Measuring Envelope products and systems contributing to next generation of healthy nearly Zero Energy buildings

D4.6
Data protection measures: implementation of measures to ensure privacy and security of sensible data

January 2026

WP4

Dissemination level
Confidential

The MEZeroE Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953157

Measuring Envelope products and systems contributing to next generation of healthy nearly Zero Energy buildings

Deliverable No.	D4.6	Dates
Related WP	WP4	
Deliverable Title	Data protection measures: implementation of measures to ensure privacy and security of sensible data	
Deliverable Dates	2026-01-31	
Deliverable Type	Report	
Dissemination level	Confidential	
Authors (s)	Massimiliano Raciti, R2M Solution Eva Coscia, R2M Solution Alberto Pes, R2M Solution Giuseppe Scarpi, R2M Solution Fabrizio Perrotta, R2M Solution	
Checked by	Alberto Pes, R2M Solution	2026-01-31
Reviewed by	Roberto Lollini, EURAC research Graziano Salvalai, PoliMI Urška Blumauer, ZAG	2026-02-09 2026-02-12
Status	Final	2026-02-23

Disclaimer/ Acknowledgment

The MEZeroE Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953157

Executive summary

Technological innovation in the construction sector is considerably difficult to implement due to several factors such as the fragmentation and complexity of this sector. Many disciplines are involved at various stages, design and production are usually separated, there is a large number of players with a vast majority of small-medium enterprises (SME), and supply chains are long and variegated. As a result, gathering the different specialists together is difficult, and many potentially effective innovative solutions do not even reach the market.

H2020 MEZeroE project aims at tackling this complex issue by creating an EU distributed open innovation ecosystem for (i) developing nearly Zero Energy Building (nZEB) Enabler Envelope technology solutions; (ii) transferring knowledge; (iii) matching testing needs with existing facilities; (iv) providing monitoring in living labs; and; (v) standardizing cutting-edge solutions coming from SMEs and larger industries, to foster inclusive change in the building sector, being accessible via a single-entry point to all users.

MEZeroE ecosystem is accessible via a single-entry point online platform which includes 9 Pilot Measurement & Verification Lines (PM&VL), 3 Open Innovation Services (OIS), a living lab (LL) building-technology match making service to enable real-world validation, and resources for training, business model development, intellectual property (IP) and knowledge management. MEZeroE fast-tracks prototypes to the market as fully characterized products.

This document, **Deliverable 4.6 (Platform security and privacy system implementation)**, constitutes the definitive technical report on the security infrastructure and data protection frameworks established for the **MEZeroE Virtual Marketplace**. It confirms that the system design proposed in Task 4.2 has been fully translated into an operational, secure, and legally compliant platform capable of hosting sensitive intellectual property and personal data.

The MEZeroE ecosystem functions as a multi-sided marketplace connecting manufacturers, testing labs, and researchers to accelerate **nZEB Enabler Envelope Solutions (nEES)**. Given the high value of the industrial data and the privacy risks associated with occupant monitoring in Living Labs, this deliverable demonstrates how the platform adheres to the "Privacy by Design" and "Security by Default" principles mandated by the **General Data Protection Regulation (GDPR)**.

Key Implementation Achievements:

- **Secure Platform Architecture:** The platform is hosted on a resilient, 3-layered reference architecture within **Amazon Web Services (AWS)**. To ensure data sovereignty and minimize transfer risks, all production instances are located strictly within **European Regions**. The infrastructure is hardened against common web vulnerabilities (OWASP Top 10) through the active configuration of the **SecKit** module and rigorous input validation protocols.

- **Data Management Framework:** Aligned with the European Commission's **FAIR principles** (Findable, Accessible, Interoperable, Reusable), the project has established a comprehensive inventory of 10 primary datasets (DS-01 to DS-10). Each dataset is governed by a specific lifecycle strategy, ensuring that public resources are open and discoverable, while sensitive proprietary data remains encrypted and strictly compartmentalized.

- **Privacy & Legal Compliance:** The platform operates under a defined legal framework that distinguishes between data processed for **Contractual Necessity** (e.g., user registration) and **Explicit Consent** (e.g., Living Lab surveys). Technical compliance with the **Privacy Directive** is enforced via the **iubenda** consent management platform, while the **SelectRegistrationRole** module technically enforces granular access rights, ensuring manufacturers cannot access competitors' data.

- **Operational Security Measures:** Active security controls are now live, including:

    - **Encryption:** Full end-to-end encryption using TLS 1.2+ for data in transit and salted hashing for credentials at rest.

