REGOLE DI USO ACCETTABILE (ACCEPTABLE USE POLICY – AUP) Società Erogatrice: DEXIMA TECH LLC, 5830 E 2nd St, Ste 7000 #32263, Casper, Wyoming 82609, USA

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

Contatti Ufficiali: contact@loricai.io | support@loricai.io | privacy@loricai.io

La presente Policy di Uso Accettabile ("AUP" o "Uso Accettabile") costituisce parte integrante e sostanziale dei **Termini di Servizio ("ToS" — Articoli 6, 15 e 17.3)**, dell'**Informativa Globale sulla Privacy ("Privacy Policy")** e dell'**Accordo sul Trattamento dei Dati ("DPA ex Art. 28 GDPR")** di **DEXIMA TECH LLC** ("Società"). L'accesso e l'utilizzo della piattaforma e dell'infrastruttura **LoricAI** comportano l'obbligo di rispettare integralmente le presenti regole.

ARTICOLO 1 – IL PRINCIPIO DEL "BLIND CONDUIT" E LA RESPONSABILITÀ ESCLUSIVA DEL CLIENTE

1.1. Assenza di Monitoraggio dei Contenuti in Chiaro. Il Cliente e i suoi utenti autorizzati ("Utente") danno atto che LoricAI opera in regime di isolamento hardware *Confidential Computing* e architettura *Zero-Knowledge*. La Società non effettua, né ha la capacità tecnica o matematica di effettuare, alcuna lettura, ispezione, filtraggio semantico o moderazione proattiva in chiaro dei documenti caricati ("Dati di Payload"), delle domande formulate o degli Output generati all'interno delle enclavi hardware (**CPU AMD con tecnologia SEV-SNP** e **GPU NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200**) situate in **Finlandia (Unione Europea)**.

1.2. Responsabilità Esclusiva dell'Utente. L'impossibilità tecnica della Società di accedere ai contenuti in chiaro non conferisce in alcun modo all'Utente una licenza di utilizzo illecito. Il Cliente (in qualità di Titolare del Trattamento ex Art. 28 GDPR e Licenziatario del Servizio) è il solo ed esclusivo responsabile, sotto il profilo civile, amministrativo, deontologico e penale, della liceità dei Dati di Payload caricati, delle istruzioni impartite al modello e dell'utilizzo degli Output generati.

1.3. Rilevazione Reattiva basata su Anomalie Tecniche e Segnalazioni Legittime. Poiché il contenuto del Payload è inaccessibile in chiaro, la Società applica la presente AUP attraverso: (a) il rilevamento automatizzato di pattern di traffico anomali o attacchi a livello di rete perimetrale (**Cloudflare WAF**) e di telemetria hardware non-content; (b) la verifica di violazioni delle policy crittografiche di attestazione su **Google Cloud KMS**; (c) segnalazioni circostanziate di abusi da parte di terzi o ordini giudiziari validi, vincolanti ed esecutivi emessi da autorità competenti in conformità alla Sezione 13 della Privacy Policy e all'Articolo 9.1 del DPA.

ARTICOLO 2 – CONFORMITÀ AL REGOLAMENTO UE 2024/1689 (EU AI ACT) E DIVIETI SULL'USO DELL'IA

In conformità all'Articolo 6 dei ToS e all'Articolo 8.2 della Privacy Policy, 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'**Articolo 6, paragrafo 3 del Regolamento (UE) 2024/1689 (AI Act)**. È fatto divieto assoluto e inderogabile all'Utente di impiegare LoricAI per:

2.1. Pratiche di Intelligenza Artificiale Vietate (Articolo 5 EU AI Act):

- **(a) Manipolazione Subliminale o Ingannevole:** implementazione di tecniche subliminali, manipolative o ingannevoli volte a distorcere materialmente il comportamento di una persona o di un gruppo di persone causando un danno significativo fisico, psicologico o finanziario;
- **(b) Sfruttamento delle Vulnerabilità:** sfruttamento delle vulnerabilità di persone fisiche dovute all'età, alla disabilità o a una specifica situazione sociale o economica;
- **(c) Punteggio Sociale (Social Scoring):** valutazione o classificazione dell'affidabilità di persone fisiche basata sul loro comportamento sociale o su caratteristiche personali note, inferite o previste, che determini un trattamento pregiudizievole o sfavorevole in contesti non correlati o sproporzionati;

