STIMPILOT · LEGAL PACK 2.1 · UP ADV

Accordo sul trattamento dei dati personali

Art. 28 Regolamento (UE) 2016/679

Versione 2.1 · 12 novembre 2026

1 Parti e incorporazione

Il presente DPA intercorre tra il Cliente quale Titolare, identificato nei dati di fatturazione e di contatto dell'ordine, e Lorenzo Zenobi quale Responsabile tecnico, Via del Fontanile Arenato 270, 00163 Roma, contatto lorenzo.zenobi@stimpilot.it, PEC l.zenobi@pec.archrm.it.

Il DPA è incorporato nell'ordine e si applica ai dati personali inseriti dal Cliente nei Progetti, nei documenti e nelle richieste AI. Il Rivenditore, identificato nell'ordine, vende in nome proprio ma non riceve l'incarico di trattare i contenuti tecnici: accede soltanto ai dati amministrativi e commerciali per proprie finalità. Se l'effettiva organizzazione diverge, il DPA deve essere adattato prima dell'uso.

Lorenzo Zenobi propone e assume direttamente gli obblighi di questo DPA mediante la sua messa a disposizione nella versione attiva del servizio da lui autorizzata. Il Cliente aderisce con l'accettazione documentata dell'ordine, che identifica le parti, la versione e la data. UP ADV non assume tali obblighi in nome di Lorenzo Zenobi e non diventa responsabile dei contenuti tecnici. La prova dell'adesione è conservata con i documenti dell'ordine.

Per finalità autonome di account, sicurezza o gestione commerciale si applica la Privacy Policy e non il presente incarico.

2 Oggetto durata natura e finalità

Il trattamento consiste nell'hosting, memorizzazione, organizzazione, elaborazione parametrica, visualizzazione, generazione di report, trasmissione tecnica, backup/disaster recovery, assistenza e cancellazione dei dati necessari a erogare il Servizio. La durata coincide con il rapporto contrattuale e con i periodi tecnici di cancellazione previsti al termine.

3 Istruzioni del Cliente

Il Responsabile tratta i dati soltanto su istruzioni documentate del Cliente, che sono costituite dal contratto, dalle configurazioni e dalle azioni eseguite dagli Utenti nel Servizio, salvo obblighi di legge. Se il Responsabile ritiene che un'istruzione violi la normativa sulla protezione dei dati, ne informa il Cliente salvo divieto legale e può sospendere l'istruzione fino a chiarimento.

4 Obblighi del Cliente

Il Cliente garantisce di essere legittimato a trattare e far trattare i dati, di aver fornito le informative necessarie, di impartire istruzioni lecite e di non usare il Servizio per categorie di dati non compatibili con il suo livello di rischio senza preventiva valutazione. Il Cliente determina finalità, basi giuridiche, tempi sostanziali di conservazione e categorie di interessati e risponde delle richieste degli interessati.

5 Riservatezza e persone autorizzate

Il Responsabile assicura che le persone autorizzate al trattamento siano vincolate alla riservatezza o a un obbligo legale equivalente e accedano ai dati solo nella misura necessaria alle proprie mansioni.

6 Misure di sicurezza

Tenuto conto dello stato dell'arte, dei costi, della natura dei dati e dei rischi, il Responsabile mantiene misure tecniche e organizzative adeguate. Le misure essenziali previste sono riepilogate nell'Allegato B e possono evolvere nel tempo senza ridurre materialmente il livello complessivo di protezione.

7 Sub responsabili

Il Cliente autorizza in via generale soltanto i sub responsabili identificati nell'Allegato C e nel documento 07, per le funzioni ivi descritte. I fornitori che agiscono come titolari autonomi sono distinti e non diventano sub responsabili per il solo fatto di essere elencati.

