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 Raffaello Barbiera 12 - 20153 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.

Revision #22
Created 2026-03-14 16:22:22 UTC by Alberto Pastorelli
Updated 2026-10-24 17:32:38 UTC by Massimiliano Ferrari