Available online: <https://eona-x.eu/> (accessed on 17 June 2026).
27. The Copernicus Data Space Ecosystem. Available online: <https://dataspace.copernicus.eu/> (accessed on 17 June 2026).
28. Petroulakis, N.; Chatziadam, P.; Mattsson, M.O.; Simko, M.; Theodorou, V.; Yioras, A.M.; Gavrielides, A.; Miaoudakis, A.; Scarfi, M.R.; Zeni, O. Designing NIKH: The NextGEM Innovation and Knowledge Hub to Access Next Generation Radio Frequency EMF Exposure and Health Data. In *Proceedings of the 2022 IEEE Conference on Standards for Communications and Networking (CSCN)*, Thessaloniki, Greece, 28–30 November 2022.
29. Eclipse Data Space Components, Minimum Viable Data Space. Available online: <https://github.com/eclipse-edc/MinimumViabledataspace> (accessed on 17 June 2026).
30. Azurite, Microsoft Azure. Available online: <https://github.com/Azure/Azurite> (accessed on 17 June 2026).
31. Keycloak, Open Source Identity and Access Management. Available online: <https://www.keycloak.org/> (accessed on 17 June 2026).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.