Business terms of service

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

TERMS OF SERVICE (ToS) - DEXIMA TECH LLC

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

1. SUBJECT MATTER AND NATURE OF THE AGREEMENT

1.1. Binding Agreement. This document ("Terms of Service" or "ToS") governs access to and use of the document processing platform and infrastructure named "LoricAI" ("Service" or "Infrastructure") and constitutes a legally binding agreement between DEXIMA TECH LLC ("Company") and the entity or individual (legal entity, professional firm, practitioner, or natural person of legal age) accessing or using the Service ("Customer", "User", or "Licensee").

1.2. Confidential Computing Infrastructure in the European Union. This Agreement governs access to an infrastructure operating through Confidential Computing technology (Trusted Execution Environments / TEE) on AMD CPUs with SEV-SNP technology and NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200 GPUs (or higher architectures), physically located in the European Union, in Finland (at qualified Verda / DataCrunch Oy data centers), with encrypted storage in the European Union (Cloudflare R2 and isolated Qdrant instances) and encrypted backups in the European Union (Backblaze B2).

1.3. Technical Inability to Access (Zero-Knowledge Architecture). The LoricAI architecture is engineered according to the Zero-Knowledge / Blind Conduit principle. The Company declares, and the User acknowledges, the technical and mathematical impossibility for the Company to access in plaintext the content of uploaded documents ("Payload Data"), submitted queries, decryption keys (DEK/KEK), or processing results: on-device encryption protects data in transit and at rest, while the key management service (Google Cloud KMS in the EU region) is structurally separated from the documents and releases keys exclusively to the authorized hardware enclave upon passing cryptographic integrity checks (AMD and NVIDIA Remote Attestation). Any interpretation of this Agreement that presupposes plaintext content control, review, or monitoring by the Company is null, void, and contrary to the technical nature of the Service.

1.4. Age Requirement and COPPA. Use of the Service is strictly prohibited for individuals under eighteen (18) years of age. The Company is not subject to COPPA (Children's Online Privacy Protection Act) as the Service is intended exclusively for an adult, corporate, and professional audience. Detection of an account registered to a minor shall result in the immediate termination of the Agreement pursuant to Article 15.1.

2. OPERATIONAL DEFINITIONS For the purposes of these ToS, and in full consistency with the Global Privacy & Data Protection Policy ("Privacy Policy") and the Data Processing Agreement ("DPA"), the following definitions apply:
• "Cryptographic Client Module (Client Aegis / Web-Client)": The software interface (local application, web-client, or authorized enterprise connector) that verifies AMD/NVIDIA hardware attestation and performs on-device encryption of Payload Data prior to transmission to the Infrastructure.
• "Hardware Enclave (Confidential Computing TEE)": The silicon-isolated hardware environment

(AMD SEV-SNP CPU and NVIDIA GPU) where volatile memory (RAM/VRAM) is hardware-encrypted and where temporary decryption and AI model inference take place.
• "KMS Service (Google Cloud KMS - EU Region)": The cryptographic key management system located in the European Union, structurally separated from document storage and governed by a Key Release Policy that conditions the release of the Customer's key upon cryptographic verification of the Hardware Enclave.
• "Cryptographic Erasure (Crypto-Shredding)": The process of permanent destruction of the Customer's dedicated cryptographic key (DEK/KEK) within the KMS Service, rendering all encrypted data stored in active storage, vector indices, and immutable backups mathematically and permanently indecipherable.
• "Payload Data (or Payload)": Any file, document, case file, text input (prompt), query, audio fragment, image, or content uploaded or generated by the User within the workspaces for processing.
• "Inference Unit (IU) / Computational Capacity": The unit of measurement of document volume, workspace allocation, and computing capacity assigned to the Customer.