    - **Threat Mitigation:** Automated scanning for all user uploads and **SecKit** integration to prevent bot attacks.

    - **Resilience:** A robust backup strategy involving geographically redundant snapshots and off-site storage in Google Workspace (EU-only) to guarantee business continuity.

In conclusion, the MEZeroE Virtual Marketplace has successfully transitioned from development to a fully operational state. The implemented measures provide a secure foundation that meets the stringent requirements of the **NIS Directive** and **GDPR**, ensuring a trusted environment for the construction sector's open innovation activities.

The organizational governance structures, decision-making rights, and long-term maintenance protocols supporting these technical measures are detailed in the complementary ***Deliverable 4.7 (Platform governance and management plan)****.*

The MEZeroE Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953157

List of acronyms

Acronym	Definition
API	Application Programming Interface
AWS	Amazon Web Services
BEM	Building Energy Models
BIM	Building Information Modelling
BMS	Building Management System
CA	Consortium Agreement
CMS	Content Management System
CRM	Customer Relationship Management
CSRF	Cross-Site Request Forgery
DoA	Description of Action
DOI	Digital Object Identifier
DMP	Data Management Plan
DPO	Data Protection Officer
DPSC	Data Privacy & Security Committee
EBS	Elastic Block Store (AWS)
EC	European Commission
ECM	Energy Conservation Measure
EEA	European Economic Area
eIDAS	electronic IDentification, Authentication and trust Services
ENISA	European Union Agency for Cybersecurity
EPBD	Energy Performance of Buildings Directive
EU	European Union
FAIR	Findable, Accessible, Interoperable, Reusable
GDPR	General Data Protection Regulation
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IEC	Innovation and Exploitation Committee

IEQ	Indoor Environmental Quality
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
NDA	Non-Disclosure Agreement
nEES	nZEB Enabler Envelope technology Solutions
NIS	Network and Information Security
nZEB	nearly Zero Energy Building
OA	Open Access
OIS	Open Innovation Services
ORDP	Open Research Data Pilot
OWASP	Open Web Application Security Project
PbD	Privacy by Design / Privacy by Default
PII	Personally Identifiable Information
PIMS	Privacy Information Management System
PM&VL	Pilot Measurement & Verification Lines
QA	Quality Assurance
RA	Registration Agency
RBAC	Role-Based Access Control
S3	Simple Storage Service (AWS)
SaaS	Software as a Service
SCC	Standard Contractual Clauses
SIRP	Security Incident Response Plan
SME	Small and Medium-sized Enterprises
SQL	Structured Query Language
SSL	Secure Sockets Layer
TFA	Two-Factor Authentication

TLS	Transport Layer Security
TOTP	Time-based One-Time Password
WP	Work Package
XSS	Cross-Site Scripting

1 Introduction

The MEZeroE project has established a distributed open innovation ecosystem for the construction sector, designed to foster cross-fertilization among stakeholders and accelerate the adoption of advanced building technologies. At the heart of this ecosystem is a multi-side virtual marketplace that provides turn-key services for modelling, testing, and monitoring nZEB Enabler Envelope technology Solutions (nEES).

This web-based platform acts as a single-entry point for the entire ecosystem, connecting users with 9 Pilot Measurement & Verification Lines (PM&VLs) and 3 Open Innovation Services (OIS). It integrates resources for training, business model development, and systematic intellectual property management, ensuring that prototypes can be fast-tracked to the market as fully characterized products. The platform is now fully operational and available at https://mezeroe-platform.eu.

1.1 Purpose and scope

The primary purpose of this document is to formally define the definitive procedures and constraints governing the entire data lifecycle within the MEZeroE virtual marketplace. It establishes the final methodology used to preserve the data privacy and security of the platform's users and the knowledge generated within the ecosystem, ensuring full adherence to the **General Data Protection Regulation (EU) 2016/679 (GDPR)**[1].

This report consolidates the security and privacy outcomes of **Work Package 4 (WP4)**. It confirms that the measures planned in the design phase have been fully implemented in the live system. Specifically, it details:

- How user requirements gathered in **Task 4.1** were translated into privacy controls.
- How the secure architecture designed in **Task 4.2** protects sensitive data.
- How data is managed operationally under the protocols defined in **Task 4.6**.

This deliverable serves as the technical complement to **D4.7 (Platform governance and management plan)**. While D4.7 focuses on the organizational governance and decision-making rights, this document (D4.6) focuses on the specific technical implementation of security measures, data protection mechanisms, and compliance with privacy laws.

