INFORMATIVA GLOBALE SULLA PRIVACY E SULLA PROTEZIONE DEI DATI (GLOBAL PRIVACY & DATA PROTECTION POLICY)

Data di Entrata in Vigore: 01/2026 — **Ultimo Aggiornamento: 11/2026**
Ambito Territoriale: Globale (USA, UE, SEE, Regno Unito ai sensi dello UK GDPR e del Data Protection Act 2018, Svizzera ai sensi della Legge federale sulla protezione dei dati - nLPD, e Resto del Mondo).

PREAMBOLO E TITOLARITÀ

La presente Informativa Globale sulla Privacy ("Policy") disciplina il trattamento dei dati effettuato da **DEXIMA TECH LLC**, con sede legale in 5830 E 2nd St, Ste 7000 #32263, Casper, Wyoming 82609, USA ("Società" o "Noi"). Ai fini del Regolamento (UE) 2016/679 ("GDPR") e dello UK GDPR, i ruoli privacy sono così ripartiti:

Ruolo di Titolare del Trattamento (Data Controller): La Società agisce in qualità di Titolare autonomo esclusivamente per i Dati di Registrazione e Account (Sez. 4.1), i Dati Precontrattuali, Demo e Assistenza (Sez. 4.2), i Dati di Fatturazione (Sez. 4.3) e i Log di Sicurezza dell'Infrastruttura (Sez. 4.4).
Ruolo di Responsabile del Trattamento (Data Processor - Art. 28 GDPR): In relazione a tutti i documenti, file, testi e contenuti caricati dall'Utente negli spazi di lavoro ("Dati di Payload"), **il Cliente (azienda, studio o professionista) agisce quale unico Titolare del Trattamento**, mentre la Società agisce esclusivamente quale **Responsabile del Trattamento** in modalità *Zero-Knowledge / Blind Conduit*, in forza dell'Accordo sul Trattamento dei Dati (DPA ex Art. 28 GDPR) sottoscritto con il Cliente.

Contatto Legale, Privacy e Punto di Contatto UE (Art. 27 GDPR): privacy@loricai.io — Tutte le istanze degli Interessati e delle Autorità di controllo dell'Unione Europea sono gestite in via diretta e prioritaria dal Dipartimento Privacy & Compliance a tale recapito; gli estremi del Rappresentante designato nell'Unione Europea ai sensi dell'Art. 27 GDPR sono resi disponibili su richiesta e riportati nel DPA aziendale.

1. DEFINIZIONI CONTRATTUALI

Ai fini della presente Policy, i seguenti termini in maiuscolo avranno il significato qui attribuito:

1.1. "Architettura Zero-Knowledge e Isolamento Hardware": L'infrastruttura di LoricAI si fonda sulla segregazione matematica e fisica del dato. Grazie alla cifratura applicata sul dispositivo per il trasferimento e l'archivio e all'impiego di processori **AMD** e **NVIDIA** in modalità *Confidential Computing*, i Dati di Payload vengono decifrati esclusivamente all'interno di un'enclave hardware isolata e verificata. DEXIMA TECH LLC attesta l'impossibilità tecnica per i propri amministratori, operatori o soggetti terzi di accedere, leggere o intercettare i dati in chiaro: la memoria volatile (RAM/VRAM) dell'enclave è protetta da chiavi hardware effimere, mentre il servizio di gestione delle chiavi (**Google Cloud KMS** in regione UE) non riceve mai i documenti e rilascia le chiavi di decrittazione esclusivamente all'ambiente protetto dopo il superamento dei controlli crittografici di integrità (Attestazione Remota AMD e NVIDIA).

1.2. "Dati di Payload": Qualsiasi file, documento, pratica, input di testo (prompt), query, frammento audio, immagine o contenuto caricato o generato dall'Utente all'interno degli spazi di lavoro per l'elaborazione.

1.3. "Confidential Computing (TEE)": Ambienti di esecuzione fidata (*Trusted Execution Environments*) residenti su hardware specializzato (**CPU AMD con tecnologia SEV-SNP** e **GPU NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200**) che impediscono l'accesso alla memoria volatile (RAM/VRAM) anche al sistema operativo, all'hypervisor ospitante e al gestore del data center.

1.4. "Cancellazione Crittografica (Crypto-Shredding)": Il processo di revoca e distruzione permanente (*Key Destruction*) della chiave crittografica dedicata del Cliente (DEK/KEK), che rende matematicamente e permanentemente indecifrabili i dati cifrati presenti nell'archivio attivo, nei database vettoriali e nelle copie di sicurezza immutabili.

