ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI (DATA PROCESSING AGREEMENT – DPA EX ART. 28 GDPR)

Data di Entrata in Vigore: 01/2026 — **Ultimo Aggiornamento:** 11/2026

Contatto Privacy e DPO: privacy@loricai.io

Il presente Accordo sul Trattamento dei Dati Personali ("DPA") è stipulato ai sensi dell'Articolo 28 del Regolamento (UE) 2016/679 ("GDPR"), dello UK GDPR e della Legge federale svizzera sulla protezione dei dati ("nLPD") tra:

Il Cliente (azienda, studio professionale o professionista che sottoscrive i Termini di Servizio o un Ordine Commerciale/Prova Tecnica), in qualità di **Titolare del Trattamento** ("Titolare" o "Data Controller"); e

DEXIMA TECH LLC, con sede legale in 5830 E 2nd St, Ste 7000 #32263, Casper, Wyoming 82609, USA, in qualità di **Responsabile del Trattamento** ("Responsabile", "Società" o "Data Processor").

Il presente DPA costituisce parte integrante e sostanziale dei Termini di Servizio ("ToS") e dell'Informativa Globale sulla Privacy ("Privacy Policy") di LoricAI.

ARTICOLO 1 – PRIMATO DELLE SPECIFICHE TECNICHE E DEFINIZIONI

1.1. Integrazione Sistematica e Principio di Impossibilità Tecnica.

Le Parti riconoscono che l'esecuzione del presente DPA si fonda sull'architettura tecnica *Zero-Knowledge* e *Confidential Computing* di LoricAI. Ogni obbligo previsto dal presente DPA deve essere interpretato ed eseguito in conformità al principio di incapacità tecnica di accesso in chiaro ai contenuti da parte del Responsabile.

1.2. Definizioni Vincolanti.

Ai fini del presente DPA si applicano le medesime definizioni di cui alla Sezione 1 della Privacy Policy e all'Articolo 2 dei ToS:

"Blind Conduit (Condotto Cieco)": Qualifica tecnica e giuridica del Responsabile quale fornitore di infrastruttura di calcolo ed elaborazione crittografata, matematicamente impossibilitato a visualizzare, decifrare o conoscere in chiaro il contenuto dei Dati di Payload.

"Architettura Zero-Knowledge e Confidential Computing (TEE)": Infrastruttura in cui i Dati di Payload sono protetti da cifratura sul dispositivo durante il trasferimento e la permanenza in archivio, le chiavi di decrittazione (DEK/KEK) sono gestite separatamente tramite **Google Cloud KMS (regione UE)** sotto vincolo di *Key Release Policy*, e la decrittazione temporanea avviene esclusivamente all'interno della memoria volatile isolata (RAM/VRAM) di enclavi hardware **CPU AMD con tecnologia SEV-SNP** e **GPU NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200** situate fisicamente in **Finlandia (Unione Europea)**.

"Dati di Payload": Qualsiasi file, documento, pratica, input di testo (prompt), query, frammento audio, immagine o contenuto caricato o generato dal Titolare o dai suoi utenti autorizzati all'interno degli spazi di lavoro per l'elaborazione, ivi inclusi gli eventuali dati personali o categorie particolari di dati (Art. 9 GDPR) o dati soggetti a segreto professionale in essi contenuti.

ARTICOLO 2 – OGGETTO, DURATA, NATURA E DETTAGLI DEL TRATTAMENTO (ART. 28.3 GDPR)

2.1. Oggetto e Finalità. Il trattamento effettuato dal Responsabile consiste esclusivamente nella messa a disposizione dell'infrastruttura *Confidential Computing* in Finlandia (UE), nell'archiviazione cifrata delle pratiche (su Cloudflare R2 e database vettoriale isolato Qdrant in regione UE), nella gestione delle copie di sicurezza cifrate (su Backblaze B2 in regione UE) e nell'esecuzione locale all'interno dell'enclave hardware dei modelli linguistici (es. *Qwen 3.6 Flash Next*) al solo fine di erogare il Servizio LoricAI richiesto dal Titolare. È tassativamente escluso qualsiasi utilizzo dei Dati di Payload per l'addestramento o il miglioramento di modelli di intelligenza artificiale (*No AI Training*).