[1] Regulation (EU) 2016/679 (GDPR): https://eur-lex.europa.eu/eli/reg/2016/679/oj

2 Data Management Framework

This chapter establishes the structured approach for handling data within the MEZeroE ecosystem. It defines the guiding principles for data governance, provides a comprehensive inventory of the datasets managed by the platform, and details of the lifecycle of data from collection to archival. This framework is designed to align with the technical realities of the live platform (as defined in D4.4) and the user workflows (as defined in D4.1 and D4.5).

2.1 Data Management Principles

The MEZeroE platform adopts a robust data management strategy grounded in European Commission guidelines for research and innovation. The core of this strategy is the adherence to **FAIR Data Principles**[2] and compliance with the **Open Research Data Pilot (ORDP)**[3].

- **Findable:**
  - **Metadata Provision:** All public resources (e.g., success stories, articles) are tagged with rich metadata, including keywords from the "Product and Testing Categories" taxonomy (e.g., "Active solar energy systems", "Thermal comfort").
  - **Identification:** Datasets intended for public dissemination or citation (e.g., in scientific publications) will be assigned unique persistent identifiers (DOIs) where applicable, ensuring they can be easily located and cited.
  - **Searchability:** The platform implements an advanced search engine, as seen in Figure 1, based on the `Search Module`, allowing users to discover content via full-text search and specific taxonomy filters.
- **Accessible:**
  - **Open by Default, Closed by Necessity:** While the project promotes Open Science, access to specific datasets is governed by granular permissions. Public data (Success Stories, News) is openly accessible, while sensitive business data (Service Requests) is strictly restricted to authorized users (Manufacturers, OIS Leaders, PM&VL Leaders, Living Laboratory Leaders) via the `Group` and `SelectRegistrationRole` modules.
  - **Metadata Availability:** Metadata for restricted datasets remains accessible to facilitate discovery without compromising confidentiality.
- **Interoperable:**
  - **Standard Formats:** Data is stored and exchanged in standard, non-proprietary formats to ensure compatibility. For example, the **BIM Package Configurator** allows users to export dataset requirements in CSV format, and time-series data from monitoring is handled in widely supported formats like CSV or JSON.
  - **Common Vocabularies:** The platform uses standardized taxonomies (e.g., `OIS Filter Categories`, `Product and Testing Categories`) to classify services and products, ensuring semantic consistency across the ecosystem.
- **Reusable:**

[2] https://horizoneuropencpportal.eu/repository/5b7fcc0e-73da-4e76-8b46-3682a36fa59b
[3] https://www.openaire.eu/what-is-the-open-research-data-pilot

- **Licensing:** Publicly shared data (e.g., in the "Success Stories" section) is released with clear usage licenses (e.g., Creative Commons) to maximize reuse.
- **Documentation:** Datasets are accompanied by documentation describing their origin and processing methods, ensuring that third parties can understand and properly utilize the data.