1.5. "Blind Index": L'indice di ricerca crittografico generato tramite funzione HMAC-SHA256, che consente la separazione logica degli ambienti e impedisce la correlazione diretta tra i record amministrativi del database e l'identità o le chiavi crittografiche del Tenant in caso di compromissione fisica dei sistemi.

---

2. SOVRANITÀ DEI DATI E CONFINI GIURISDIZIONALI (DATA RESIDENCY)

2.1. Confinamento Geografico (EU Data Residency) e Cifratura Persistente. A deroga della costituzione societaria nello Stato del Wyoming (USA), la Società stabilisce un perimetro rigoroso di residenza ed elaborazione dei dati nell'Unione Europea:

- i nodi di calcolo *Confidential Computing* (CPU AMD e GPU NVIDIA) risiedono fisicamente nell'**Unione Europea, in Finlandia**;i **Dati di Payload in formato nativo in chiaro (plaintext)** non vengono mai materializzati, allocati o scritti su supporti di archiviazione persistenti (Block Storage, SSD o Object Storage);
- i documenti caricati nelle pratiche, gli indici vettoriali (su database Qdrant) e le copie di sicurezza sono conservati **esclusivamente in formato cifrato** all'interno dell'Unione Europea (su archivio **Cloudflare R2** in regione UE e copie di sicurezza su **Backblaze B2** in regione UE), protetti da una chiave crittografica dedicata a ciascun Cliente gestita separatamente tramite **Google Cloud KMS** (regione UE).

2.2. Protezione contro Ordini Extraterritoriali (es. US CLOUD Act). I documenti cifrati e le chiavi di decrittazione rimangono strutturalmente separati. Poiché la policy crittografica di rilascio delle chiavi (*Key Release Policy*) autorizza la consegna della chiave esclusivamente all'interno dell'enclave hardware AMD/NVIDIA verificata tramite Attestazione Remota e mai agli amministratori di DEXIMA TECH LLC o al fornitore del servizio KMS, la Società si trova nell'impossibilità tecnica materiale di decifrare o esibire in chiaro i Dati di Payload a fronte di ordini giudiziari o governativi extraterritoriali (incluso lo US CLOUD Act). La Società si impegna in ogni caso a contestare formalmente qualsiasi richiesta governativa extra-UE in conflitto con l'Art. 48 del GDPR, informando tempestivamente il Cliente ove legalmente consentito.

2.3. DIRITTI DEI RESIDENTI IN CALIFORNIA (CCPA/CPRA).

Ai sensi delle leggi sulla privacy degli Stati Uniti, DEXIMA TECH LLC fornisce la presente 'Notice at Collection'.

- **Categorie di dati raccolti:** Identificativi e dati di contatto professionali (nome, cognome, e-mail, telefono, azienda, indirizzo IP temporaneo/hash per sicurezza), informazioni commerciali e di fatturazione (storico transazioni), e attività su rete internet (log tecnici di sicurezza e accesso), come dettagliato alla Sezione 4. La Società NON raccoglie, accede o "condivide" Informazioni Personali Sensibili (*Sensitive Personal Information - SPI*). I Dati di Payload caricati dall'Utente sono soggetti a crittografia hardware Zero-Knowledge; di conseguenza, la Società non possiede le chiavi di decrittazione e considera tali dati come frammenti crittografici opachi, non riconducibili a informazioni personali leggibili dalla Società medesima.
- **Finalità:** Fornitura del servizio e sicurezza informatica.

Diritti: La Società non 'vende' (Sell) né 'condivide' (Share) dati personali per pubblicità comportamentale. I residenti negli Stati Uniti possono esercitare i diritti di accesso, rettifica e cancellazione inviando una richiesta a privacy@loricai.io. Applichiamo i medesimi standard di protezione hardware (Root of Trust) a tutti i dati dei residenti USA.

3. MECCANICA DEL TRATTAMENTO E BLINDATURA DELL'INFERENZA AI

La Società agisce come *Blind Conduit* (condotto cieco) rispetto ai Dati di Payload. La responsabilità legale e tecnica è limitata dai seguenti parametri operativi:

3.1. Separazione tra Archivio Cifrato e Decrittazione nell'Enclave. La cifratura sul dispositivo protegge i documenti durante il trasferimento e la permanenza in archivio. I Dati di Payload e le relative rappresentazioni vettoriali cifrate (*embeddings* su Qdrant) risiedono su storage persistente nell'Unione Europea unicamente come testo cifrato opaco (*ciphertext*). Per elaborare una richiesta dell'Utente, i dati vengono decifrati **soltanto all'interno della memoria volatile isolata (RAM/VRAM) dell'enclave hardware autorizzata**, dove opera localmente il modello AI.

