Data Processing Agreement (DPA) (EN)

Agreement and Appointment as Data Processor for Personal Data Processing (Standard Version)

1. Role of the parties

The **Client** acts as Data Controller of the personal data.
The **Provider** acts as Data Processor pursuant to Art. 28 of Regulation (EU) 2016/679 (GDPR), limited to the data processed in the context of service delivery.

1.1 Processor details

Forma Farm S.r.l. Address: via Savona 10 – 20144 Milan
Referent Name, Title and Contact: Alberto Pastorelli, CEO
Administration Email: amministrazione@formafarm.com

1.2 Data Protection Officer (DPO)

Forma Farm is not subject to the obligation to appoint a Data Protection Officer (DPO) pursuant to Art. 37 of Regulation (EU) 2016/679 (GDPR) and has not appointed one.

1.3 Organizational model and security governance

Forma Farm adopts an internal organizational structure for the management of information security and personal data protection. This structure includes the definition of roles, responsibilities, and operational processes aimed at ensuring compliance with Regulation (EU) 2016/679 (GDPR) and the secure delivery of services.

In particular, the Provider has implemented a structured set of procedures and organizational controls governing:

- access management to systems and data
- secure development and maintenance of platforms
- vulnerability management and security updates
- security incident and data breach management
- backup and business continuity processes

These measures constitute the Provider’s internal security organizational framework and are documented in this DPA and in the technical documentation “Infrastructure & Security Standards”.

1.4 Compliance with Arts. 40–42 GDPR

Forma Farm does not currently adhere to any code of conduct pursuant to Art. 40 GDPR nor holds any certification pursuant to Art. 42.

---

2. Personnel authorized to process data

The Provider uses internal personnel and external collaborators authorized to process personal data pursuant to Art. 29 GDPR.

Such subjects:

- operate under the direct authority of the Provider
- are bound by contractual confidentiality obligations
- receive documented instructions on personal data protection
- access data exclusively for technical purposes related to service delivery, maintenance, and development

Access to data is restricted to authorized personnel only and is granted according to the principle of data minimization.

An updated list of authorized personnel is maintained internally by the Provider and made available to the Data Controller upon request.

2.1 Assistance to the Data Controller

The Processor shall provide the Controller, taking into account the nature of the processing and the information available to it, with reasonably necessary assistance to enable compliance with obligations under Articles 32 to 36 of the GDPR, as well as to handle data subject requests pursuant to Articles 15–22 of the GDPR.

In particular, the Processor supports the Controller in managing:

- security of processing and technical and organizational measures (Art. 32)
- notification of personal data breaches to the supervisory authority (Art. 33)
- communication of data breaches to data subjects (Art. 34)
- data protection impact assessments (DPIA) (Art. 35)
- prior consultations with the supervisory authority (Art. 36)
- requests for the exercise of data subject rights

---

3. Sub-processors

For service delivery, the Provider may engage sub-processors pursuant to Art. 28 GDPR.

3.1 Main sub-processors

- **Cloud provider**: Amazon Web Services (AWS)
  - **Location**: European Union (primary data center: Dublin, Ireland)
  - **Service**: cloud infrastructure and application hosting
  - **Processing**: storage and management of data on infrastructure

The Provider ensures that sub-processors:

- are bound by agreements compliant with Art. 28 GDPR
- implement appropriate technical and organizational measures for personal data protection

The Provider undertakes to keep the list of sub-processors updated and to communicate any changes to the Data Controller upon request or through publication within this documentation.

---

4. Technical and organizational measures (Art. 32 GDPR)

The Provider adopts a set of procedures and technical and organizational measures for information security and personal data protection management.

These measures govern roles and responsibilities, access management, secure development, vulnerability management, incident response, backup, business continuity, and supplier control.