3. SERVICE MODELS, TECHNICAL TRIAL, AND FINANCIAL TERMS

3.1. Preliminary Technical Trial ("Results First, Contract Later"). Where agreed with the Company, a Business or Professional Customer may access a preliminary trial phase on real use cases prior to executing a subscription or commercial agreement. Such phase is governed exclusively by this confidentiality undertaking, these ToS, and the DPA pursuant to Art. 28 GDPR. During the trial, documents are protected by the same Zero-Knowledge architecture with a dedicated key. Should the Customer decide not to enter into a commercial agreement upon completion of the trial, no fee shall be due and the Company shall immediately (T=0) execute the Cryptographic Erasure of the trial data pursuant to Article 7.1 of the Privacy Policy.

3.2. Plans for Professionals, Firms, and Enterprises (B2B - SaaS and Enterprise).
• Standard Plans (Professionals and Firms): Entail an advance monthly or annual subscription fee scaled according to workspace allocation, number of authorized users, and assigned processing capacity.
• Custom Enterprise Projects and Contracts (Enterprise): For enterprises requiring dedicated capacity, custom vertical workflows, or connectors to corporate repositories and management systems (ERP/CRM), the applicable fees (broken down between recurring fee, optional setup/onboarding, and agreed integrations), payment methods (including SEPA/Wire Transfer against invoice), and any dedicated Service Level Agreements (SLA) are set forth in the relevant Commercial Order Form or Enterprise Agreement. No extra setup or integration fee is ever applied without prior written agreement.
• Renewal and Cancellation: Unless otherwise agreed in writing in the Commercial Order Form, recurring subscriptions renew automatically for periods of equal duration, subject to cancellation by the Customer up to twenty-four (24) hours prior to the expiration of the current term via the Dashboard or by written notice. No pro-rata refunds are provided for partially used periods, except in the event of breach attributable to the Company.

3.3. Pay-Per-Use Access and Consumers (B2C). Where the Company makes available the prepaid purchase of Inference Unit (IU) packages or access to individuals qualifying as Consumers:
• Nature of Purchase: The purchase of Inference Units constitutes an advance payment for the provision of computational technology services and does not constitute a deposit of value or electronic money. Unused Units expire twelve (12) months from the date of purchase.
• Immediate Performance and Right of Withdrawal (Art. 59 Italian Consumer Code / EU Directive 2011/83/EU): The Consumer User expressly acknowledges and agrees that initiating the first computational processing at the User's request prior to the expiration of the 14-day withdrawal

period entails the immediate performance of the digital supply and the consequent extinguishment of the right of withdrawal strictly with respect to the services and units already consumed.

4. INTELLECTUAL PROPERTY AND OWNERSHIP OF ENCRYPTED ARCHIVES

4.1. Company Ownership, Inspectable Components, and AI Models. The cloud orchestration architecture, proprietary procedural workflows, and the LoricAI trademark are the exclusive property of DEXIMA TECH LLC. In order to guarantee the verifiability of the Zero-Knowledge architecture and enable the Customer's IT department to perform the AMD and NVIDIA Remote Attestation procedure, the client verification software components and attestation protocols are made inspectable or released under an Open Source license (e.g., Apache License 2.0 or MIT) as specified in the official technical documentation. The Artificial Intelligence language models executed locally within the Enclave (e.g., Qwen 3.6 Flash Next) remain the property of their respective authors in accordance with their applicable licenses.

4.2. Exclusive User Ownership of Payload and Output. The User retains full and exclusive intellectual property and legal ownership over all uploaded Payload Data and acquires exclusively all rights, title, and interest in and to the Outputs (drafts, analyses, quotes, documents) generated by the Service from the User's Payload Data. The Company claims no ownership or usage rights over the Customer's Outputs.

4.3. Technical Use Restrictions. The User is strictly prohibited from: (a) using the Service to perform automated mass extraction (model extraction, distillation, or imitation training) aimed at replicating the weights of the underlying models; (b) omitting disclosures of AI-assisted generation where strictly required by statutory or professional ethics rules applicable to the User.