3.2. Volatilità della Sessione di Calcolo. All'interno dell'enclave hardware, i dati decifrati risiedono esclusivamente in memoria volatile protetta (`tmpfs` / VRAM cifrata) per il tempo strettamente necessario a completare l'inferenza e trasmettere la risposta cifrata allo spazio di lavoro dell'Utente tramite canale protetto, con distruzione immediata dei buffer temporanei di sessione al termine del calcolo (e comunque con *Time-To-Live* dei buffer inattivi post-inferenza non superiore a 60 secondi).

3.3. Azzeramento della Memoria (VRAM Scrubbing). Al termine di ciascuna richiesta di elaborazione all'interno dell'enclave, il sistema esegue forzatamente l'azzeramento crittografico dei buffer di memoria GPU *(cudaMemset(ptr, 0, size) e cudaDeviceReset()*) e la pulizia della memoria volatile allocata, garantendo l'assenza totale di residui forensi in chiaro dei Dati di Payload.

3.4. Isolamento del Modello AI e Divieto di Addestramento (NO AI TRAINING). L'elaborazione avviene tramite modelli linguistici (es. **Qwen 3.6 Flash Next**) eseguiti direttamente e interamente all'interno dell'enclave hardware isolata in Finlandia. I Dati di Payload non vengono mai trasmessi a servizi AI di terze parti esterne né vengono mai utilizzati per l'addestramento, il *fine-tuning* o il miglioramento di alcun modello di Intelligenza Artificiale. Ogni inferenza è eseguita in modalità *stateless* rispetto ai pesi del modello.

3.5. Natura Giuridica e Tecnica degli Archivi Cifrati e degli Embeddings. I documenti cifrati (archiviati su Cloudflare R2 in regione UE) e le relative Rappresentazioni Vettoriali Cifrate (*embeddings* archiviate su database vettoriale Qdrant eseguito in istanza isolata sull'infrastruttura europea della Società) costituiscono estensioni digitali del Payload dell'Utente. Essi rimangono sotto la piena ed esclusiva titolarità e sovranità legale del Cliente. La Società agisce esclusivamente come custode tecnico (*Bailee*) di tali blocchi cifrati, senza alcun diritto di accesso in chiaro, utilizzo per finalità proprie o pretesa di proprietà intellettuale.

4. CATEGORIE DI DATI RACCOLTI COME TITOLARE, FINALITÀ E BASI GIURIDICHE

In qualità di Titolare del Trattamento per la gestione del rapporto commerciale e la sicurezza del servizio, la Società raccoglie esclusivamente i seguenti dati personali (Art. 5.1.c GDPR):

4.1. Dati di Registrazione e Autenticazione (Account Data)

Elementi raccolti: Nome, cognome, indirizzo e-mail professionale, ruolo/organizzazione e credenziali di autenticazione.

Trattamento crittografico: Nessuna password è memorizzata in chiaro; viene applicato un hashing crittografico (Argon2id) con *salt* casuale secondo i parametri OWASP vigenti.

Base Giuridica: Esecuzione del contratto (Art. 6.1.b GDPR).

4.2. Dati Precontrattuali, Richieste Demo e Assistenza Clienti

Elementi raccolti: Nome e cognome, azienda o studio professionale, indirizzo e-mail di lavoro, recapito telefonico e informazioni sul caso d'uso fornite volontariamente dall'Utente tramite il modulo "Prenota la demo", via e-mail (contact@loricai.io, support@loricai.io) o tramite contatto telefonico su appuntamento. Si invita l'Utente a non inserire dati riservati o sensibili nel modulo di contatto pubblico.

Base Giuridica: Esecuzione di misure precontrattuali adottate su richiesta dell'interessato e assistenza contrattuale (Art. 6.1.b GDPR). Conservazione massima in caso di mancata contrattualizzazione: 12 mesi dall'ultimo contatto.

4.3. Dati Finanziari e di Fatturazione (Billing Data)

Elementi raccolti: Ragione sociale, dati fiscali (Partita IVA/Codice Fiscale), coordinate di fatturazione, token di transazione opachi, estremi di bonifico bancario, importi e storico contrattuale.

