Acceptable use

Service terms and information. The customer’s executed agreement, order, and schedules govern.

ACCEPTABLE USE POLICY (AUP)
Service Provider: DEXIMA TECH LLC, 5830 E 2nd St, Ste 7000 #32263, Casper, Wyoming 82609, USA Effective Date: 01/2026 - Last Updated: 11/2026
Official Contacts: contact@loricai.io | support@loricai.io | privacy@loricai.io

This Acceptable Use Policy ("AUP" or "Acceptable Use") constitutes an integral and substantial part of the Terms of Service ("ToS" - Articles 6, 15, and 17.3), the Global Privacy & Data Protection Policy ("Privacy Policy"), and the Data Processing Agreement ("DPA pursuant to Art. 28 GDPR") of DEXIMA TECH LLC ("Company"). Access to and use of the LoricAI platform and infrastructure entail the obligation to fully comply with these rules.

ARTICLE 1 - THE "BLIND CONDUIT" PRINCIPLE AND EXCLUSIVE CUSTOMER RESPONSIBILITY

1.1. Absence of Plaintext Content Monitoring. The Customer and its authorized users ("User") acknowledge that LoricAI operates under a Confidential Computing hardware isolation regime and Zero-Knowledge architecture. The Company does not perform, nor does it have the technical or mathematical ability to perform, any reading, inspection, semantic filtering, or proactive moderation in plaintext of uploaded documents ("Payload Data"), submitted queries, or Outputs generated inside the hardware enclaves (AMD CPUs with SEV-SNP technology and NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200 GPUs) located in Finland (European Union).

1.2. Exclusive User Responsibility. The technical impossibility for the Company to access content in plaintext does not in any way grant the User a license for unlawful use. The Customer (in its capacity as Data Controller pursuant to Art. 28 GDPR and Licensee of the Service) is solely and exclusively responsible and liable, under civil, administrative, professional ethics, and criminal law, for the lawfulness of uploaded Payload Data, the instructions given to the model, and the use of generated Outputs.

1.3. Reactive Detection Based on Technical Anomalies and Legitimate Reports. Because Payload content is inaccessible in plaintext, the Company enforces this AUP through: (a) automated detection of anomalous traffic patterns or attacks at the perimeter network level (Cloudflare WAF) and non-content hardware telemetry; (b) verification of breaches of cryptographic attestation policies on Google Cloud KMS; (c) substantiated abuse reports from third parties or valid, binding, and enforceable judicial orders issued by competent authorities in accordance with Section 13 of the Privacy Policy and Article 9.1 of the DPA.

ARTICLE 2 - COMPLIANCE WITH REGULATION (EU) 2024/1689 (EU AI ACT) AND PROHIBITIONS ON AI USE
In accordance with Article 6 of the ToS and Article 8.2 of the Privacy Policy, the LoricAI Software is provided exclusively as a tool for documentary support, source-verified search, and drafting subject to mandatory human review (Human-in-the-Loop), operating within the scope of preparatory and procedural tasks under Article 6(3) of Regulation (EU) 2024/1689 (AI Act). The User is strictly and non-derogably prohibited from using LoricAI for:

2.1. Prohibited Artificial Intelligence Practices (Article 5 EU AI Act):
(a) Subliminal or Deceptive Manipulation: implementing subliminal, manipulative, or deceptive techniques aimed at materially distorting the behavior of a person or a group of persons in a manner that causes or is reasonably likely to cause significant physical, psychological, or financial harm;

(b) Exploitation of Vulnerabilities: exploiting the vulnerabilities of natural persons due to their age, disability, or a specific social or economic situation;
(c) Social Scoring: evaluating or classifying the trustworthiness of natural persons based on their social behavior or known, inferred, or predicted personal or personality characteristics, leading to detrimental or unfavorable treatment in unrelated or disproportionate contexts;
(d) Profile-Based Predictive Policing and Justice: assessing or predicting the risk of a natural person committing a criminal offense based solely on the profiling of a natural person or on assessing their personality traits and characteristics;
(e) Untargeted Scraping of Facial Images: creating or expanding facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
(f) Prohibited Emotion Recognition: inferring the emotions of a natural person in the areas of workplace and education institutions;
(g) Sensitive Biometric Categorization and Remote Biometric Identification: biometric categorization systems that deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation, as well as unauthorized remote biometric identification systems.