4.4. Ownership of Encrypted Archives and Vector Indices. The User acknowledges that the Infrastructure stores in encrypted form the case documents (on Cloudflare R2 in the EU region), encrypted backups (on Backblaze B2 in the EU region), and encrypted mathematical vector representations (Embeddings on an isolated Qdrant database in the EU) for the sole purpose of enabling workspace persistence and source-verified search:
• Exclusive Customer Ownership: Such encrypted blocks and Embeddings constitute digital extensions of the Payload Data and belong exclusively to the Customer.
• Technical Custody Mandate: The Customer grants the Company solely a technical mandate (as Bailee and Data Processor pursuant to Art. 28 GDPR) to hold in custody and process such encrypted blocks for the provision of the Service, subject to an absolute prohibition on model training (No AI Training).
• Effects of Termination: Upon termination of the contractual relationship or upon instruction from the Customer, the Company executes Cryptographic Erasure (Crypto-Shredding) by destroying the key on Google Cloud KMS in accordance with the timelines set forth in Section 7 of the Privacy Policy (T=0 or T=30).

5. SERVICE DELIVERY, "HUMAN-IN-THE-LOOP", SLA, AND AUDIT LOGS

5.1. Probabilistic Nature of AI and "AS IS" Delivery. Artificial intelligence models operate on a statistical and probabilistic basis. Although LoricAI provides direct source linking (document, page, and paragraph) for every response, the Company does not warrant that the Output will be free from logical errors, omissions, or inaccuracies ("hallucinations").

5.2. Mandatory Human Oversight ("Human-in-the-Loop"). LoricAI is a technical and documentary support tool. A human being always makes the final decision: the Customer (or the qualified professional appointed by the Customer: attorney, accountant, psychologist, physician, insurer, engineer, or corporate officer) has the non-derogable obligation to verify the cited sources and

validate every draft, quote, or analysis prior to any external use, execution, or submission to third parties. The Company shall not be liable for decisions taken by the Customer without adequate human verification.

5.3. Service Availability and Service Level Agreements (SLA). For standard plans and trial phases, the Service is provided without a contractual guarantee of uninterrupted continuity; temporary suspensions for scheduled maintenance or security updates of the AMD/NVIDIA enclaves do not constitute a breach. For Business/Enterprise Customers that have executed a specific Service Level Agreement (SLA), the availability metrics (uptime), support response times, and contractual remedies set forth therein shall apply.

5.4. Cryptographic Traceability and Audit Logs (Non-Content Hashes). Without prejudice to the cryptographic erasure of Payload Data guaranteed by the destruction of the Customer's key on Google Cloud KMS, the User acknowledges that, in accordance with Article 4.6(b) of the Privacy Policy, pseudonymized technical records devoid of any plaintext content (cryptographic session hashes, hardware attestation logs, and key access logs) are retained for a period of five (5) years in order to ensure technical verifiability of the service, regulatory accountability, and the establishment, exercise, or defense of legal claims (Art. 6.1.f and Art. 17.3.e GDPR). Such records never contain plaintext documents or text and do not allow reconstruction of the Payload in any way.