Trattamento: Per i pagamenti elettronici tramite carta (conformità PCI-DSS SAQ A), i dati delle carte sono gestiti esclusivamente da **Stripe Payments Europe Ltd.** e **PayPal (Europe) S.à r.l. et Cie, S.C.A.**; per i contratti aziendali saldati tramite bonifico bancario, i flussi sono gestiti tramite istituti bancari autorizzati. Tramite tecniche di separazione degli ambienti (*Blind Indexing*), i dati di fatturazione sono isolati dalle chiavi crittografiche del Tenant.

Base Giuridica: Esecuzione del contratto (Art. 6.1.b GDPR) e adempimento di obblighi di legge fiscali, contabili e AML/KYC (Art. 6.1.c GDPR).

Natura del conferimento (Art. 13.2.e GDPR): Il conferimento dei dati di cui alle Sezioni 4.1, 4.2 e 4.3 è necessario per la conclusione ed esecuzione del contratto o delle misure precontrattuali; il mancato conferimento comporta l'impossibilità di attivare l'account, erogare la demo o fornire il Servizio.

4.4. Dati Operativi, Log di Sicurezza e Controllo Accessi Chiavi (Audit & Security Logs)

Elementi raccolti: Hash dell'Indirizzo IP, timestamp, endpoint interrogato, ed eventi di controllo integrità/rilascio chiavi KMS.

Trattamento: Nel database applicativo gli Indirizzi IP sono conservati esclusivamente come hash SHA-256 con *salt* giornaliero rotante. Nei soli Log di Infrastruttura Perimetrale (es. Cloudflare WAF e GCP Cloud Logging), gli Indirizzi IP in chiaro (*raw*) vengono registrati temporaneamente per un periodo tassativo massimo di trenta (30) giorni al solo fine di mitigare attacchi DDoS, prevenire abusi e garantire la sicurezza delle reti, senza alcuna finalità di profilazione.

Base Giuridica: Legittimo interesse alla sicurezza delle reti e delle informazioni (Art. 6.1.f e Considerando 49 del GDPR).

4.5. Gestione delle Violazioni dei Dati (Data Breach). In caso di violazione della sicurezza che comprometta Dati Personali o Metadati trattati dalla Società quale Titolare, la Società provvederà alle notifiche di legge entro 72 ore (Artt. 33 e 34 GDPR). Qualora un incidente di sicurezza coinvolga l'infrastruttura relativa ai Dati di Payload, la Società informerà il Cliente Titolare senza ingiustificato ritardo ai sensi dell'Art. 33, par. 2 del GDPR e secondo le tempistiche stabilite nel DPA.

4.6. Periodo di Conservazione dei Dati (Data Retention)

(a) Log di Sicurezza e IP Perimetrali: Massimo 30 giorni per finalità di sicurezza informatica.

(b) Registri Crittografici di Tracciabilità e Audit (Non-Content Hashes): I soli registri tecnici pseudonimizzati privi di contenuto in chiaro (hash crittografici delle sessioni, log di attestazione hardware e tracciamento degli accessi alle chiavi) sono conservati per 5 (cinque) anni al fine di garantire la verificabilità tecnica del servizio, l'accountability normativa e l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (Art. 6.1.f e Art. 17.3.e GDPR).

(c) Dati di Account, Fatturazione e Record Contrattuali: I dati di autenticazione dell'account (Sez. 4.1) vengono eliminati entro 30 giorni dalla cessazione del contratto (contestualmente alla procedura di chiusura di cui alla Sez. 7.1), mentre i dati contabili, fiscali e contrattuali (Sez. 4.3) sono conservati per 10 anni dalla cessazione del rapporto in conformità agli obblighi fiscali e civilistici applicabili.

(d) Dati di Payload: Rimangono sotto il controllo esclusivo del Cliente Titolare e seguono le istruzioni di cancellazione di cui alla Sezione 7 e al DPA.

5. RINUNCE E DICHIARAZIONI DI NON TRATTAMENTO (NEGATIVE COVENANTS)

A garanzia di trasparenza e quale impegno contrattuale vincolante nei confronti dell'Utente e di terzi, la Società dichiara formalmente di NON raccogliere, elaborare o conservare le seguenti categorie:
5.1. Nessun Tracciamento Comportamentale: Assenza totale di telemetria comportamentale, profilazione psicologica, Google Analytics, Meta Pixel, o software di session-replay (es. Hotjar).
5.2. Nessun Addestramento Modelli (No Model Training): Nessun Dato di Payload, prompt o interazione dell'Utente viene utilizzato per il fine-tuning, il pre-training o il miglioramento dei modelli di Intelligenza Artificiale proprietari o di terze parti.