- **(d) Polizia e Giustizia Predittiva basata sulla Profilazione:** valutazione o previsione del rischio che una persona fisica commetta un reato basata esclusivamente sulla profilazione della persona o sulla valutazione dei tratti e delle caratteristiche della personalità;
- **(e) Raccolta Non Mirata di Immagini Facciali:** creazione o espansione di database di riconoscimento facciale mediante lo *scraping* non mirato di immagini facciali da internet o da filmati di videosorveglianza (CCTV);
- **(f) Riconoscimento delle Emozioni Vietato:** inferenza delle emozioni di una persona fisica nei luoghi di lavoro e nelle istituzioni di istruzione e formazione;
- **(g) Categorizzazione Biometrica Sensibile e Identificazione Biometrica Remota:** sistemi di categorizzazione biometrica che deducono la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale, nonché sistemi di identificazione biometrica remota non autorizzati dalla legge.

2.2. Divieto di Decisioni Interamente Automatizzate in Ambiti ad "Alto Rischio" (Allegato III EU AI Act e Art. 22 GDPR): Fermo restando l'uso legittimo di LoricAI da parte di professionisti e aziende come strumento preparatorio di analisi documentale e redazione di bozze sottoposte a verifica e decisione umana finale (*Human-in-the-Loop*), è fatto divieto assoluto di utilizzare gli Output del Servizio per adottare **decisioni interamente automatizzate, prive di effettiva verifica, controllo e validazione umana decisoria**, in ambiti classificati ad "Alto Rischio" dall'Allegato III dell'AI Act (quali, a titolo esemplificativo: selezione e valutazione automatizzata dei candidati o dei lavoratori, determinazione autonoma del merito creditizio o della tariffazione/liquidazione assicurativa su persone fisiche, valutazione autonoma dell'ammissibilità a prestazioni e servizi pubblici essenziali, o adozione di provvedimenti giudiziari non supervisionati).

ARTICOLO 3 – ILLICEITÀ DEI CONTENUTI, REATI INTERNAZIONALI E SEGRETO PROFESSIONALE (ZERO TOLERANCE)

L'infrastruttura LoricAI non può in alcun caso essere utilizzata per attività che costituiscano reato o illecito civile/amministrativo ai sensi del diritto dell'Unione Europea, delle leggi degli Stati membri, del diritto federale e statale degli Stati Uniti o del diritto internazionale. È severamente vietato caricare, elaborare, generare o archiviare contenuti relativi a:

3.1. Materiale di Abuso e Sfruttamento Sessuale di Minori (CSAM / CSEM): qualsiasi contenuto pedopornografico o di sfruttamento minorile. Pur non potendo la Società visualizzare i Dati di Payload in chiaro, in presenza di segnalazioni qualificate o ordini delle autorità competenti la Società collaborerà senza riserve con il *NCMEC (National Center for Missing & Exploited Children)* e con le autorità giudiziarie e di polizia nazionali ed europee, fornendo i metadati tecnici e amministrativi effettivamente disponibili secondo i periodi di conservazione e i protocolli di separazione degli ambienti (*Blind Indexing*) stabiliti nelle Sezioni 4 e 13 della Privacy Policy.

3.2. Terrorismo, Minacce CBRN e Violenza Grave: progettazione, assistenza tecnica o istruzioni operative per la fabbricazione o l'impiego di armi biologiche, chimiche, radiologiche o nucleari (CBRN), esplosivi, atti di terrorismo, incitamento all'odio o alla violenza, autolesionismo o traffico di esseri umani.

3.3. Attacchi Informatici, Malware e Cyber-Crime: sviluppo, perfezionamento o distribuzione di codice malevolo (*malware*, *ransomware*, *spyware*, *trojan*), sfruttamento illecito di vulnerabilità (*zero-day exploits*), campagne di *phishing* o *spear-phishing*, compromissione non autorizzata di sistemi informatici di terzi o violazione di misure di sicurezza tecnologiche.