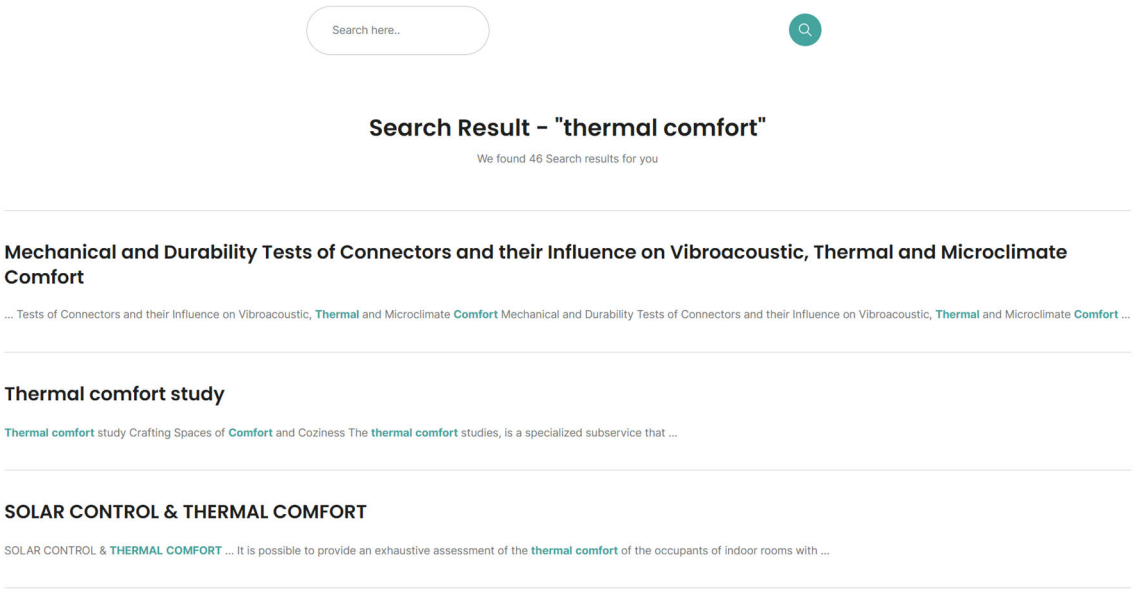

Figure 1: Screenshot from the MEZeroE platform Search Engine with results for thermal comfort

2.2 Dataset Inventory

The platform manages a diverse range of datasets, classified by their sensitivity and usage within the virtual marketplace. The following inventory updates (Table 1) the initial list from D1.5 to reflect the final platform implementation with some key datasets used in the platform.

Table 1: Dataset Inventory

ID	Dataset Name	Data Type	Sensitivity	Marketplace Usage	Description
DS-01	User Profile Data	Personal	High	Yes (Private)	Registration details (Name, Email, Company) managed via the Profile module.
DS-02	Service Request Data	Business (Confidential)	High	Yes (Private)	Input forms and communications exchanged between Manufacturers and Service Providers during the matchmaking process.
DS-03	Product Specifications	Technical (IPR)	Medium	Yes (Private)	Technical details (datasheets, drawings) uploaded by manufacturers

					to characterize their products for testing.
DS-04	Test Reports & Results	Technical (IPR)	Medium	Yes (Private)	Output documents (PDFs, raw data files) generated by PM&VLs and uploaded to the request page for the client.
DS-05	IoT Monitoring Data	Time-series	Medium	Yes (Private)	Environmental data (temperature, IAQ, energy) collected from sensors in Living Labs or pilot sites.
DS-06	Occupant Feedback	Personal	High	Yes (Private)	Post-occupancy evaluation surveys regarding comfort perception. Requires explicit consent.
DS-07	BIM Configurator Datasets	Technical	Low	Yes (Public/Private)	Envelope Package BIM digitalized information dataset according to the respective construction segment and four different use scenarios.
DS-08	Success Stories	Content	Low	Yes (Public)	Non-competitive product journeys and results published explicitly by manufacturers for dissemination.
DS-09	News & Events	Content	Low	Yes (Public)	Articles, event listings, and webinar details managed via the News content type.
DS-10	Analytics Data	Statistical	Low	No (Internal)	Aggregated website usage statistics collected via Matomo (anonymized IP addresses).

2.3 Data Lifecycle

The lifecycle of data within the MEZeroE platform is strictly managed to ensure security and compliance from creation to deletion.

Creation and Collection:

- Data is generated through specific user actions defined in the platform scenarios (e.g., **Platform-Sc6: Account Creation**, **PM&VL-Sc1: Service Request**).
- **Validation:** Input data is validated at the point of entry. The `service_request` module checks user roles and sanitizes inputs to prevent malicious code injection.

- **Consent:** For personal data (e.g. DS-01, DS-06), consent is obtained immediately via the `iubenda` plugin (cookies) or specific consent forms (surveys).

Processing and Usage:

- **Active Use:** Data is actively used to facilitate services. For example, product data (DS-03) is used by the **PM&VL Controller** to allow lab leaders to assess feasibility.
- **Matchmaking:** The system processes user needs (filtered via taxonomies) to match manufacturers with appropriate OIS or PM&VL providers, generating dynamic views without exposing the underlying database to unauthorized users.
- **Security:** During processing, data remains encrypted in transit (HTTPS) and access is logged via the `logger` module.

Storage and Retention:

- **Storage:** Data is stored in the AWS cloud environment (EC2/S3) located in Europe. Sensitive business data is logically separated from public content to minimize risk.
- **Retention:** Data is retained only for as long as necessary to fulfil the service contract or legal obligations.
    - *User Accounts:* Retained until the user requests deletion.
    - *Service Data:* Retained as per the agreement between the Manufacturer and Provider, typically for the duration of the project plus a defined auditing period (e.g., 2 years).