2.2. Durata. Il presente DPA decorre dall'attivazione dell'account, dell'Ordine Commerciale o della Prova Tecnica Preliminare e resta in vigore fino alla completa Cancellazione Crittografica dei Dati di Payload ai sensi dell'Articolo 11.

2.3. Categorie di Interessati e Tipologia di Dati Personali. Poiché il Responsabile opera in modalità *Zero-Knowledge* senza accesso in chiaro ai Dati di Payload, le categorie di Interessati e di Dati Personali dipendono esclusivamente dai documenti caricati dal Titolare negli spazi di lavoro e possono includere, a discrezione del Titolare: clienti, pazienti, assistiti, dipendenti, fornitori, controparti contrattuali o terzi menzionati nelle pratiche; dati identificativi, di contatto, contrattuali, finanziari, giudiziari nonché categorie particolari di dati personali di cui all'Art. 9 del GDPR (es. dati sanitari o psicologici).

2.4. Ciclo di Elaborazione nell'Enclave e VRAM Scrubbing. Per elaborare una richiesta del Titolare, i Dati di Payload vengono decifrati esclusivamente all'interno della memoria volatile isolata (RAM/VRAM) dell'enclave hardware autorizzata per il tempo strettamente necessario a completare l'inferenza (con *Time-To-Live* dei buffer inattivi post-inferenza non superiore a 60 secondi). Al termine di ciascuna richiesta, il sistema esegue forzatamente l'azzeramento crittografico della memoria GPU (cudaMemset(ptr, 0, size) e cudaDeviceReset()) e la pulizia della memoria volatile allocata (*VRAM Scrubbing*), garantendo l'assenza totale di residui forensi in chiaro.

ARTICOLO 3 – OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO (ART. 28 GDPR)

3.1. Trattamento su Istruzione Documentata (Art. 28.3.a GDPR). Il Responsabile tratta i Dati di Payload esclusivamente su istruzione documentata del Titolare — costituita dal presente DPA, dai ToS e dai comandi tecnici impartiti dal Titolare tramite l'interfaccia del Software — salvo che lo richieda il diritto dell'Unione o degli Stati membri; in tal caso, il Responsabile informa tempestivamente il Titolare prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico. Il Responsabile informa immediatamente il Titolare qualora ritenga che un'istruzione violi il GDPR o altre disposizioni applicabili.

3.2. Riservatezza e Barriere Hardware (Art. 28.3.b GDPR). Il Responsabile garantisce che tutte le persone autorizzate a gestire l'infrastruttura siano vincolate da rigorosi obblighi contrattuali o legali di riservatezza. Le Parti danno atto che la riservatezza dei Dati di Payload è primariamente imposta da barriere fisiche nel silicio (*Hardware Root of Trust* AMD e NVIDIA) che impediscono tecnicamente anche agli amministratori di sistema del Responsabile di accedere ai dati in chiaro.

3.3. Misure Tecniche e Organizzative di Sicurezza (Art. 28.3.c e Art. 32 GDPR). Il Responsabile adotta e mantiene le misure di sicurezza di livello stato dell'arte descritte nelle Sezioni 1, 2 e 3 della Privacy Policy e nella documentazione di verifica tecnica, tra cui: (i) cifratura sul dispositivo in transito (TLS 1.3) e in archivio (AES-256-GCM); (ii) isolamento *Confidential Computing* su CPU AMD SEV-SNP e GPU NVIDIA RTX PRO 6000 Blackwell / B200 in Finlandia; (iii) separazione delle chiavi su Google Cloud KMS (regione UE) con *Key Release Policy* vincolata all'Attestazione Remota; (iv) *VRAM Scrubbing* automatico a fine sessione; (v) separazione logica degli ambienti tramite *Blind Indexing* (HMAC-SHA256).