5.3. Esclusività dei Cookie Tecnici: La Società utilizza esclusivamente cookie tecnici essenziali (o token JWT) al solo fine di mantenere attiva la sessione autenticata dell'Utente nella Dashboard. Tali elementi non effettuano profilazione comportamentale cross-site. I token di autenticazione proprietari vengono distrutti al termine della sessione, mentre i cookie di sicurezza e prevenzione frodi gestiti dai Sub-Responsabili (es. Stripe, Cloudflare) mantengono la persistenza tecnica strettamente necessaria indicata nell'apposita Cookie Policy.

6. GESTIONE DEI SUB-RESPONSABILI (SUB-PROCESSORS - ART. 28 GDPR)

Ai sensi dell'Art. 28 del GDPR e in conformità al DPA, la Società si avvale dei seguenti Sub-Responsabili qualificati, vincolati da Data Processing Agreements (DPA) e, ove applicabile per soggetti con capogruppo extra-SEE, dalla certificazione EU-US Data Privacy Framework (DPF) (Art. 45 GDPR) e/o dalle Clausole Contrattuali Standard (SCC) della Commissione Europea (Art. 46 GDPR):

Verda (operato da DataCrunch Oy, Data Center in Finlandia, Unione Europea): Fornitura ed hosting dell'infrastruttura hardware dedicata Confidential Computing (server con CPU AMD SEV-SNP e GPU NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200) su territorio finlandese (UE).

Google Ireland Limited (Unione Europea): Servizi infrastrutturali applicativi e servizio di gestione delle chiavi crittografiche (Google Cloud KMS configurato in regione UE). Il servizio di gestione delle chiavi è separato dall'archivio dei documenti e opera sotto una Key Release Policy che subordina il rilascio delle chiavi alla verifica crittografica dell'attestazione hardware AMD e NVIDIA.

Cloudflare, Inc. (Infrastruttura Edge e Storage R2 in Unione Europea): Utilizzata per: (i) servizi di sicurezza perimetrale di rete (WAF, mitigazione DDoS ed edge routing) coperti da certificazione attiva nell'EU-US Data Privacy Framework; (ii) archiviazione oggetti cifrata (Cloudflare R2) con confinamento geografico rigoroso (EU Jurisdiction) nell'Unione Europea per i file cifrati del Cliente.

Backblaze, Inc. (Regione Unione Europea): Servizio di archiviazione per le copie di sicurezza cifrate (Backblaze B2) localizzato esclusivamente in data center situati nell'Unione Europea.

AWS EMEA SARL (Lussemburgo / Regione eu-central-1 Francoforte, Germania): Servizio di invio e-mail transazionali (AWS SES) interamente confinato nell'Unione Europea.

Stripe Payments Europe Ltd. (Irlanda) e PayPal (Europe) S.à r.l. et Cie (Lussemburgo): Utilizzati esclusivamente quali gestori autonomi/responsabili per i pagamenti elettronici dei soli Dati di Fatturazione (Sez. 4.3), senza alcun coinvolgimento nell'infrastruttura dei Dati di Payload.

In conformità al principio di Privacy by Design (Art. 25 GDPR), nessun Sub-Responsabile ha accesso ai Dati di Payload in chiaro: i fornitori di storage (Cloudflare R2 e Backblaze B2) ospitano esclusivamente blocchi cifrati sul dispositivo/nell'enclave, il fornitore KMS (Google Cloud KMS) non riceve mai i documenti, e il fornitore hardware (Verda) è tecnicamente escluso dall'accesso alla memoria RAM/VRAM dall'isolamento fisico del silicio AMD e NVIDIA.

Ai sensi dell'Art. 28, par. 2 del GDPR e secondo le modalità previste nel DPA, la Società informerà preventivamente il Cliente Titolare di qualsiasi eventuale aggiunta o sostituzione dei Sub-Responsabili sopra elencati, garantendo al Cliente il diritto di opporsi o di recedere dal contratto con cancellazione crittografica immediata (Sez. 7.1) prima che il nuovo Sub-Responsabile entri in funzione.