2.2. Prohibition of Fully Automated Decisions in "High-Risk" Areas (Annex III EU AI Act and Art. 22 GDPR): Without prejudice to the legitimate use of LoricAI by professionals and enterprises as a preparatory tool for document analysis and drafting subject to final human verification and decision-making (Human-in-the-Loop), the User is strictly prohibited from using the Outputs of the Service to take fully automated decisions, devoid of effective human verification, control, and decision-making validation, in areas classified as "High-Risk" by Annex III of the AI Act (such as, by way of example: automated recruitment screening and evaluation of candidates or workers, autonomous determination of creditworthiness or insurance pricing/claims settlement concerning natural persons, autonomous assessment of eligibility for essential public assistance benefits and services, or adoption of unsupervised judicial decisions).

ARTICLE 3 - UNLAWFUL CONTENT, INTERNATIONAL CRIMES, AND PROFESSIONAL SECRECY (ZERO TOLERANCE)
The LoricAI infrastructure may under no circumstances be used for activities that constitute a criminal offense or a civil/administrative wrong under European Union law, the laws of EU Member States, United States federal and state law, or international law. It is strictly prohibited to upload, process, generate, or store content relating to:

3.1. Child Sexual Abuse and Exploitation Material (CSAM / CSEM): any child pornography or child sexual exploitation material. Although the Company cannot view Payload Data in plaintext, in the presence of qualified reports or orders from competent authorities, the Company shall cooperate without reservation with the NCMEC (National Center for Missing & Exploited Children) and national and European judicial and law enforcement authorities, providing the technical and administrative metadata actually available in accordance with the retention periods and environment separation protocols (Blind Indexing) established in Sections 4 and 13 of the Privacy Policy.

3.2. Terrorism, CBRN Threats, and Severe Violence: design, technical assistance, or operational instructions for the manufacture or use of chemical, biological, radiological, or nuclear (CBRN) weapons, explosives, acts of terrorism, incitement to hatred or violence, self-harm, or human trafficking.

3.3. Cyberattacks, Malware, and Cyber-Crime: development, refinement, or distribution of malicious code (malware, ransomware, spyware, trojans), unlawful exploitation of vulnerabilities (zero-day exploits), phishing or spear-phishing campaigns, unauthorized compromise of third-

party IT systems, or circumvention of technological security measures.

3.4. Fraud, Electoral Disinformation, and Market Manipulation: generation of deepfakes or synthetic content aimed at scams, financial or insurance fraud, identity theft, money laundering, abusive manipulation of financial markets, or coordinated fraudulent disinformation campaigns in electoral or institutional processes.

3.5. Infringement of Third-Party Personal Data, Trade Secrets, and Intellectual Property: uploading into workspaces documents, databases, or confidential information unlawfully misappropriated from third parties, acquired in violation of the GDPR, professional, industrial, or official secrecy, or in infringement of third-party copyright and intellectual property rights (Art. 7.3 ToS and Art. 4.1 DPA).

3.6. Violation of International Sanctions and Export Control: use of the Service by sanctioned persons or from/toward embargoed countries in violation of Article 14 of the ToS (EAR / OFAC / EU Sanctions Regulations).

ARTICLE 4 - PROTECTION OF HARDWARE AND CRYPTOGRAPHIC INFRASTRUCTURE INTEGRITY
The User undertakes not to threaten or compromise in any way the physical, logical, and cryptographic integrity of the LoricAI Infrastructure. Any of the following constitutes a material breach of contract and an immediate violation of this AUP (Art. 6 ToS):

4.1. Attempts to Evade or Bypass the Hardware Enclave (TEE): any side-channel attack, fault injection, manipulation of AMD/NVIDIA Remote Attestation packets, attempt to exfiltrate or intercept cryptographic keys (DEK/KEK managed via Google Cloud KMS in the EU region), or attempt to breach the memory isolation of the AMD SEV-SNP CPUs and NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200 GPUs.

4.2. Model Extraction, Reverse Engineering, and Computational Scraping: any attempt to decompile proprietary platform components, or to extract or clone the weights of the language models residing within the enclave (e.g., Qwen 3.6 Flash Next) through model inversion attacks, unauthorized distillation, or automated mass querying (scraping via scripts or bots).