3.4. Assistenza per Diritti degli Interessati, DPIA e Consultazione Preventiva (Art. 28.3.e–f GDPR). Tenuto conto della natura *Zero-Knowledge* del trattamento:

(a) Richieste degli Interessati (Artt. 15–22 GDPR): Poiché il Responsabile non può decifrare i Dati di Payload, l'estrazione, la rettifica, la portabilità e la cancellazione dei documenti sono garantite nativamente al Titolare in totale autonomia tramite le funzioni della piattaforma (Art. 7.4 Privacy Policy). Il Responsabile assiste il Titolare fornendo ogni necessaria attestazione tecnica sull'infrastruttura;

(b) Valutazione d'Impatto (DPIA ex Art. 35 GDPR) e Consultazione Preventiva (Art. 36 GDPR): Il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi di cui agli Artt. 32–36 del GDPR mettendo a disposizione tutta la documentazione architetturale, le guide di verifica dell'Attestazione Remota AMD/NVIDIA e le informazioni sulle misure crittografiche adottate.

ARTICOLO 4 – OBBLIGHI E RESPONSABILITÀ DEL TITOLARE (IL CLIENTE)

4.1. Liceità del Trattamento e Titolarità dei Dati. Il Titolare dichiara e garantisce di disporre di un'idonea base giuridica ai sensi degli Artt. 6 e 9 del GDPR per il trattamento dei dati personali contenuti nei Dati di Payload e di aver fornito agli Interessati le prescritte informative di legge.

4.2. Supervisione Umana ("Human-in-the-Loop") e Custodia Credenziali. In conformità agli Artt. 5.2, 6 e 12.1 dei ToS, il Titolare è l'unico responsabile della custodia delle credenziali dei propri utenti autorizzati e della verifica umana obbligatoria delle fonti e degli Output generati prima di qualsiasi utilizzo professionale o decisionale.

ARTICOLO 5 – CONFINAMENTO EUROPEO, TRASFERIMENTI E CONFORMITÀ "SCHREMS II"

5.1. Residenza ed Elaborazione nell'Unione Europea.

L'elaborazione dei Dati di Payload (server in Finlandia), l'archiviazione cifrata (Cloudflare R2 e Qdrant in regione UE), le copie di sicurezza cifrate (Backblaze B2 in regione UE) e il servizio di gestione delle chiavi (Google Cloud KMS in regione UE) sono interamente confinati all'interno dell'Unione Europea.

5.2. Clausole Contrattuali Standard (SCC) e Addendum UK/Svizzera. Nella misura in cui il rapporto contrattuale con il Responsabile (stabilito negli Stati Uniti) comporti un trasferimento di dati personali o metadati ai sensi del Capo V del GDPR, sono incorporate per riferimento nel presente DPA le **Clausole Contrattuali Standard (SCC)** approvate dalla Commissione Europea con Decisione di esecuzione (UE) 2021/914 (**Modulo 2: Controller-to-Processor** per i trattamenti svolti quale Responsabile;

Modulo 1: Controller-to-Controller per i metadati trattati quale Titolare), integrate dall'*International Data Transfer Addendum (IDTA)* per il Regno Unito e dalle clausole integrative dell'*IFPDT* per la Svizzera.

5.3. Misure Tecniche Supplementari (Conformità Schrems II e Raccomandazioni EDPB 01/2020). Ai fini della piena conformità alla sentenza della Corte di Giustizia UE C-311/18 (*Schrems II*) e alle Raccomandazioni EDPB 01/2020, le Parti danno atto che la cifratura sul dispositivo, il confinamento dei server di calcolo in **Finlandia (UE)**, la separazione delle chiavi e l'elaborazione esclusivamente all'interno delle enclavi hardware AMD e NVIDIA (*Data-in-use encryption*) costituiscono misure tecniche supplementari efficaci che impediscono materialmente a chiunque — inclusi il Responsabile e qualsiasi autorità governativa statunitense o di Paesi terzi — di accedere in chiaro ai Dati di Payload.