---

7. CICLO DI CANCELLAZIONE, COPIE DI SICUREZZA E DIRITTO ALL'OBLIO (ART. 17 GDPR E DPA)

Le richieste di cancellazione dei Dati di Payload e degli spazi di lavoro sono eseguite secondo il DPA e le istruzioni del Cliente Titolare, previo superamento delle verifiche di autenticazione per prevenire distruzioni accidentali o dolose (*Verifiable Request*). *Nota Bene:* ***L'Utente è l'esclusivo responsabile dell'esportazione dei propri dati prima di ordinare la distruzione delle chiavi crittografiche; una volta distrutta la chiave, il recupero dei dati è matematicamente impossibile.***

7.1. Cancellazione Immediata su Istruzione del Titolare (inclusa Fine Prova) o Quarantena Standard:

Cancellazione Immediata (T=0): Su richiesta esplicita del Cliente Titolare (nonché automaticamente al termine di una prova tecnica qualora il Cliente decida di non sottoscrivere il contratto), la Società procede all'eliminazione immediata dei documenti dall'archivio attivo (Cloudflare R2 / Qdrant) e alla contestuale distruzione irreversibile della chiave crittografica dedicata (DEK/KEK) su Google Cloud KMS (*Cryptographic Shredding*).

Procedura Standard con Grace Period (T=0 -> T=30): Salvo richiesta di distruzione immediata, alla chiusura ordinaria dell'account i token di accesso vengono revocati istantaneamente (T=0) e si applica un periodo di sicurezza di 30 giorni contro cancellazioni involontarie, al termine del quale (T=30) il sistema esegue la distruzione definitiva della chiave crittografica su Google Cloud KMS.

7.2. Effetto sulle Copie di Sicurezza (Backblaze B2) e Sovrascrittura Fisica: Dal momento esatto della distruzione della chiave crittografica del Cliente (a T=0 o T=30), qualsiasi copia cifrata residua presente nelle copie di sicurezza immutabili su Backblaze B2 diventa istantaneamente uno scarto entropico matematicamente indecifrabile. I cicli di rotazione delle copie di sicurezza giungono successivamente a naturale scadenza e sovrascrittura fisica secondo il piano di continuità operativa definito nel DPA.

7.3. Eccezione Fiscale (Fiscal Ledger): Restano esclusi dalla cancellazione i soli dati contabili, contrattuali e di transazione (Sez. 4.3), conservati per dieci (10) anni in ottemperanza al Wyoming Title 17 W.S. e alle normative fiscali e IVA europee.

7.4. Autonomia di Esportazione e Cancellazione in Ambiente Zero-Knowledge: Il diritto di accesso (Art. 15 GDPR), portabilità (Art. 20 GDPR) e cancellazione sui Dati di Payload è garantito nativamente all'interno dell'interfaccia del Software: il Cliente può in qualsiasi momento scaricare, esportare o eliminare le proprie pratiche e i propri documenti senza alcuna intermediazione della Società.

---

8. CONFORMITÀ EU AI ACT E STRUMENTO DI AUSILIO TECNICO

La Società fornisce il Servizio esclusivamente come strumento di ausilio tecnico ("Human-in-the-Loop").

In conformità all'AI Act e all'art. 22 del GDPR, l'Utente ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato. Si informa l'Utente che il Software opera su modelli probabilistici di elaborazione del linguaggio naturale. Tuttavia, agendo la Società come Blind Conduit (infrastruttura Zero-Knowledge) priva di accesso in chiaro ai dati di Payload, è tecnicamente impossibile per la Società medesima effettuare una "revisione umana" degli output generati. L'obbligo di supervisione umana, interpretazione e validazione dei risultati ricade integralmente ed esclusivamente sull'Utente finale o sul professionista incaricato dall'Utente, come stabilito nei Termini di Servizio (ToS). L'Utente riconosce la natura statistica dell'output; la logica di elaborazione si basa esclusivamente sui parametri semantici del Payload e sulle istruzioni dell'Utente, senza l'uso di filtri decisionali occulti.

8.1. Obbligo di Trasparenza (Art. 50 AI Act). Ai sensi dell'Art. 50 del Regolamento UE 2024/1689 (AI Act), si notifica formalmente che l'Utente interagisce con un sistema di intelligenza artificiale e che gli output sono generati da modelli probabilistici suscettibili di allucinazioni, errori logici o inesattezze, richiedendo sempre la verifica delle fonti citate da parte del professionista umano.