3.4. Frodi, Disinformazione Elettorale e Manipolazione dei Mercati: generazione di *deepfake* o contenuti sintetici finalizzati a truffe, frodi finanziarie o assicurative, furto d'identità, riciclaggio di denaro, manipolazione abusiva dei mercati finanziari o campagne coordinate di disinformazione fraudolenta in processi elettorali o istituzionali.

3.5. Violazione di Dati Personali, Segreti Industriali e Proprietà Intellettuale di Terzi: caricamento negli spazi di lavoro di documenti, banche dati o informazioni confidenziali sottratti illecitamente a terzi, acquisiti in

violazione del GDPR, del segreto professionale, industriale o d'ufficio, ovvero in violazione del diritto d'autore e dei diritti di proprietà intellettuale altrui (Art. 7.3 ToS e Art. 4.1 DPA).

3.6. Violazione di Sanzioni Internazionali ed Export Control: utilizzo del Servizio da parte di soggetti sanzionati o da/verso Paesi sottoposti a embargo in violazione dell'Articolo 14 dei ToS (*EAR / OFAC / Regolamenti Sanzionatori UE*).

ARTICOLO 4 – PROTEZIONE DELL'INTEGRITÀ DELL'INFRASTRUTTURA HARDWARE E CRITTOGRAFICA L'Utente si impegna a non minacciare né compromettere in alcun modo l'integrità fisica, logica e crittografica dell'Infrastruttura LoricAI. Costituisce gravissimo inadempimento contrattuale e violazione immediata della presente AUP (Art. 6 ToS):

4.1. Tentativi di Evasione o Bypass dell'Enclave Hardware (TEE): qualsiasi attacco di tipo *side-channel*, *fault injection*, manipolazione dei pacchetti di Attestazione Remota AMD/NVIDIA, tentativo di esfiltrazione o intercettazione delle chiavi crittografiche (**DEK/KEK** gestite tramite **Google Cloud KMS** in regione UE) o tentativo di violare l'isolamento della memoria delle **CPU AMD SEV-SNP** e delle **GPU NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200**.

4.2. Model Extraction, Reverse Engineering e Scraping Computazionale: qualsiasi tentativo di decompilare i componenti proprietari della piattaforma, estrarre o clonare i pesi dei modelli linguistici residenti nell'enclave (es. *Qwen 3.6 Flash Next*) tramite attacchi di *model inversion*, *distillation* non autorizzata o interrogazione massiva automatizzata (*scraping* tramite script o bot).

4.3. Attacchi Volumetrici, Replay Attacks e Saturazione delle Risorse (OOM / Denial of Wallet): l'invio deliberato di payload malformati, l'alterazione dei *timestamp* crittografici (*Replay Attacks*), l'esecuzione di attacchi *Denial of Service (DDoS)* o qualsiasi azione volta a saturare dolosamente la memoria VRAM delle GPU (*Out-of-Memory attacks*) o la banda di rete a danno dell'infrastruttura e degli altri Clienti.

ARTICOLO 5 – MISURE DI SOSPENSIONE ("KILL-SWITCH"), RISOLUZIONE E GESTIONE DEGLI ARCHIVI

5.1. Accertamento Tecnico delle Violazioni. DEXIMA TECH LLC valuta le violazioni della presente AUP sulla base di evidenze tecniche oggettive (quali alert di sicurezza di **Cloudflare WAF**, anomalie nei controlli di integrità delle sessioni, tentativi di forzatura delle policy KMS o attacchi all'infrastruttura), nonché sulla base di provvedimenti vincolanti delle autorità competenti.

