Privacy & GDPR

- Data Processing Agreement (DPA) (IT)
- Data Processing Agreement (DPA) (EN)
- Default Cookie Policy

Data Processing Agreement (DPA) (IT)

Accordo e Nomina a Responsabile per il trattamento dei dati personali (versione standard)

1. Ruolo delle parti

Il Cliente agisce in qualità di Titolare del trattamento dei dati personali.
Il Fornitore agisce in qualità di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR), limitatamente ai dati trattati nell'ambito dell'erogazione del servizio.

1.1 Dati del responsabile

Forma Farm S.r.l. Indirizzo: via Savona 10 – 20144 Milano Nome, qualifica e dati di contatto del referente: Alberto Pastorelli, Amministratore Delegato Indirizzo mail amministrazione@formafarm.com

1.2 Data Protection Officer (DPO)

Forma Farm non è soggetta all'obbligo di nomina del Data Protection Officer (DPO) ai sensi dell'art. 37 del Regolamento (UE) 2016/679 (GDPR) e non ha proceduto alla sua designazione.

1.3 Modello organizzativo e governance della sicurezza

Forma Farm adotta un assetto organizzativo interno per la gestione della sicurezza delle informazioni e della protezione dei dati personali. Tale assetto include la definizione di ruoli,

responsabilità e processi operativi finalizzati a garantire la conformità al Regolamento (UE) 2016/679 (GDPR) e la gestione sicura dei servizi erogati.

In particolare, il Fornitore ha implementato un insieme strutturato di procedure e controlli organizzativi che disciplinano:

- la gestione degli accessi ai sistemi e ai dati
- lo sviluppo e la manutenzione sicura delle piattaforme
- la gestione delle vulnerabilità e degli aggiornamenti di sicurezza
- la gestione degli incidenti di sicurezza e dei data breach
- i processi di backup e business continuity

Tali misure costituiscono il framework organizzativo interno di sicurezza del Fornitore e sono documentate nel presente DPA e nella documentazione tecnica “Infrastructure & Security Standards”.

1.4 Conformità art. 40–42 GDPR

Forma Farm non aderisce attualmente a un codice di condotta ai sensi dell'art. 40 del GDPR né dispone di una certificazione ai sensi dell'art. 42.

---

2. Personale autorizzato al trattamento

Il Fornitore si avvale di personale interno e collaboratori esterni autorizzati al trattamento dei dati personali ai sensi dell’art. 29 del GDPR.

Tali soggetti:

- operano sotto la diretta autorità del Fornitore
- sono vincolati da obblighi di riservatezza contrattuali
- ricevono istruzioni documentate in materia di protezione dei dati personali
- accedono ai dati esclusivamente per finalità tecniche connesse all’erogazione, manutenzione e sviluppo del servizio

L’accesso ai dati è limitato ai soli soggetti autorizzati e avviene secondo il principio di minimizzazione.

L’elenco aggiornato dei soggetti autorizzati è mantenuto internamente dal Fornitore ed è reso disponibile al Titolare su richiesta.

2.1 Assistenza al Titolare del trattamento

Il Responsabile presta al Titolare, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, l’assistenza ragionevolmente necessaria per consentire l’adempimento degli obblighi previsti dagli articoli da 32 a 36 del GDPR, nonché per la gestione delle richieste degli interessati ai sensi degli articoli 15–22 del GDPR.

In particolare, il Responsabile supporta il Titolare nella gestione di:

sicurezza del trattamento e misure tecniche e organizzative (art. 32) notifiche di violazioni dei dati personali all’autorità di controllo (art. 33) comunicazioni di data breach agli interessati (art. 34) valutazioni di impatto sulla protezione dei dati (DPIA) (art. 35) consultazioni preventive con l’autorità di controllo (art. 36) richieste di esercizio dei diritti da parte degli interessati

---

3. Sub-responsabili del trattamento

Per l’erogazione dei servizi, il Fornitore può avvalersi di sub-responsabili del trattamento ai sensi dell’art. 28 GDPR.

3.1 Sub-responsabili principali

- Provider cloud: Amazon Web Services (AWS)
  - Localizzazione: Unione Europea (data center primario: Dublino, Irlanda)
  - Servizio: infrastruttura cloud e hosting applicativo
  - Trattamento: conservazione e gestione dei dati su infrastruttura

Il Fornitore garantisce che i sub-responsabili:

- siano vincolati da accordi conformi all’art. 28 GDPR
- adottino misure tecniche e organizzative adeguate alla protezione dei dati personali

Il Fornitore si impegna a mantenere aggiornato l’elenco dei sub-responsabili e a comunicarne eventuali modifiche al Titolare su richiesta o tramite pubblicazione nella presente documentazione.

---

4. Misure tecniche e organizzative (Art. 32 GDPR)

Il Fornitore adotta un insieme di procedure e misure tecniche e organizzative per la gestione della sicurezza delle informazioni e della protezione dei dati personali.