6. ACCEPTABLE USE (AUP), SECURITY, AND EU AI ACT COMPLIANCE The commission of any of the following conducts constitutes a material breach of contract entitling the Company to immediate suspension or termination of the Agreement for cause (Art. 15.1):
• Infrastructure Attacks and Hardware Bypass: Any attempt to breach, alter, or bypass the hardware isolation of the AMD SEV-SNP CPU and NVIDIA GPU enclaves, the Remote Attestation mechanisms, or the Google Cloud KMS policies.
• Computational Abuse, Replay Attacks, and DDoS: The malicious submission of malformed payloads, volumetric attacks (DDoS), replay attacks, or the use of unauthorized scripts aimed at saturating GPU resources; such anomalies shall result in immediate blocking at the Web Application Firewall level (Cloudflare WAF).
• Compliance with Regulation (EU) 2024/1689 (EU AI Act) and Prohibition of High-Risk Automated Decisions: In accordance with Article 8.2 of the Privacy Policy, LoricAI operates as a preparatory, procedural, and documentary support tool subject to mandatory human review pursuant to Article 6(3) of Regulation (EU) 2024/1689 (AI Act) and does not constitute a "High-Risk" AI system under Annex III. The User is strictly prohibited from using the Outputs of the Service to take fully automated decisions, devoid of effective human verification and decision-making validation, in areas classified as prohibited (Art. 5 AI Act) or "High-Risk" (Annex III AI Act, such as fully automated recruitment screening, autonomous creditworthiness scoring or access to essential services, biometric categorization, or emotion recognition). The User assumes sole and exclusive liability in the event of breach of such mandatory human oversight obligation.

7. LIMITATION OF LIABILITY AND INDEMNIFICATION

7.1. Quantitative Limitation of Liability (Liability Cap). To the maximum extent permitted by applicable law, and except in cases of willful misconduct or gross negligence that cannot be limited by law, the total aggregate liability of DEXIMA TECH LLC for any contractual or extra-contractual claim arising out of or relating to this Agreement shall under no circumstances exceed: (1) for Customers with an active paid plan or contract, the total amount of fees actually paid by the Customer to the Company during the twelve (12) months preceding the event giving rise to liability (or the higher cap specifically agreed in writing in a dedicated Enterprise Agreement / SLA); (2) for Users in a free trial phase or with total expenditure below EUR 100.00

during the preceding twelve (12) months, the all-inclusive sum of EUR 100.00 (or $100.00 USD). By way of derogation from point (1) above, in the event of an established personal data breach (Data Breach) attributable exclusively to a breach of the Company's security obligations, the cap under point (1) is increased to twice (2x) the fees paid by the Customer during the preceding twelve (12) months. Mandatory provisions of applicable law, including Article 82 of the GDPR, remain unaffected in all cases.

7.2. Exclusion of Indirect Damages. Except in cases of willful misconduct or gross negligence, the Company shall under no circumstances be liable for indirect, consequential, or incidental damages, loss of profits, loss of revenue, or business interruption arising from the use of or failure to perform human verification of the Outputs. 7.3. Indemnification. The Business or Professional Customer agrees to indemnify, defend, and hold harmless DEXIMA TECH LLC, its directors, employees, and Sub-Processors from and against any third-party claim, regulatory fine, or damage arising from: (a) uploading into Payload Data content acquired by the Customer in breach of law, professional secrecy, or third-party intellectual property rights; (b) use of the Service in violation of the prohibitions under Article 6 or the human oversight obligation under Article 5.2; (c) opinions, filings, quotes, or decisions rendered or taken by the Customer toward its own clientele or third parties based on the generated Outputs.

8. GOVERNING LAW AND JURISDICTION (JURISDICTIONAL SEGMENTATION)

8.1. Business and Professional Users (USA and Non-European Jurisdictions, excluding EEA, UK, and Switzerland). For corporate and professional Customers established in the United States or in jurisdictions outside the European Union, the European Economic Area (EEA), the United Kingdom, and Switzerland, this Agreement is governed by the laws of the State of Wyoming (USA), without regard to conflict of law principles. Any dispute arising out of or relating to these ToS shall be resolved exclusively through binding arbitration administered by the American Arbitration Association (AAA) seated in Casper, Wyoming, USA, with the Parties waiving the jurisdiction of any other court.