5.2. Sospensione Cautelare Immediata ("Kill-Switch Computazionale"). In presenza di un attacco informatico attivo, di un tentativo di compromissione dell'enclave hardware o di una grave violazione degli Articoli 2, 3 o 4, la Società ha il diritto di attivare immediatamente il protocollo di protezione tecnica (*Kill-Switch*), che comporta la **sospensione istantanea dei token di sessione, delle credenziali API e dei cicli di elaborazione AI**. Qualora per un Cliente Enterprise l'anomalia riguardi unicamente la singola credenziale compromessa di un utente autorizzato senza coinvolgere l'intero Tenant, la Società potrà limitare la sospensione cautelare all'utenza interessata dandone immediato avviso al referente IT del Cliente.

5.3. Risoluzione di Diritto e Tutela del Diritto di Esportazione Dati (Art. 15.2 ToS e Art. 28.3.g GDPR). Qualora la violazione sia confermata e costituisca causa di risoluzione immediata del contratto ai sensi dell'Articolo 15.1 dei ToS:

- **(a) Corrispettivi:** il contratto si intenderà risolto di diritto per fatto e colpa del Cliente (Art. 1456 c.c.), senza alcun diritto del Cliente al rimborso dei canoni o delle unità del periodo in corso, ferma restando la facoltà della Società di agire per il risarcimento dell'eventuale maggior danno subito;
- **(b) Esportazione e Cancellazione Crittografica:** in piena coerenza con l'Articolo 15.2 dei ToS, la Sezione 7 della Privacy Policy e l'Articolo 11 del DPA, anche in caso di risoluzione del contratto la Società consente al Cliente Titolare l'esportazione dei propri archivi cifrati prima di procedere alla **Cancellazione Crittografica definitiva (T=0 / T=30)** della chiave su Google Cloud KMS (e conseguente inintelligibilità su Cloudflare R2, Qdrant e Backblaze B2), **salvo il caso in cui la conservazione, la messa a disposizione o l'esportazione siano espressamente vietate da un ordine legittimo**

dell'autorità giudiziaria ovvero il Payload stesso costituisca uno strumento attivo di attacco informatico (*malware / exploit*) contro l'infrastruttura. Per i Consumatori UE restano salve le garanzie di cui all'Articolo 15.2 dei ToS.

ARTICOLO 6 – MANLEVA E INDENNITÀ PER SANZIONI E PROCEDIMENTI

In conformità e in piena applicazione dell'**Articolo7.3 dei Termini di Servizio (*Manleva e Indennità – Indemnification*)** e dell'**Articolo 10.2 del DPA**, qualora la violazione della presente AUP da parte del Cliente o dei suoi utenti autorizzati determini contestazioni di terzi, ispezioni, procedimenti giudiziari o sanzioni amministrative/pecuniarie (incluse sanzioni delle Autorità Garanti per la protezione dei dati personali, delle autorità di vigilanza sull'IA ex Regolamento UE 2024/1689 o di autorità governative statunitensi ed europee) nei confronti di **DEXIMA TECH LLC** o dei suoi Sub-Responsabili, il Cliente si obbliga a manlevare e tenere integralmente indenne la Società da ogni sanzione, danno, costo di bonifica tecnica, onere di perizia forense e spesa legale sostenuta per la propria difesa.

ARTICOLO 7 – SEGNALAZIONE DI ABUSI, LEGGE APPLICABILE E FORO COMPETENTE

7.1. Segnalazione di Violazioni. Qualsiasi segnalazione relativa a presunte violazioni della presente AUP o alla sicurezza dell'infrastruttura può essere inviata a: **privacy@loricai.io** o **support@loricai.io**.

7.2. Legge Applicabile e Giurisdizione. La presente AUP è regolata dalla medesima legge applicabile ed è soggetta alla medesima giurisdizione esclusiva stabilite dall'**Articolo 8 dei Termini di Servizio (ToS)** e dalla **Sezione 10 della Privacy Policy** (Legge della Repubblica d'Irlanda e giurisdizione esclusiva delle Corti di Dublino per i Clienti Business e Professionali stabiliti in Unione Europea, SEE, Regno Unito e Svizzera; Legge dello Stato del Wyoming e arbitrato vincolante AAA in Casper, Wyoming per i Clienti Business stabiliti negli USA e nel resto del mondo extra-europeo; foro inderogabile di residenza per i Consumatori UE).