Tali misure disciplinano ruoli e responsabilità, gestione degli accessi, sviluppo sicuro, gestione delle vulnerabilità, incident response, backup, business continuity e controllo dei fornitori.

Nel dettaglio, il Fornitore adotta misure adeguate per garantire un livello di sicurezza proporzionato al rischio, tra cui:

- **Controllo accessi e autenticazione**: Accesso ai sistemi consentito esclusivamente a personale autorizzato tramite credenziali individuali, con profilazione degli accessi e, per gli account amministrativi, autenticazione a più fattori.
- **Tracciamento e logging**: Sono implementati sistemi di logging e monitoraggio degli accessi e delle attività sui sistemi, con conservazione dei log per un periodo definito e protezione da accessi non autorizzati.
- **Cifratura dei dati**: I dati personali sono protetti mediante protocolli di cifratura durante la trasmissione (TLS) e, ove applicabile, tramite cifratura dei dati a riposo o dei sistemi di backup.
- **Backup e disaster recovery**: Sono effettuati backup periodici dei dati con procedure di verifica del ripristino, al fine di garantire la disponibilità e la resilienza dei sistemi.
- **Gestione delle vulnerabilità e aggiornamenti**: Sono adottate procedure per l'aggiornamento periodico dei sistemi e per la gestione delle vulnerabilità, al fine di garantire un livello di sicurezza adeguato.
- **Protezione dell'infrastruttura** mediante firewall e controlli di sicurezza • Segregazione degli ambienti (produzione, test, sviluppo ove applicabile)

Per maggiori dettagli sulle misure tecniche implementate si può fare riferimento al documento apposito: **Infrastructure & Security Standards**

---

5. Gestione degli incidenti e data breach

Il Fornitore adotta procedure interne per la gestione degli incidenti di sicurezza e delle violazioni dei dati personali.

In caso di violazione dei dati personali, il Fornitore:

- ne dà comunicazione al Titolare senza ingiustificato ritardo
- fornisce le informazioni necessarie per consentire al Titolare di adempiere agli obblighi previsti dagli artt. 33 e 34 del GDPR

---

6. Trasferimenti di dati

I dati personali sono trattati all’interno dello Spazio Economico Europeo.

Eventuali trasferimenti verso paesi terzi avvengono nel rispetto del Capo V del GDPR e mediante adeguate garanzie (es. clausole contrattuali standard), ove applicabili.

---

7. Durata del trattamento

Il trattamento dei dati personali è limitato alla durata del servizio erogato dal Fornitore.

Al termine del rapporto contrattuale i dati saranno restituiti al Titolare su richiesta, o cancellati secondo i tempi di retention dichiarati nella documentazione di "Infrastructure & Security Standards", salvo obblighi di legge.

---

8. Descrizione del trattamento dei dati personali

8.1 Tipologia di servizio

Il servizio consiste nell’erogazione di una piattaforma LMS (Learning Management System) in modalità SaaS, comprensiva di hosting, manutenzione applicativa e supporto tecnico.

8.2 Categorie di interessati

I dati personali trattati possono riguardare:

- utenti della piattaforma LMS (discenti)
- docenti / formatori
- amministratori della piattaforma lato Cliente
- referenti aziendali del Cliente

8.3 Categorie di dati personali

A seconda della configurazione del Cliente, possono essere trattati:

- dati anagrafici (nome, cognome)
- dati di contatto (email)

- credenziali di accesso (username, password cifrata)
- dati di utilizzo della piattaforma (log di accesso, attività svolte)
- dati relativi alla formazione (corsi frequentati, risultati, progressi)

8.4 Dati particolari (se presenti)

Il servizio non è progettato per il trattamento di categorie particolari di dati personali.

Tuttavia, il Cliente può caricare contenuti che includano dati particolari. In tal caso:

- il trattamento avviene sotto la responsabilità del Cliente
- il Fornitore applica misure tecniche adeguate alla protezione dei dati

---

8.5 Natura del trattamento

Il trattamento consiste in:

- raccolta e registrazione dei dati
- organizzazione e conservazione
- consultazione e utilizzo
- eventuale cancellazione o anonimizzazione

Il trattamento è effettuato esclusivamente per finalità tecniche e operative connesse all’erogazione del servizio.

8.6 Finalità del trattamento

I dati personali sono trattati per:

- erogazione e gestione della piattaforma LMS
- autenticazione e gestione degli utenti
- tracciamento delle attività formative
- assistenza tecnica e supporto
- sicurezza e monitoraggio dei sistemi

8.7 Conservazione e cancellazione dei dati

I dati sono trattati per tutta la durata del rapporto contrattuale con il Cliente.