8.2. Business and Professional Users (B2B - European Union, EEA, UK, and Switzerland). For corporate and professional Customers established in the European Union (as well as in the EEA, the United Kingdom, or Switzerland), this Agreement is governed by and construed in accordance with the laws of the Republic of Ireland. Without prejudice to the non-derogable rights of Data Subjects under Articles 77, 78, and 79 of the GDPR, any contractual, commercial, or tort dispute arising out of these ToS or connected contractual documents shall be subject to the exclusive jurisdiction of the Courts of Dublin (Republic of Ireland). The Parties explicitly waive US jurisdiction and Wyoming AAA arbitration for this category of Customers.

8.3. Consumers (B2C - European Union). Where the User acts as a consumer under European Union law, this clause does not affect in any way the application of mandatory provisions and non-derogable venues provided by the law of the country of habitual residence of the consumer (including Regulation (EU) 1215/2012 and Regulation (EC) 593/2008 "Rome I"). In such cases, the consumer may bring proceedings before the courts of their place of residence.

8.4. Evidentiary Relevance of the Technical Architecture. In any judicial or arbitral proceeding, the Parties acknowledge the objective technical characteristics of impossibility of plaintext access to Payload Data resulting from the Zero-Knowledge Architecture, the Remote Attestation certificates signed by AMD and NVIDIA, and the cryptographic policies recorded on Google Cloud KMS.

8.5. Class Action Waiver. To the maximum extent permitted by applicable law, and without prejudice to the non-derogable rights of consumers residing in the European Union or other jurisdictions that prohibit such limitation, the User agrees to bring any legal action against the

Company solely in an individual capacity, waiving any right to participate as a plaintiff or class member in any class, collective, or consolidated proceeding (Class Action or Representative Proceeding).

9. MASS ARBITRATION PROTOCOL (Applicable exclusively to disputes subject to US AAA Arbitration pursuant to Art. 8.1)

9.1. Definition of Mass Claim. A "Mass Claim" arises where twenty-five (25) or more Users subject to the jurisdiction under Art. 8.1 file substantially similar arbitration demands against the Company, represented by the same law firms or acting in coordination, within a one hundred eighty (180) day period.

9.2. Mandatory Informal Resolution and Mediation. Prior to formal filing with the AAA, a global negotiation and mediation phase of sixty (60) days is mandatory.

9.3. Bellwether Procedure. Should mediation fail to resolve the disputes, the Parties shall select ten (10) "Bellwether Cases" (5 chosen by the claimants and 5 by the Company) to proceed to immediate arbitration. All remaining claims (and their associated administrative filing fees) shall be stayed, with simultaneous tolling of applicable statutes of limitation (tolling).

9.4. Batching. Upon completion of the Bellwether Cases without a global settlement, the remaining claims shall be administered in subsequent Batches of no more than fifty (50) cases at a time.

10. WEB PORTAL, WORKSPACES, AND ENVIRONMENT SEPARATION

10.1. Separation Between Administrative Management and Compute Enclave. The public web portal and account administrative management systems are structurally separated from the processing Hardware Enclave. Administrative systems handle exclusively authentication, usage volume monitoring, contracting, and billing (via PCI-DSS certified gateways such as Stripe Payments Europe Ltd., PayPal, or bank transfer) and never perform inference functions nor have plaintext access to Payload Data. All temporary decryption and AI document processing operations take place exclusively within the isolated Hardware Enclave (AMD SEV-SNP CPU and NVIDIA GPU) located in Finland (EU).

10.2. Mandatory Retention of Fiscal Records. In accordance with Article 7.3 of the Privacy Policy, account deletion and Cryptographic Erasure of Payload Data do not entail the removal of accounting, contractual, and billing records, which the Company is legally required to retain for ten (10) years in a logically isolated environment (Blind Indexing).

11. AI MODEL ISOLATION AND ABSENCE OF THIRD-PARTY TRANSMISSIONS

11.1. Local Execution Within the Enclave. The Company executes the Artificial Intelligence language models (e.g., Qwen 3.6 Flash Next) directly and entirely within its hardened hardware infrastructure in Finland (EU). 11.2. Absence of Connections to Third-Party AI. The LoricAI Infrastructure operates within an isolated processing perimeter: it makes no outbound API calls to external artificial intelligence providers (such as OpenAI, Anthropic, or other third-party services) for the processing of Payload Data, technically guaranteeing that no User document or query is ever passed to third-party AI systems or used to train any model.