Archiving and Deletion**:**

- **Archiving:** Inactive data may be moved to cheaper storage classes (AWS S3 Infrequent Access) or offline backups (Google Workspace) for long-term preservation, if required.
- **Deletion:** When the retention period expires or a "Right to Erasure" request is received, data is securely deleted from the live database and backups.

3 Legal and Regulatory Framework

The MEZeroE Virtual Marketplace handles personal and sensitive business data (e.g. DS-01: User Profile Data) and is therefore designed and implemented in strict adherence to the General Data Protection Regulation (EU) 2016/679 (GDPR). This chapter defines the legal grounds for data processing and the specific regulatory obligations the platform is mandated to fulfil.

3.1 Legal Basis for Data Processing

In accordance with Article 6 of the GDPR, the platform processes personal data based on the following distinct legal grounds:

In accordance with **Article 6 of the GDPR**[4], the platform processes personal data based on specific, documented legal grounds required for the operation of a digital marketplace:

- **Contractual Necessity (Art. 6(1)(b)):** This is the primary basis for processing data required to establish the user's account and deliver the requested services. The collection of contact and company details is legally justified as strictly necessary to fulfil the service contract between the platform and the user.
- **Legitimate Interest (Art. 6(1)(f)):** The platform processes limited technical data (e.g., server logs, session identifiers) to ensure the security, integrity, and performance of the system. This interest is balanced against user rights by ensuring such data is not used for profiling or marketing purposes without consent.
- **Explicit Consent (Art. 6(1)(a)):** For data collection that is not strictly necessary for the service but involves sensitive research (e.g., Living Lab surveys, **DS-06**) or promotional communication, processing occurs only after obtaining clear, affirmative consent from the data subject.

3.2 User Rights and Data Sovereignty

The platform's governance framework guarantees that data subjects can exercise their rights under GDPR Articles 15–20. These rights are binding obligations for the Data Controller:

- **Right of Access and Rectification (Art. 15-16):** Data subjects have the legal right to access their personal data and request corrections to inaccurate or incomplete information without undue delay.
- **Right to Erasure ('Right to be Forgotten') (Art. 17):** Users have the right to request the deletion of their personal data when it is no longer necessary for the purposes for which it was collected, or if they withdraw consent.
- **Right to Data Portability (Art. 20):** Where processing is based on consent or contract, users have the right to receive their personal data in a structured, commonly used, and machine-readable format to transmit it to another controller.

[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj

- **Right to Restriction of Processing (Art. 18):** Users have the right to request the restriction of processing in specific circumstances, such as when the accuracy of the data is contested.

3.3 Specific Regulatory Compliance Measures

Beyond the general GDPR framework, the MEZeroE platform aligns its data governance with specific regulations relevant to the construction sector and digital services.

- **Privacy in Communications (ePrivacy Directive)[5]:** The platform adheres to the requirements regarding the confidentiality of communications and the use of cookies/trackers. No non-essential tracking is permitted without prior informed consent.

- **Building and Energy Data (EPBD)[6]:** Data related to energy consumption and Indoor Environmental Quality (IEQ) collected in Living Labs (**DS-03**) is processed in compliance with the **Energy Performance of Buildings Directive (EPBD)**. The framework ensures that technical building data is treated distinctly from personal occupant data to prevent unauthorized behavioural profiling.

- **Cybersecurity Act & NIS Directive[7,8]:** As a digital service provider, the platform is aligned with the resilience and security notification requirements mandated for essential digital services.

3.4 Alignment with International Standards

To ensure a defensible and recognized approach to information security and privacy, the platform's governance measures are aligned with the following standards:

- **ISO/IEC 27001 (Information Security Management)[9]:** Managing the security of assets and infrastructure.

- **ISO/IEC 27701 (Privacy Information Management)[10]:** Extending security controls to specifically address the management of personally identifiable information (PII).

[5] https://eur-lex.europa.eu/eli/dir/2002/58/oj
[6] https://eur-lex.europa.eu/eli/dir/2010/31/oj
[7] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[8] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[9] https://www.iso.org/standard/27001
[10] https://www.iso.org/standard/71670.html

The MEZeroE Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953157

4 Privacy Implementation Strategy

This chapter translates the legal and regulatory commitments outlined in the previous sections into specific technical and organizational measures implemented across the MEZeroE Virtual Marketplace. The development process, led by R2M Solution as the Data Processor, strictly adheres to the principles of Privacy by Design and by Default.

The platform's privacy strategy governs the collection, processing, and storage of all personal data, ensuring compliance with the General Data Protection Regulation (GDPR). This includes defining clear protocols for data minimization, secure storage, and the explicit management of user consent and rights.