Il Responsabile impone ai sub responsabili, mediante atto scritto, obblighi coerenti con l'articolo 28 GDPR, conserva la responsabilità prevista dal paragrafo 4 di tale articolo e verifica i trasferimenti pertinenti. Per aggiunte o sostituzioni informa preventivamente il Cliente con almeno 15 giorni di preavviso e gli consente un'obiezione motivata entro 10 giorni dalla comunicazione. Le parti cercano una soluzione; in mancanza la funzione coinvolta non viene utilizzata sui dati di quel Cliente o si concorda la cessazione pertinente.

Le entità contrattuali, sedi e garanzie mancanti nell'elenco devono essere completate prima di trattare dati per conto del Cliente. Il riferimento a una categoria di provider non sostituisce l'identificazione richiesta.

8 Trasferimenti internazionali

Il Responsabile non effettua o consente trasferimenti di dati fuori dallo SEE se non in presenza di una base valida ai sensi del capo V GDPR, quali decisione di adeguatezza, clausole contrattuali standard o altra garanzia applicabile. Quando necessario, adotta misure supplementari proporzionate e mette a disposizione del Cliente le informazioni pertinenti compatibilmente con gli obblighi di riservatezza dei fornitori.

9 Assistenza per i diritti degli interessati

Tenuto conto della natura del trattamento, il Responsabile assiste il Cliente con misure tecniche e organizzative ragionevoli per rispondere a richieste di accesso, rettifica, cancellazione, limitazione, portabilità o opposizione. Se riceve direttamente una richiesta relativa a dati trattati per conto del Cliente, la inoltra al Cliente senza rispondere nel merito salvo istruzione o obbligo di legge.

10 Violazioni di dati personali

Il Responsabile informa il Cliente senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione di dati personali che riguardi i dati trattati per conto del Cliente e fornisce, per quanto disponibile, le informazioni utili a valutare obblighi di notifica/comunicazione. La comunicazione non costituisce ammissione di responsabilità. Il Cliente resta responsabile delle notifiche all'autorità e agli interessati quando agisce quale titolare.

11 DPIA consultazioni e compliance

Il Responsabile fornisce assistenza ragionevole, tenuto conto delle informazioni disponibili e della natura del trattamento, per valutazioni d'impatto e consultazioni preventive con l'autorità quando il trattamento del Cliente lo richieda. Attività straordinarie, personalizzate o eccedenti la normale assistenza possono essere oggetto di accordo economico separato, salvo obblighi inderogabili.

12 Audit e informazioni

Il Responsabile mette a disposizione le informazioni ragionevolmente necessarie a dimostrare il rispetto dell'art. 28 GDPR. Salvo incidenti, richieste dell'autorità o comprovate ragioni di non conformità, gli audit del Cliente sono preferibilmente documentali o remoti, non più di una volta all'anno, con almeno 30 giorni di preavviso, durante orari lavorativi e senza compromettere sicurezza, segreti o dati di altri clienti. I costi straordinari dell'audit sono a carico del Cliente, salvo accertata non conformità significativa imputabile al Responsabile.

13 Restituzione e cancellazione

Alla cessazione, a scelta del Cliente, il Responsabile restituisce o cancella i dati personali trattati per suo conto ed elimina le copie esistenti, salvo conservazione imposta dal diritto dell'Unione o nazionale. La restituzione avviene con le esportazioni disponibili e, ove necessario per adempiere l'articolo 28 GDPR, con modalità concordate idonee; non si promette un formato di esportazione non disponibile.

Il termine operativo previsto per i dati attivi è di 30 giorni dalla richiesta o dalla cessazione secondo le istruzioni concordate. Le copie di backup seguono la rotazione delle ultime 30 copie giornaliere e 4 settimanali; la cancellazione dai backup avviene nel ciclo di rotazione, salvo conservazione imposta dalla legge. Le copie residue restano isolate dall'uso ordinario.

La mera indisponibilità all'Utente non equivale a cancellazione. Le copie residue restano soggette agli obblighi del DPA e non possono essere utilizzate per altre finalità; ogni obbligo legale di conservazione è comunicato al Cliente ove consentito.