12. LICENSING REGIME, SUSPENSION, AND DELETION CYCLE

12.1. Credentials and Workspace. Each license grants the Customer and its authorized users the right to access their encrypted workspace and use the dedicated key in accordance with configured policies. The Customer is responsible for safeguarding the access credentials of its authorized users.

12.2. Non-Payment, Default Interest, Suspension, and Data Export. In the event of late payment, non-payment at maturity, or subscription termination (without prejudice, for Business Customers, to the automatic accrual of statutory commercial default interest pursuant to Directive 2011/7/EU without the need for formal notice of default): (1) the execution of new AI processing requests is suspended; (2) except in the case of a request for Immediate Deletion (T=0), during the thirty (30) day security Grace Period set forth in Article 7.1 of the Privacy Policy, the Customer retains the ability to autonomously export and download its documents and archives (including pursuant to Regulation (EU) 2023/2854 - EU Data Act) before the system executes, on the thirtieth day (T=30), the permanent Cryptographic Erasure of the key on Google Cloud KMS.

13. EXCLUSION OF PROFESSIONAL ADVICE AND OBLIGATION OF MEANS

13.1. Exclusion of Regulated Professional Qualification. DEXIMA TECH LLC is a technology provider of software infrastructure and confidential computing and is not a law, medical, psychological, accounting, engineering, or insurance firm. No Output generated by the Software constitutes or may be construed as legal advice, medical/psychological diagnosis, financial advice, or technical certification.

13.2. Obligation of Technological Means. Without prejudice to the Company's absolute commitment to guarantee the promised cryptographic and hardware isolation (infrastructural security obligation), with respect to the drafting and interpretative quality of the Outputs generated by the language model, the Company's performance constitutes exclusively an obligation of technological means and never an obligation of professional result.

14. EXPORT CONTROL AND INTERNATIONAL SANCTIONS (EAR / OFAC / EU) Use of the Infrastructure is subject to export control and economic sanctions laws in force in the United States (EAR, ITAR, OFAC regulations) and the European Union. The Customer represents and warrants that it is not listed on any restricted sanctions list (Sanctions Lists) and that it shall not access or permit access to the Service from or toward comprehensively embargoed territories (including Iran, North Korea, Syria, Cuba, and regions subject to US/EU sanctions restrictions).

15. SERVICE INTERRUPTION, SUSPENSION, AND TERMINATION OF THE AGREEMENT

15.1. Immediate Termination for Cause. The Company reserves the right to suspend or terminate this Agreement with immediate effect (Termination for Cause / Art. 1456 Italian Civil Code) should the Customer: (a) breach the security or usage prohibitions under Articles 1.4, 4.3, 6, or 14; (b) attempt cyberattacks or compromise of the infrastructure; (c) remain in default of payment obligations fifteen (15) days after written notice.

15.2. Data Protection Upon Termination. In any event of expiration or termination of the Agreement, the Company guarantees the Customer the ability to export its Payload Data prior to the execution of Cryptographic Erasure of the key, unless retention or access is expressly prohibited by a lawful order of a judicial authority. For EU Consumers, reasonable prior notice before deactivation remains guaranteed, except in cases of fraud or immediate threat to infrastructure security.

16. CONTRACTUAL AMENDMENTS AND CODE INTEGRITY ("SEALED CODE")

16.1. Enclave Code Updates and Right of Technical Rejection. In accordance with the technical transparency commitment ("Sealed Code"), the program executed inside the Hardware Enclave possesses a cryptographic measurement certified by the AMD and NVIDIA silicon. Every new version of the enclave software is published prior to deployment so that the Customer's IT department may verify it; should an update modify the agreed attestation parameters, the Customer always has the right not to authorize it or to withdraw from the Agreement with

immediate Cryptographic Erasure (T=0) before the change takes effect on its data.