8.2. Classificazione AI Act (Regolamento UE 2024/1689). **Il Software LoricAI è fornito esclusivamente quale strumento di ausilio documentale, ricerca con prova della fonte e redazione di bozze sottoposte a revisione umana obbligatoria (*Human-in-the-Loop*)**, operando nell'ambito delle attività preparatorie e procedurali di cui all'Art. 6, paragrafo 3 del Regolamento UE 2024/1689 (AI Act). **LoricAI non costituisce un sistema di IA ad "Alto Rischio" ai sensi dell'Allegato III dell'AI Act in quanto non effettua decisioni autonome o vincolanti**. È fatto divieto assoluto all'Utente di utilizzare gli output del Servizio per adottare decisioni interamente automatizzate, prive di effettiva verifica e validazione umana, in ambiti classificati ad "Alto Rischio" dall'Allegato III dell'AI Act (quali selezione automatizzata del personale, determinazione autonoma del merito creditizio o dell'accesso a servizi essenziali, profilazione biometrica o riconoscimento delle emozioni).

---

9. TUTELA DEI MINORI

L'utilizzo dell'infrastruttura è tassativamente interdetto ai soggetti di età inferiore a diciotto (18) anni. La Società non è soggetta al COPPA (Children's Online Privacy Protection Act) in quanto il servizio è inteso esclusivamente per un pubblico adulto e professionale. La rilevazione di account intestati a minori comporterà la cessazione unilaterale e senza preavviso del servizio.

---

10. LEGGE APPLICABILE, FORO COMPETENTE E CLASS ACTION WAIVER

10.1. Legge Applicabile (Segmentazione).
La legge applicabile alla presente Policy segue la medesima segmentazione contrattuale stabilita dall'Articolo 8 dei Termini di Servizio (ToS). Nello specifico:
per gli Utenti Business e Professionali stabiliti negli USA e in giurisdizioni Extra-Europee (esclusi SEE, Regno Unito e Svizzera) si applica la legge dello Stato del Wyoming (USA);

per gli Utenti Business e Professionali stabiliti nell'Unione Europea, nello Spazio Economico Europeo (SEE), nel Regno Unito e in Svizzera si applica la legge della Repubblica d'Irlanda;

per i Consumatori restano salvi i diritti inderogabili previsti dalla legge del rispettivo foro di residenza.

10.2. Arbitrato e Foro Competente (Segmentazione Giurisdizionale).

a) Utenti Business e Professionali (USA e Giurisdizioni Extra-Europee, esclusi SEE, UK e Svizzera): Qualsiasi controversia derivante dalla presente Policy sarà risolta esclusivamente tramite arbitrato vincolante amministrato dall'*American Arbitration Association (AAA)* con sede in Casper, Wyoming, USA. Le parti rinunciano alla giurisdizione di qualsiasi altra corte.

(b) Utenti Business e Professionali (B2B - Unione Europea, SEE, UK e Svizzera): Fatti salvi i diritti inderogabili degli Interessati previsti dagli Artt. 77, 78 e 79 del GDPR, per i clienti aziendali e professionali stabiliti nell'Unione Europea, SEE, Regno Unito o Svizzera qualsiasi controversia contrattuale, commerciale o risarcitoria derivante dalla presente Policy sarà soggetta alla giurisdizione esclusiva delle Corti di Dublino (Repubblica d'Irlanda). Le Parti derogano esplicitamente all'arbitrato AAA del Wyoming per questa specifica categoria.

(c) Consumatori (B2C - Unione Europea): Qualora l'Utente agisca in qualità di consumatore, la presente clausola non pregiudica i diritti inderogabili previsti dalle normative UE (incluso il Regolamento UE 1215/2012). Il consumatore potrà adire il tribunale del proprio luogo di residenza, dando atto delle oggettive caratteristiche tecniche di impossibilità di accesso in chiaro derivanti dall'Architettura Zero-Knowledge.

Fatto salvo quanto sopra, le controversie soggette alla giurisdizione statunitense e all'American Arbitration Association (AAA) ai sensi del precedente punto (a), saranno altresì strettamente vincolate al Protocollo per i Reclami di Massa (Mass Arbitration) definito nei Termini di Servizio (ToS).

10.3. Rinuncia a Class Action (Class Action Waiver). *Nella misura massima consentita dalle leggi applicabili, e fatti salvi i diritti inderogabili dei consumatori residenti nell'Unione Europea o in altre giurisdizioni che vietano tale rinuncia, l'Utente accetta* espressamente di intentare azioni legali nei confronti della Società esclusivamente a titolo individuale. È fatto divieto esplicito all'Utente di operare come attore o membro di una classe in un'azione collettiva, rappresentativa o consolidata (*Class Action* o *Representative Proceeding*). L'arbitro non può consolidare le rivendicazioni di più di una persona.