ARTICOLO 6 – SUB-RESPONSABILI (ART. 28.2 E 28.4 GDPR)

6.1. Elenco Autorizzato dei Sub-Responsabili. Il Titolare conferisce autorizzazione scritta all'impiego dei Sub-Responsabili indicati alla Sezione 6 della Privacy Policy, tutti vincolati al confinamento nell'Unione Europea per l'infrastruttura del Payload:

Verda (operato da DataCrunch Oy – Data Center in Finlandia, UE): Hosting fisico dei server *Confidential Computing* (CPU AMD SEV-SNP e GPU NVIDIA RTX PRO 6000 Blackwell / NVIDIA B200);

Google Ireland Limited (Regione UE): Infrastruttura applicativa e gestione chiavi crittografiche (**Google Cloud KMS** in regione UE) vincolata da *Key Release Policy*;

Cloudflare, Inc. (Regione UE): Sicurezza di rete WAF/DDoS e archivio oggetti cifrato (**Cloudflare R2** con *EU Jurisdiction*);

Backblaze, Inc. (Regione UE): Archiviazione delle copie di sicurezza cifrate (**Backblaze B2** in data center UE);

AWS EMEA SARL (Regione eu-central-1 Francoforte, Germania): Consegna e-mail transazionali di servizio (**AWS SES**).

6.2. Preavviso di Modifica e Diritto di Opposizione/Recesso (Art. 28.2 GDPR). Il Responsabile informerà per iscritto il Titolare di qualsiasi eventuale aggiunta o sostituzione dei Sub-Responsabili sopra elencati con un preavviso minimo di **quindici (15) giorni** (ovvero il maggior termine concordato nel Contratto Enterprise) prima dell'entrata in funzione. Durante tale periodo il Titolare potrà opporsi per iscritto per motivi legittimi legati alla protezione dei dati ovvero recedere dal contratto senza penalità ordinando la Cancellazione Crittografica immediata (T=0) prima che la modifica abbia effetto.

6.3. Obblighi e Responsabilità verso il Titolare (Art. 28.4 GDPR). Il Responsabile impone a ciascun Sub-Responsabile, mediante contratto scritto, obblighi di protezione dei dati non meno rigorosi di quelli stabiliti nel presente DPA e risponde nei confronti del Titolare dell'adempimento degli obblighi dei propri Sub-Responsabili ai sensi dell'Art. 28, par. 4 del GDPR.

ARTICOLO 7 – NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH – ART. 33.2 GDPR)

7.1. Tempistica e Contenuto della Notifica. In caso di violazione della sicurezza accertata che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati trattati per conto del Titolare, il Responsabile informerà il Titolare **senza ingiustificato ritardo e, in ogni caso, entro quarantotto (48) ore** (e comunque mai oltre il termine massimo di legge di cui all'Art. 4.5 della Privacy Policy) dal momento in cui ne è venuto a conoscenza, fornendo tutte le informazioni tecniche necessarie per consentire al Titolare di valutare l'evento ed effettuare le eventuali notifiche all'Autorità di controllo (Art. 33 GDPR) e agli Interessati (Art. 34 GDPR).

7.2. Protezione Crittografica e Hardware del Payload. Le Parti danno atto che, poiché i Dati di Payload risiedono in archivio esclusivamente in formato cifrato e vengono elaborati solo in enclavi hardware AMD/NVIDIA, un incidente perimetrale che non comprometta la chiave crittografica del Titolare né l'integrità dell'enclave hardware lascia i Dati di Payload inintelligibili ai sensi dell'Art. 34, par. 3, lett. a) del GDPR.