16.2. Amendments to the Terms of Service. The Company may update these ToS to adapt them to regulatory developments (e.g., AI Act/GDPR implementing regulations) or Service improvements that never reduce the guaranteed level of cryptographic and hardware protection. Material changes shall be notified to registered Users via e-mail or Dashboard notification with a minimum prior notice of fifteen (15) days - extended to thirty (30) days for EU Consumers and Customers with an Enterprise Agreement - prior to their effective date. Should the User not wish to accept the changes, the User may withdraw from the Agreement without penalty prior to the effective date, exporting its data.

17. FINAL PROVISIONS AND CONTRACTUAL HIERARCHY

17.1. Severability. Should any provision of these ToS be held invalid, ineffective, or unenforceable by a competent court or arbitral tribunal, the remaining provisions shall remain in full force and effect, and the invalid clause shall be replaced or interpreted to the minimum extent necessary to render it fully valid while preserving the original balance between the Parties.

17.2. Language Versions. These ToS are made available in Italian, English, and the other languages published on the official website. For Customers established in Italy, the Italian language version is authoritative for all purposes; for international relationships outside Italy, in the event of interpretative divergence, the English language version shall prevail, without prejudice to the non-derogable rights of consumers in their national language.

17.3. Entire Agreement and Order of Precedence. These Terms of Service (ToS), together with the Privacy Policy, the Data Processing Agreement (DPA pursuant to Art. 28 GDPR), the Acceptable Use Policy (AUP), and, for corporate Customers, any executed Commercial Order Form / Enterprise Agreement and SLA, constitute the entire agreement between the Parties. In the event of conflict between the documents, the following order of precedence shall apply: (1) for personal data protection matters, the DPA pursuant to Art. 28 GDPR and the Privacy Policy; (2) for dedicated commercial and service level parameters, the executed Enterprise Agreement / SLA; (3) these ToS.

18. DECLARATION OF ACCEPTANCE By creating an account, initiating a technical trial, executing a Commercial Order Form, or using the LoricAI Infrastructure, the Customer declares that it has read, understood, and accepted these Terms of Service, the Privacy Policy, and the DPA pursuant to Art. 28 GDPR, and also confirms, where applicable pursuant to Articles 1341 and 1342 of the Italian Civil Code and equivalent international rules, its specific acceptance of the clauses set forth in Articles: 3.2 (Automatic renewal), 5.1 and 5.2 (Probabilistic nature of AI and mandatory human oversight), 5.3 (Availability and SLA), 6 (Acceptable use and AI Act prohibitions), 7.1, 7.2, and 7.3 (Limitation of liability, exclusion of indirect damages, and indemnification), 8.1, 8.2, and 8.5 (Governing law, exclusive Dublin venue / AAA arbitration, and class action waiver), 9 (Mass claims), 12.2 (Suspension of performance for non-payment), 15.1 (Immediate termination), and 16.1-16.2 (Technical and contractual amendments).

19. THE SEAL CLAUSE

19.1. Physical and Cryptographic Inviolability of the Architecture. The Parties acknowledge and agree that the entire technical and legal framework of LoricAI and DEXIMA TECH LLC is founded upon the cardinal principle of the technical impossibility of plaintext access to Payload Data (Zero-Knowledge Hardware Isolation). Because documents are encrypted on the device, decryption keys are separated on Google Cloud KMS (EU region) under cryptographic attestation constraints, and processing takes place exclusively inside the encrypted memory of the AMD and NVIDIA hardware enclaves in Finland, any contractual claim or interpretation that presupposes a faculty of inspection, reading, moderation, or autonomous decryption of content by the Company is

technically unfeasible and legally devoid of effect between the Parties.