---

11. ESERCIZIO DEI DIRITTI (GDPR & CCPA) E TRASFERIMENTI INTERNAZIONALI

Fermi restando i limiti di impossibilità tecnica delineati alle Sezioni 2 e 3 (la Società non può accedere in chiaro ai Dati di Payload), l'Utente può esercitare in qualsiasi momento i diritti di Accesso, Rettifica, Cancellazione, Limitazione, Portabilità e Opposizione (Artt. 15–22 GDPR), nonché il diritto di proporre reclamo a un'Autorità di controllo (Art. 77 GDPR).

Per gli Utenti residenti nello Spazio Economico Europeo (SEE), Regno Unito e Svizzera, qualsiasi eventuale trasferimento di Dati Personali (limitato ai soli Metadati di account, contatto e sicurezza) verso la Società negli Stati Uniti è disciplinato dalle **Clausole Contrattuali Standard (SCC)** approvate dalla Commissione Europea (Decisione di esecuzione UE 2021/914), integrate dall'*International Data Transfer Addendum (IDTA)* per il Regno Unito e dalle clausole integrative dell'*IFPDT* per la Svizzera, mentre i trattamenti affidati a Sub-Responsabili con capogruppo statunitense sono coperti dalla rispettiva certificazione attiva nell'**EU-US / UK-US / Swiss-US Data Privacy Framework (DPF)** (Art. 45 GDPR) e/o dalle SCC vigenti. L'Utente può richiedere informazioni o copia delle garanzie di trasferimento adottate scrivendo a privacy@loricai.io (Art. 13.1.f GDPR).

Ogni richiesta di esercizio dei diritti o comunicazione formale può essere inviata via posta elettronica ordinaria o certificata (senza vincoli di forma) a: **DEXIMA TECH LLC — Data Protection & Legal Compliance Department E-mail: privacy@loricai.io**

La Società fornirà riscontro alle istanze legittime senza ingiustificato ritardo e, in ogni caso, entro trenta (30) giorni dal ricevimento della richiesta ai sensi dell'Art. 12, par. 3 del GDPR (ovvero entro quarantacinque (45) giorni per le istanze soggette al CCPA statunitense), prorogabili nei casi di particolare complessità previsti dalla legge.

12. CLAUSOLA DI SALVAGUARDIA (SEVERABILITY). Qualora una qualsiasi disposizione della presente Policy sia ritenuta invalida, illegale o inapplicabile da un tribunale della giurisdizione competente, le restanti disposizioni rimarranno pienamente valide ed efficaci e la disposizione invalida sarà modificata nella misura minima necessaria per renderla valida ed esecutiva, riflettendo il più fedelmente possibile l'intento originale.

13. TRASPARENZA SULLE RICHIESTE GOVERNATIVE E GARANZIA HARDWARE La Società si impegna a non divulgare Dati Personali o Metadati degli Utenti ad autorità governative, salvo in presenza di un ordine giudiziario valido, vincolante ed esecutivo. In relazione ai Dati di Payload, grazie al *Confidential Computing*, i documenti vengono decifrati solo temporaneamente all'interno della memoria volatile isolata (RAM/VRAM protetta) dell'enclave hardware per il tempo necessario all'elaborazione, venendo immediatamente sovrascritti al termine della sessione (*Memory Scrubbing*). Poiché la sicurezza è imposta da barriere fisiche nel silicio (*Hardware Root of Trust*) e da protocolli di Attestazione Remota (*Remote Attestation*) verificati prima del rilascio della chiave, nessun ordine giudiziario o intervento umano può forzare l'estrazione di contenuti in chiaro che la Società stessa è matematicamente impossibilitata a visualizzare o intercettare.

14. MODIFICHE E AGGIORNAMENTI ALLA POLICY

La Società si riserva il diritto di aggiornare la presente Policy per adeguarla a evoluzioni normative o miglioramenti infrastrutturali che non riducano il livello di tutela crittografica e hardware garantito. Eventuali modifiche sostanziali saranno comunicate agli Utenti registrati con un preavviso minimo di quindici (15) giorni tramite e-mail o notifica nella Dashboard, pubblicando la versione aggiornata con la relativa data di entrata in vigore.