14 Responsabilità

La responsabilità contrattuale tra le parti è disciplinata dai Termini del Servizio, fermo restando che il presente DPA non limita i diritti degli interessati, i poteri delle autorità o responsabilità che il GDPR rende inderogabili. Ciascuna parte risponde dei propri obblighi e delle istruzioni, decisioni o violazioni a essa imputabili.

15 Prevalenza

In caso di conflitto tra DPA e Termini su materie di protezione dei dati trattati per conto del Cliente, prevale il DPA. Per il resto prevalgono i documenti secondo l'ordine stabilito nei Termini.

Allegato A Dettagli del trattamento

Voce	Descrizione
Interessati	Personale e collaboratori del Cliente; clienti/committenti; professionisti; referenti; proprietari o soggetti collegati ai Progetti solo se il Cliente inserisce i relativi dati.
Categorie di dati	Dati identificativi e di contatto; indirizzi e localizzazioni di progetto; riferimenti catastali; dati contenuti in documenti caricati; metadati e contenuti necessari all'elaborazione.

Categorie particolari	Non previste come necessarie. Il Cliente deve evitarne l'inserimento salvo necessità, liceità e preventiva valutazione.
Operazioni	Raccolta tramite upload/inserimento, hosting, organizzazione, elaborazione, consultazione, generazione report, trasmissione a sub-responsabili strettamente necessari, backup e cancellazione.
Finalità	Erogazione delle funzioni SaaS richieste dal Cliente, assistenza autorizzata, sicurezza e continuità tecnica.
Durata	Rapporto contrattuale + finestre tecniche di cancellazione definite nel DPA/Termini.

Allegato B Misure tecniche e organizzative essenziali

- Cifratura TLS/HTTPS delle comunicazioni verso l'applicazione.
- Password memorizzate mediante funzioni di hashing robuste e gestione sicura delle credenziali.
- Accessi amministrativi limitati secondo principio del minimo privilegio; autenticazione forte/MFA ove supportata e per gli account amministrativi critici.
- Segregazione logica dei dati per account/progetto e controlli di autorizzazione applicativi.
- Sono previste copie dei dati quotidiane e copie complete settimanali. La politica di conservazione prevede le ultime 30 copie giornaliere e le ultime 4 copie settimanali. La presenza dei backup non garantisce l'assenza di perdita dei dati né il recupero di uno specifico contenuto.
- Logging e monitoraggio di eventi di autenticazione, errori e attività rilevanti per la sicurezza.
- Gestione di aggiornamenti, patch e vulnerabilità dell'infrastruttura e delle dipendenze software.
- Gestione dei segreti e delle chiavi API fuori dal codice client e limitazione delle autorizzazioni.
- Procedure di gestione incidenti e canale per escalation privacy/sicurezza.
- Processi di cancellazione e disattivazione account coerenti con i periodi dichiarati.

Allegato C Sub responsabili

L'elenco aggiornato è mantenuto nel documento "Elenco fornitori e sub-responsabili STIMPILOT". Prima del go-live devono essere verificati entità contrattuali, ruoli, ubicazione del trattamento, DPA e meccanismi di trasferimento effettivamente applicabili.

Allegato D Funzioni AI

I dati dei Clienti non sono utilizzati da StimPilot per training o affinamento AI; è vietato autorizzare il provider a tali usi. Trasmissione e conservazione API sono disciplinate nel documento 09 e nel DPA. Non viene promessa conservazione zero né una configurazione provider non verificata.

L'attivazione volontaria della funzione da parte del Cliente costituisce istruzione di trasmettere i dati strettamente necessari al sub responsabile AI autorizzato. Il Responsabile non utilizza i dati per finalità di training proprie né permette opt in del provider per tale finalità. Il Cliente minimizza e, quando possibile, anonimizza i dati; sono esclusi dati particolari o giudiziari non previamente concordati e adeguatamente tutelati.

Per richieste degli interessati, cancellazione, trasferimenti, incidenti e assistenza continuano ad applicarsi le clausole del presente DPA; la natura AI non le deroga.