4.1 Privacy by Design and by Default Principles

The MEZeroE Virtual Marketplace integrates the fundamental principles of **Privacy by Design (PbD)** and **Privacy by Default** into the system's architecture from the initial conception phase[11].

- **Privacy by Design (PbD):** Security and privacy controls (e.g., encryption, access controls) are embedded as foundational features of the platform rather than add-ons. This ensures that data protection is an integral part of the core functionality.

- **Privacy by Default:** The platform is configured to process only the minimum amount of personal data necessary to carry out a specific service. For any non-essential data collection, such as website analytics or optional surveys, the default setting is always the most privacy-respecting option (i.e., "opt-out" or "not collected").

GDPR Principles Applied: In alignment with GDPR Article 5, the platform ensures that personal data is processed lawfully, fairly, and transparently. This applies to any information relating to an identified or identifiable natural person, such as names, emails, or location data.

4.2 Data Minimisation and Pseudonymisation/Anonymisation

Compliance with data minimization ensures that only data directly relevant to the MEZeroE ecosystem is collected and retained for the necessary retention period. To protect user privacy during processing, the platform employs specific data sharing techniques adapted from best practices:

1. **Data Minimisation:** Input and output data for Open Innovation Services (OISs) and Pilot Measurement & Verification Lines (PM&VLs) are strictly limited to technical characteristics, test parameters, and project-relevant results, avoiding unnecessary personal identifiers.

2. **Pseudonymisation:** For research data where tracking back to an origin is necessary (e.g., Living Lab longitudinal studies), the platform substitutes the identity of the data subject with a code.

[11] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Additional information required to re-identify the subject is stored separately and securely, ensuring that the data cannot be attributed to a specific individual without the use of this separate key[12].

3. **Anonymisation:** A systematic procedure for irreversible anonymisation is followed for all data intended for long-term storage or public sharing (e.g., in the Success Stories section). This process purges all person-related data that could allow backtracking, ensuring the data subject is no longer identifiable. Once anonymized, the data falls outside the scope of GDPR[13].

4. **Aggregation:** When possible, particularly for energy and comfort analysis, data is aggregated to provide average or cumulative values across a group. This removes personal data entirely, allowing for the detection of trends without risking individual privacy.

5. **Website Usage Data (Cookies):** The website uses cookies solely to monitor navigation via **Matomo**[14]. These cookies contain a unique, non-personal identifier per user. Internet Protocol (IP) anonymization is enabled, ensuring no personal data is shared with third parties. Users are informed via the **iubenda** banner that they may opt-out of tracking or delete cookies at any time.

4.3 Management of Personal Data Collection

Personal data is collected via transparent mechanisms with clear purposes defined at the point of collection.

Standard Platform Collection:

- **Membership Data:** User registration details (Name, Company, Email) are collected strictly for access to platform services and stored securely in the EU territory.

- **Contact Forms:** Inquiries collected via forms are stored in a GDPR-compliant CRM hosted on an Amazon AWS instance in Paris (EU-west-3).

- **Newsletter Subscriptions:** Only email addresses are collected and stored using the Infomaniak platform, which adheres to data privacy standards.

Sensitive Data Collection: For sensitive activities such as **Dataset 1 (Registration details managed via the Profile module)**, **Dataset 2 (Service Request Data)** and **Dataset 6 (Post-occupancy evaluation surveys)**, the last of which involves understanding comfort levels and wellness status of building occupants, a rigorous consent protocol is enforced:

- **Informed Consent:** Prior to any data collection, participants are provided with an **Information Sheet** describing the purpose of research, benefits, risks, and data usage.

[12] https://eur-lex.europa.eu/eli/dir/1995/46/oj
[13] https://amnesia.openaire.eu/
[14] https://matomo.org/

- **Written Consent Form:** Participants must sign a consent form confirming they have understood the project information and voluntarily agree to participate. This form explicitly separates consent for interviews, audio, or video recording.

- **Online Surveys:** For web-based surveys, a "click-to-accept" mechanism is used. Participants must actively click a button indicating they have read the consent information before accessing the questionnaire.

- **Risk Disclosure:** Participants are informed that while confidentiality is protected, online data collection carries inherent risks of external tampering, and they are free to decline answering any specific questions.

4.4 Technical Implementation of User Rights

To ensure users can effectively exercise the rights defined in Chapter 3, the platform implements specific technical mechanisms allowing data owners to maintain control and sovereignty over their data.