ARTICOLO 8 – VERIFICA TECNICA E DIRITTO DI AUDIT (ART. 28.3.H GDPR)

8.1. Verifica Crittografica Continua e Audit Documentale. In conformità all'Art. 28, par. 3, lett. h) del GDPR e alla procedura pubblicata nella sezione *Verifica Tecnica* del sito ufficiale, il Titolare e il suo reparto IT hanno il diritto di verificare la conformità del Responsabile in qualsiasi momento mediante:

(a) Attestazione Remota Hardware in tempo reale: verifica diretta dei report crittografici firmati dai processori **CPU AMD SEV-SNP** e **GPU NVIDIA RTX PRO 6000 / B200** tramite i verificatori ufficiali AMD e NVIDIA, nonché verifica delle misure del codice dell'enclave ("Codice sigillato") e delle policy di rilascio delle chiavi su Google Cloud KMS;

(b) Documentazione di Conformità e Certificazioni dei Data Center: esame della documentazione tecnica di sicurezza messa a disposizione dal Responsabile e dei report di certificazione indipendenti (es. ISO/IEC 27001, SOC 2 Type II) rilasciati ai Sub-Responsabili infrastrutturali e ai data center europei di cui all'Articolo 6.1;

(c) Richieste di Informazioni Scritte: invio di questionari di audit di sicurezza al Dipartimento Compliance del Responsabile (privacy@loricai.io), a cui il Responsabile darà riscontro documentato.

8.2. Sicurezza Fisica dei Data Center. Al fine di preservare l'integrità fisica delle infrastrutture multi-tenant e la sicurezza crittografica degli ambienti, le verifiche si svolgono tramite gli strumenti crittografici e documentali di cui all'Art. 8.1, restando escluso l'accesso fisico diretto dei clienti all'interno delle sale server dei data center.

ARTICOLO 9 – CLAUSOLA DI SIGILLO E RICHIESTE GOVERNATIVE (THE SEAL CLAUSE)

9.1. Impossibilità Tecnica di Esibizione in Chiaro. Il Titolare e il Responsabile danno atto che l'architettura di LoricAI impedisce matematicamente al Responsabile di decifrare i Dati di Payload al di fuori delle sessioni attivate dal Titolare nell'enclave hardware. Pertanto, il Responsabile non può tecnicamente ottemperare a richieste di terzi o di autorità governative volte all'estrazione dei contenuti in chiaro. In caso di ricezione di un ordine giudiziario relativo a metadati dell'account del Titolare, il Responsabile si impegna a verificarne la legittimità, a contestare qualsiasi richiesta extra-UE in conflitto con l'Art. 48 del GDPR e a informarne preventivamente il Titolare, salvo divieto penale inderogabile.

ARTICOLO 10 – RESPONSABILITÀ E RINVIO AI TERMINI DI SERVIZIO

10.1. Allineamento al Massimale Contrattuale (Art. 7 ToS). La responsabilità complessiva delle Parti derivante dal presente DPA è regolata dalle disposizioni e dai massimali stabiliti all'**Articolo 7 (Limitazione di Responsabilità e Manleva)** dei Termini di Servizio (ToS) (ovvero dal maggiore massimale specificamente pattuito per iscritto nel Contratto Enterprise sottoscritto con il Titolare):

(1) per i Clienti con contratto attivo, il massimale ordinario è pari all'importo totale dei corrispettivi effettivamente pagati dal Titolare nei dodici (12) mesi precedenti, **innalzato al doppio (2x)** dei corrispettivi pagati nei dodici (12) mesi precedenti in caso di *Data Breach* accertato e imputabile a inadempimento degli obblighi di sicurezza del Responsabile;

(2) per gli Utenti in fase di prova gratuita o con spesa inferiore a Euro 100,00 nei dodici (12) mesi precedenti, il massimale è pari a Euro 100,00 (o $ 100.00 USD). Resta in ogni caso impregiudicata l'applicazione delle norme inderogabili di legge, incluso l'Art. 82 del GDPR e le clausole inderogabili delle SCC.

10.2. Esclusione di Responsabilità sugli Output e Manleva del Titolare. In conformità agli Artt. 5.2, 7.2 e 7.3 dei ToS, poiché i modelli linguistici (es. *Qwen 3.6 Flash Next*) sono eseguiti in un'enclave cieca senza possibilità di revisione umana da parte del Responsabile, il Titolare mantiene l'esclusiva responsabilità sulla liceità dei Dati di Payload caricati e sulla validazione professionale degli Output generati, manlevando il Responsabile da pretese di terzi derivanti da violazioni degli obblighi facenti capo al Titolare ai sensi del GDPR o dell'EU AI Act.