4.3. Volumetric Attacks, Replay Attacks, and Resource Saturation (OOM / Denial of Wallet): deliberate submission of malformed payloads, alteration of cryptographic timestamps (Replay Attacks), execution of Denial of Service (DDoS) attacks, or any action aimed at maliciously saturating GPU VRAM memory (Out-of-Memory attacks) or network bandwidth to the detriment of the infrastructure and other Customers.

ARTICLE 5 - SUSPENSION MEASURES ("KILL-SWITCH"), TERMINATION, AND ARCHIVE MANAGEMENT

5.1. Technical Determination of Violations. DEXIMA TECH LLC assesses violations of this AUP based on objective technical evidence (such as Cloudflare WAF security alerts, anomalies in session integrity checks, attempts to force KMS policies, or attacks on the infrastructure), as well as on binding orders from competent authorities.

5.2. Immediate Precautionary Suspension ("Computational Kill-Switch"). In the presence of an active cyberattack, an attempt to compromise the hardware enclave, or a severe violation of Articles 2, 3, or 4, the Company has the right to immediately activate the technical protection protocol (Kill-Switch), which entails the instantaneous suspension of session tokens, API credentials, and AI processing cycles. Where, for an Enterprise Customer, the anomaly concerns solely the compromised credential of a single authorized user without involving the entire Tenant, the Company may limit the precautionary suspension to the affected user account while giving immediate notice to the Customer's IT contact.

5.3. Termination for Cause and Protection of Data Export Rights (Art. 15.2 ToS and Art. 28.3.g GDPR). Where the violation is confirmed and constitutes grounds for immediate termination of the Agreement pursuant to Article 15.1 of the ToS:
(a) Fees: the Agreement shall be terminated for cause attributable to the Customer (Termination for Cause / Art. 1456 Italian Civil Code), without any right of the Customer to a refund of fees or units for the current period, without prejudice to the Company's right to claim compensation for any greater damage suffered;
(b) Data Export and Cryptographic Erasure: in full consistency with Article 15.2 of the ToS, Section 7 of the Privacy Policy, and Article 11 of the DPA, even in the event of contract termination the Company allows the Controller Customer to export its encrypted archives prior to executing the permanent Cryptographic Erasure (T=0 / T=30) of the key on Google Cloud KMS (and consequent unintelligibility on Cloudflare R2, Qdrant, and Backblaze B2), except where retention, provision, or export is expressly prohibited by a lawful order of a judicial authority or where the Payload itself constitutes an active cyberattack tool (malware / exploit) against the infrastructure. For EU Consumers, the safeguards set forth in Article 15.2 of the ToS remain unaffected.

ARTICLE 6 - INDEMNIFICATION FOR SANCTIONS AND PROCEEDINGS
In accordance with and in full application of Article 7.3 of the Terms of Service (Indemnification) and Article 10.2 of the DPA, should a violation of this AUP by the Customer or its authorized users result in third-party claims, inspections, judicial proceedings, or administrative/pecuniary sanctions (including fines by Data Protection Supervisory Authorities, AI market surveillance authorities under Regulation (EU) 2024/1689, or US and European governmental authorities) against DEXIMA TECH LLC or its Sub-Processors, the Customer undertakes to fully indemnify, defend, and hold harmless the Company from and against any fine, damage, technical remediation cost, forensic audit expense, and legal fee incurred for its defense.

ARTICLE 7 - ABUSE REPORTING, GOVERNING LAW, AND EXCLUSIVE JURISDICTION

7.1. Reporting Violations. Any report concerning suspected violations of this AUP or infrastructure security may be sent to: privacy@loricai.io or support@loricai.io.

7.2. Governing Law and Jurisdiction. This AUP is governed by the same applicable law and is subject to the same exclusive jurisdiction established by Article 8 of the Terms of Service (ToS) and Section 10 of the Privacy Policy (Law of the Republic of Ireland and exclusive jurisdiction of the Courts of Dublin for Business and Professional Customers established in the European Union, EEA, United Kingdom, and Switzerland; Law of the State of Wyoming and binding AAA arbitration in Casper, Wyoming for Business Customers established in the USA and the rest of the non-European world; non-derogable venue of residence for EU Consumers).