- **Autonomous Management (Right to Access & Rectification):** The platform utilizes the **Profile** module to allow users direct, autonomous access to their personal data. Through the "My Profile" section, users can review and update their information (including email addresses) without needing administrative intervention.

- **Consent Management (Right to Withdrawal):**

    - *Cookie Consent:* The **iubenda** plugin allows users to modify their consent preferences for tracking scripts at any time.

- **Data Portability:** Administrative tools have been implemented to generate user data exports in structured, machine-readable formats (e.g., CSV) to satisfy data portability requests.

- **Secure Deletion (Right to Erasure):** The system includes workflows to securely expunge personal data from both the Drupal database and the connected CRM upon user request, provided no overriding legal retention obligations exist.

Secure Access Control: Access to personal data is strictly limited to the designated Data Processor (R2M Solution) and necessary personnel. To prevent unauthorized access:

- **User Account Databases:** Stored separately from research data logic.

- **Password Security:** User passwords are hashed with a random salt before storage, ensuring the password itself is never stored in the database.

The MEZeroE Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953157

- **Audit Logging:** All access to sensitive data is logged via the **logger** module to track processing activities and ensure accountability.

5 Security Measures Implementation Strategy

This chapter details the technical and organizational security measures implemented to protect the MEZeroE Virtual Marketplace and the sensible data it processes. These measures are designed in line with Task 4.2 (platform architecture design and core services implementation), adhering to the security standards outlined in Chapter 3, specifically ISO/IEC 27001 and ISO/IEC 27002.

5.1 Secure Platform Architecture and Core Services

The platform's architecture provides a foundation of security, reliability, and resilience, which is crucial for handling confidential project data and user information.

- **Infrastructure Security & Cloud Base Deployment:** The production environment utilizes Amazon EC2 instances located strictly within European Regions to comply with GDPR data transfer restrictions[15]. Access to the server infrastructure is restricted via AWS Security Groups, allowing traffic only on essential ports (HTTP/HTTPS). The production version utilizes a robust cloud environment to ensure high availability, facilitating the adoption of advanced security services offered by the cloud provider.
- **Modular and Secure Framework:** The application is built upon the well-established **Drupal** open-source framework, which is continually maintained and updated for security. The core framework allows for a monolithic architecture that simplifies security maintenance while supporting logical separation of data layers[16].
- **Input Validation and Control:** A key functionality to mitigate security risks involves the control of the uploaded files and the SQL queries. Strict validation protocols are implemented to sanitize all user-supplied input, including uploaded files and requests, thereby reducing the potential surface of attack from injection and malicious file execution.
- **Hardening Modules:** The platform integrates the SecKit (Security Kit) module[17], which is actively configured to harden the HTTP headers. This implementation provides technical protection against specific attack vectors, including Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and Clickjacking.

5.2 Data access control and user authentication

Access to the platform and its data is governed by strong authentication and authorization protocols to ensure data integrity, confidentiality, and accountability.

- **Secure User Authentication:** The platform implements a secure authentication system aligned with **eIDAS** standards[18], including strong password policies. Additionally, the **reCAPTCHA**

[15] https://aws.amazon.com/compliance/gdpr-center/
[16] https://www.drupal.org/security
[17] https://www.drupal.org/project/seckit
[18] https://eur-lex.europa.eu/eli/reg/2014/910/oj

module[19] can be configured on all entry forms (login, registration) to technically block automated bot attacks and brute-force attempts.

- **Granular Permission Enforcement:** The **SelectRegistrationRole** module is configured to assign specific, limited permissions upon user registration. This ensures that a user registered as a "Manufacturer" is technically restricted at the database query level from accessing data belonging to "OIS Leaders", "PM&VL Leaders", "Living Lab Leaders" or other Manufacturers.
- **Role-Based Access Control (RBAC) and Least Privilege:** A strict RBAC model is employed to enforce the **principle of least privilege**, ensuring users have the **minimum needed privileges to perform tasks in the market**. Access to sensitive platform features and datasets is strictly compartmentalized based on the user's role.
- **Accountability and Logging:** The platform is designed to **control and log access to data**. Comprehensive audit trails and access logs are maintained for all sensitive operations, demonstrating accountability and providing forensic data in the event of an incident.

5.3 Data Storage, Transmission, and Encryption

All sensible data is protected both in transit and at rest, and storage solutions are managed to comply with EU data sovereignty requirements.