ARTICOLO 11 – CESSAZIONE DEL CONTRATTO, RESTITUZIONE E CANCELLAZIONE CRITTOGRAFICA (ART. 28.3.G GDPR)

11.1. Esportazione e Restituzione dei Dati. In conformità all'Art. 28, par. 3, lett. g) del GDPR, all'Art. 7.4 della Privacy Policy e all'Art. 12.2 dei ToS, durante tutta la vigenza del contratto e fino all'esecuzione della Cancellazione Crittografica, il Titolare ha la piena facoltà tecnica di esportare e scaricare autonomamente in chiaro tutti i propri Dati di Payload e documenti tramite l'interfaccia protetta dalla propria chiave.

11.2. Cancellazione Crittografica (T=0 o T=30) e Rotazione Copie di Sicurezza. Alla cessazione del rapporto contrattuale o su istruzione del Titolare, il Responsabile esegue il protocollo di cancellazione stabilito alla Sezione 7 della Privacy Policy:

(a) Cancellazione Immediata (T=0): su richiesta esplicita del Titolare (nonché automaticamente al termine di una Prova Tecnica Preliminare non seguita da contratto), il Responsabile elimina immediatamente i documenti dall'archivio attivo (Cloudflare R2 e Qdrant) ed esegue la contestuale **distruzione irreversibile della chiave crittografica dedicata del Titolare (DEK/KEK) su Google Cloud KMS** (*Cryptographic Shredding*);

(b) Procedura Standard con Grace Period (T=0 -> T=30): salvo richiesta di distruzione immediata, alla chiusura ordinaria dell'account i token di accesso sono revocati a T=0, lasciando al Titolare trenta (30) giorni per completare l'esportazione dei propri archivi, decorsi i quali (T=30) il sistema esegue la distruzione definitiva della chiave crittografica su Google Cloud KMS;

(c) Copie di Sicurezza (Backblaze B2): dal momento esatto della distruzione della chiave (a T=0 o T=30), ogni blocco cifrato residuo nelle copie di sicurezza immutabili su Backblaze B2 diventa istantaneamente uno scarto entropico matematicamente indecifrabile e giunge a definitiva sovrascrittura fisica al termine del ciclo di rotazione di trentacinque (35) giorni.

ARTICOLO 12 – LEGGE APPLICABILE, FORO COMPETENTE E PUNTO DI CONTATTO UE

12.1.Legge Applicabile e Foro Competente.

Il presente DPA segue esattamente la segmentazione giurisdizionale stabilita dall'**Articolo 8 dei Termini di Servizio (ToS)** e dalla **Sezione 10 della Privacy Policy**:

per i Titolari stabiliti nell'**Unione Europea, nello Spazio Economico Europeo (SEE), nel Regno Unito e in Svizzera**, il presente DPA è regolato dalla legge della **Repubblica d'Irlanda** e qualsiasi controversia è devoluta alla **giurisdizione esclusiva delle Corti di Dublino (Repubblica d'Irlanda)**, fatti salvi i diritti inderogabili degli Interessati e i poteri delle Autorità di controllo di cui agli Artt. 77, 78 e 79 del GDPR;

per i Titolari stabiliti negli **Stati Uniti e in giurisdizioni Extra-Europee (esclusi SEE, UK e Svizzera)**, il presente DPA è regolato dalla legge dello Stato del **Wyoming (USA)** con arbitrato vincolante presso l'*American Arbitration Association (AAA)* in Casper, Wyoming.

12.2. Contatto Privacy e Rappresentante UE (Art. 27 GDPR). Per qualsiasi comunicazione inerente al presente DPA, all'esercizio dei diritti di audit o alla notifica di istruzioni sul trattamento, il punto di contatto ufficiale del Responsabile è: **DEXIMA TECH LLC — Data Protection & Legal Compliance Department, E-mail: privacy@loricai.io**.