In detail, the Provider implements appropriate measures to ensure a level of security proportional to the risk, including:

- **Access control and authentication**: Access to systems is granted exclusively to authorized personnel through individual credentials, with access profiling and, for administrative accounts, multi-factor authentication.
- **Tracking and logging**: Logging and monitoring systems are implemented for access and system activities, with logs retained for a defined period and protected from unauthorized access.
- **Data encryption**: Personal data is protected through encryption protocols during transmission (TLS) and, where applicable, through encryption of data at rest or backup systems.
- **Backup and disaster recovery**: Periodic backups are performed with restore verification procedures to ensure system availability and resilience.
- **Vulnerability and update management**: Procedures are in place for regular system updates and vulnerability management to ensure an adequate security level.
- **Infrastructure protection** through firewalls and security controls
- **Segregation of environments** (production, testing, development where applicable)

For further details on implemented technical measures, please refer to the dedicated document:

Infrastructure & Security Standards

---

5. Incident and data breach management

The Provider adopts internal procedures for managing security incidents and personal data breaches.

In the event of a personal data breach, the Provider:

- notifies the Data Controller without undue delay
- provides the information necessary to allow the Controller to comply with obligations under Arts. 33 and 34 GDPR

---

6. Data transfers

Personal data are processed within the European Economic Area (EEA).

Any transfers to third countries are carried out in compliance with Chapter V of the GDPR and subject to appropriate safeguards (e.g. Standard Contractual Clauses), where applicable.

---

7. Duration of processing

Personal data processing is limited to the duration of the service provided by the Provider.

Upon termination of the contractual relationship, data will be returned to the Controller upon request or deleted according to the retention periods stated in the “Infrastructure & Security Standards” documentation, unless otherwise required by law.

---

8. Description of personal data processing

8.1 Type of service

The service consists of providing an LMS (Learning Management System) platform in SaaS mode, including hosting, application maintenance, and technical support.

8.2 Categories of data subjects

The personal data processed may relate to:

- LMS platform users (learners)
- teachers / trainers
- platform administrators on the Client side
- Client company contacts

8.3 Categories of personal data

Depending on the Client’s configuration, the following may be processed:

- personal data (name, surname)
- contact data (email)

- access credentials (username, encrypted password)
- platform usage data (access logs, performed activities)
- training-related data (courses attended, results, progress)

8.4 Special categories of data (if any)

The service is not designed to process special categories of personal data.

However, the Client may upload content including special categories of data. In such cases:

- processing is carried out under the Client’s responsibility
- the Provider applies appropriate technical measures for data protection

---

8.5 Nature of processing

Processing consists of:

- collection and recording of data
- organization and storage
- consultation and use
- possible deletion or anonymization

Processing is carried out exclusively for technical and operational purposes related to service delivery.

8.6 Purposes of processing

Personal data are processed for:

- provision and management of the LMS platform
- user authentication and management
- tracking of training activities
- technical assistance and support
- system security and monitoring

8.7 Data retention and deletion

Data are processed for the entire duration of the contractual relationship with the Client.

Upon termination of the service:

- data are deleted or returned upon request
- they may be temporarily retained in backup systems according to the Provider’s technical policies

---

8.8 Scope of processing by sub-processors

Sub-processors process data exclusively for:

- hosting the infrastructure
- ensuring system availability and security

They do not carry out processing for their own purposes.

---

9. Audit and verification

The Provider makes available to the Data Controller the information necessary to demonstrate compliance with GDPR obligations.

The Controller may request audits or verification activities, which shall be agreed in advance between the parties and carried out in such a way as not to compromise system security and the confidentiality of other clients.

In particular:

- audits must be notified with reasonable advance notice
- they must be limited to aspects relevant to personal data processing
- they may be conducted directly by the Controller or by appointed third parties
- they must not involve direct access to production systems, unless otherwise agreed

The Provider undertakes to cooperate in good faith and to provide documentary evidence of the technical and organizational measures implemented.

Revision #4
Created 2026-04-08 19:26:59 UTC by Alberto Pastorelli
Updated 2026-06-28 18:58:04 UTC by Alberto Pastorelli