Alla cessazione del servizio:

- i dati vengono cancellati o restituiti su richiesta
- possono essere conservati temporaneamente nei sistemi di backup secondo le politiche tecniche del Fornitore

---

8.8 Ambito del trattamento da parte dei sub-responsabili

I sub-responsabili del trattamento trattano i dati esclusivamente per:

- ospitare l’infrastruttura
- garantire disponibilità e sicurezza dei sistemi

Non effettuano trattamenti per finalità proprie.

9. Audit e verifiche

Il Fornitore mette a disposizione del Titolare le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal GDPR.

Il Titolare può richiedere verifiche o attività di audit, che saranno concordate preventivamente tra le parti e svolte secondo modalità tali da non compromettere la sicurezza dei sistemi e la riservatezza di altri clienti.

In particolare:

- gli audit devono essere notificati con un preavviso ragionevole
- devono essere limitati agli aspetti rilevanti per il trattamento dei dati personali
- possono essere effettuati direttamente dal Titolare o tramite soggetti terzi incaricati
- non devono comportare accesso diretto ai sistemi produttivi, salvo diverso accordo

Il Fornitore si impegna a collaborare in buona fede e a fornire evidenze documentali delle misure tecniche e organizzative adottate.

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.

Default Cookie Policy

Cookie Policy – Forma Cloud

This Cookie Policy explains how Forma Cloud uses cookies and similar technologies within the platform.

Cookies are small text files stored on a user’s device or browser during navigation. They are commonly used to ensure the proper operation of web applications, maintain authenticated sessions, remember user preferences, and support security-related features.

By default Forma Cloud uses exclusively technical and functional first-party cookies, and may use analytics cookies if optionally set by an administrator. The platform does not use third-party cookies, advertising cookies, or profiling technologies.

Types of Cookies Used

Forma Cloud uses three categories of technical cookies:

Session Cookies

Session cookies are temporary cookies that are automatically deleted when the browser is closed. These cookies are required to maintain active user sessions and ensure secure navigation throughout the platform.

Functional Cookies

Functional cookies are persistent cookies used to remember user preferences and improve usability. Examples include accessibility settings or interface preferences selected by the user.

Optional Tracking Cookies (Google Analytics)

The platform allows administrators to optionally integrate **Google Analytics** for usage analysis and reporting. This feature is provided as an optional tool and is not required for the core operation of the service.

- **Manual Activation:** Tracking cookies are **not active by default**. They are only triggered if the administrator explicitly enters a Tracking ID or configures the integration within the platform's administrative settings.
- **User Consent & Responsibility:** By enabling these features, the administrator acknowledges the responsibility to inform end-users and ensure that such processing aligns with their specific privacy governance. The acceptance of this Cookie Policy, in conjunction with the Privacy Policy, covers the optional use of these tools when configured.
- **Data Usage:** If activated, Google Analytics cookies (such as `_ga` and `_gid`) collect site traffic data. This information is transmitted to and stored by Google on servers that may be located outside the European Economic Area (EEA).
- **Opt-Out:** Users who wish to avoid tracking, even when enabled by the administrator, can do so by adjusting their browser settings or by installing the Google Analytics Opt-out Browser Add-on.

Default Cookies Used by Forma Cloud

#	Cookie Name	Purpose	Duration	HttpOnly	Secure	SameSite
1	`FORMALMS`	User session management over HTTP connections	2 hours (configurable)	Yes	No	Lax
2	`__Secure-FORMALMS`	User session management over HTTPS connections	2 hours (configurable)	Yes	Yes	Lax
3	`docebo_cookie_data[high_accessibility]`	Stores advanced accessibility preference during login	365 days	No	No	–
4	`high_contrast`	Stores high contrast accessibility preference	Session	No	No	–
5	`{userId}.my_course.category`	Stores selected course category filter in “My Courses” page	365 days	No	No	–

Additional Notes

- Cookies `FORMALMS` and `__Secure-FORMALMS` are mutually exclusive and used depending on the connection protocol (HTTP vs HTTPS).
- The cookie `{userId}.my_course.category` is dynamic: `{userId}` corresponds to the numeric ID of the logged-in user (e.g. `42.my_course.category`).
- Forma Cloud does not use third-party cookies, analytics cookies, advertising cookies, or profiling technologies.
- No cookies contain personal data in plain text. Session cookies contain only opaque technical tokens required for authentication and session management.

Managing Cookies

Users can manage cookie preferences through their browser settings. Typical options include:

- viewing stored cookies
- deleting cookies
- blocking specific cookies
- disabling all cookies

Disabling technical cookies may prevent parts of the platform from functioning correctly.

Browser-specific documentation is available from:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari
- Opera

Updates to This Policy

This Cookie Policy may be updated periodically to reflect technical, operational, or legal changes.

The latest version published on the platform is always considered the current one.

For more information about personal data processing, please refer to the Forma Cloud Privacy Policy.