- **Secure Transmission (HTTPS):** The system is configured to Force the use of HTTPS (to maintain users' confidentiality) for all data exchanges between the user's browser and the server. This ensures all communication is encrypted via TLS/SSL protocols.
- **Encrypted Data Storage:** Encrypted data storage is utilized for all sensible data, such as raw passwords. This includes volume-level and database encryption for data at rest, mitigating the risk of unauthorized access to stored data.
- **EU Storage Location:** All personal and generated data are hosted on a secure cloud environment within the European Union (e.g., Amazon AWS EU-west-3, Paris).

5.4 Data Backup, Recovery, and Loss Prevention

A continuous backup and recovery plan is maintained, aligning with ISO/IEC 27001 requirements to ensure business continuity and data integrity. The web server is configured to force HTTPS for all connections. All data transmitted between the client browser and the MEZeroE servers is encrypted using TLS 1.2+ protocols, preventing man-in-the-middle attacks and eavesdropping. Full and incremental backups of the database and application files are performed regularly. All backup data is itself encrypted and stored in geographically redundant locations within the EU. Data retention policies are enforced, and formal procedures are maintained for testing data recovery and system restoration on a scheduled basis.

To ensure business continuity and data availability (a key requirement of GDPR), the platform implements automated technical recovery mechanisms.

[19] https://www.drupal.org/project/recaptcha

- **Automated Snapshots:** The AWS environment is configured to perform regular snapshots of the Elastic Block Store (EBS) volumes and the database. These backups are stored in geographically redundant locations within the EU to protect against local data center failures.

Redundant Storage: Critical files are synchronized to a secondary **Google Workspace** environment (configured for Europe-only storage) if required. This system is technically capable of providing a 30-day recovery window for immediate restoration of accidentally deleted or corrupted files.

5.5 Risk Mitigation and Vulnerability Management

Active technical measures are in place to detect and mitigate software vulnerabilities before they can be exploited. Risk management is a continuous process guided by ISO/IEC 27002[20] principles and industry best practices to proactively address vulnerabilities:

- **Secure Development Practices (OWASP):** MEZeroE follows OWASP secure coding best practices during development. All development, testing, and deployment cycles incorporate checks against common web application vulnerabilities defined by the OWASP Top Ten[21].
- **Dependency Validation:** Security risk is mitigated through the careful validation of third-party libraries, tools, APIs and services before they are integrated into the Marketplace. All external components are continuously monitored for known vulnerabilities.
- **System Hardening:** The platform's infrastructure undergoes periodic server updates and hardening. This includes timely application of security patches, disabling unnecessary services, and configuring system settings to minimize the attack surface, in alignment with the NIS Directive.
- **Security Incident Response:** A formal Security Incident Response Plan (SIRP) is maintained to quickly and effectively manage security breaches, ensuring timely notification to the Data Controller and relevant supervisory authorities.
- **Sanitization:** Strict input validation protocols are implemented at the API level. All user-supplied input is sanitized to prevent SQL injection and malicious code execution.
- **Audit Logging:** The **logger** module is enabled to capture comprehensive technical logs of system events. These logs provide a forensic audit trail of who accessed what data and when, which is essential for identifying potential security incidents.

*Note: The governance procedures regarding who reviews these logs and the decision-making process for incident response are detailed in **Deliverable 4.7 (Platform governance and management plan)**.*

[20] https://www.iso.org/standard/75652.html
[21] https://owasp.org/Top10/2025/

6 Conclusion

This deliverable confirms that the MEZeroE Virtual Marketplace has successfully transitioned from a design concept to a secure, operational platform. The data protection measures outlined in this document have been fully implemented and validated, ensuring a trusted environment for stakeholders to exchange sensitive intellectual property and personal data.

The platform utilizes a robust **3-layered architecture** hosted on **AWS Europe**, featuring strict logical segregation between public content and private business data. Comprehensive security controls, including **Role-Based Access Control (RBAC)**, **encrypted storage**, **sanitization** and **audit logging**, are active and operational. Furthermore, the privacy framework explicitly addresses the complexities of sensitive data collection through rigorous consent protocols and pseudonymization techniques validated during the project's pilot phases.

By integrating advanced privacy modules (e.g., iubenda, SecKit, Select Registration Role) and enforcing strict governance protocols, the platform achieves full compliance with the **GDPR** and the **NIS Directive**. This technical foundation ensures that the MEZeroE ecosystem is resilient, legally compliant, and ready to support the long-term open innovation needs of the construction sector.