Privacy notice

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

GLOBAL PRIVACY & DATA PROTECTION POLICY
Effective Date: 01/2026 - Last Updated: 11/2026
Territorial Scope: Global (USA, EU, EEA, United Kingdom pursuant to the UK GDPR and the Data Protection Act 2018, Switzerland pursuant to the Federal Act on Data Protection - FADP/nLPD, and Rest of the World).

PREAMBLE AND CONTROLLER/PROCESSOR ROLES
This Global Privacy & Data Protection Policy ("Policy") governs the data processing carried out by DEXIMA TECH LLC, with registered office at 5830 E 2nd St, Ste 7000 #32263, Casper, Wyoming 82609, USA ("Company" or "We"). For the purposes of Regulation (EU) 2016/679 ("GDPR") and the UK GDPR, privacy roles are allocated as follows:
Role of Data Controller: The Company acts as an independent Data Controller exclusively for Registration and Account Data (Sec. 4.1), Pre-Contractual, Demo, and Support Data (Sec. 4.2), Billing Data (Sec. 4.3), and Infrastructure Security Logs (Sec. 4.4).
Role of Data Processor (Art. 28 GDPR): In relation to all documents, files, texts, and content uploaded by the User into the workspaces ("Payload Data"), the Customer (enterprise, professional firm, or practitioner) acts as the sole Data Controller, while the Company acts exclusively as Data Processor in Zero-Knowledge / Blind Conduit mode, pursuant to the Data Processing Agreement (DPA under Art. 28 GDPR) executed with the Customer.
Legal, Privacy, and EU Point of Contact (Art. 27 GDPR): privacy@loricai.io - All requests from Data Subjects and European Union Supervisory Authorities are handled directly and with priority by the Privacy & Compliance Department at this address; the details of the Representative designated in the European Union pursuant to Art. 27 GDPR are made available upon request and set forth in the corporate DPA.

1. CONTRACTUAL DEFINITIONS For the purposes of this Policy, the following capitalized terms shall have the meanings set forth below:

1.1. "Zero-Knowledge Architecture and Hardware Isolation": The LoricAI infrastructure is founded upon the mathematical and physical segregation of data. Thanks to on-device encryption applied for transit and storage and the use of AMD and NVIDIA processors in Confidential Computing mode, Payload Data is decrypted exclusively inside an isolated and verified hardware enclave. DEXIMA TECH LLC attests to the technical impossibility for its administrators, operators, or third parties to access, read, or intercept data in plaintext: the volatile memory (RAM/VRAM) of the enclave is protected by ephemeral hardware keys, while the key management service (Google Cloud KMS in the EU region) never receives the documents and releases decryption keys exclusively to the protected environment after passing cryptographic integrity checks (AMD and NVIDIA Remote Attestation).

1.2. "Payload Data": 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.

1.3. "Confidential Computing (TEE)": Trusted Execution Environments residing on specialized hardware (AMD CPUs with SEV-SNP technology and NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200 GPUs) that prevent access to volatile memory (RAM/VRAM) even by the operating system, the host hypervisor, and the data center operator.

1.4. "Cryptographic Erasure (Crypto-Shredding)": The process of revocation and permanent destruction (Key Destruction) of the Customer's dedicated cryptographic key (DEK/KEK), rendering all encrypted data stored in active storage, vector databases, and immutable backups mathematically and permanently indecipherable.

1.5. "Blind Index": The cryptographic search index generated via the HMAC-SHA256 function, which enables logical separation of environments and prevents direct correlation between administrative database records and the identity or cryptographic keys of the Tenant in the event of physical compromise of the systems.

2. DATA SOVEREIGNTY AND JURISDICTIONAL BOUNDARIES (DATA RESIDENCY)

2.1. Geographic Confinement (EU Data Residency) and Persistent Encryption. Notwithstanding its corporate formation in the State of Wyoming (USA), the Company establishes a strict perimeter of data residency and processing within the European Union:
the Confidential Computing compute nodes (AMD CPUs and NVIDIA GPUs) physically reside in the European Union, in Finland;
Payload Data in native plaintext format is never materialized, allocated, or written to persistent storage media (Block Storage, SSD, or Object Storage);
documents uploaded into workspaces, vector indices (on the Qdrant database), and backups are stored exclusively in encrypted format within the European Union (on Cloudflare R2 storage in the EU region and backups on Backblaze B2 in the EU region), protected by a cryptographic key dedicated to each Customer managed separately via Google Cloud KMS (EU region).

2.2. Protection Against Extraterritorial Orders (e.g., US CLOUD Act). Encrypted documents and decryption keys remain structurally separated. Because the cryptographic Key Release Policy authorizes delivery of the key exclusively inside the AMD/NVIDIA hardware enclave verified via Remote Attestation and never to DEXIMA TECH LLC administrators or the KMS service provider, the Company is in a state of material technical impossibility to decrypt or produce Payload Data in plaintext in response to extraterritorial judicial or governmental orders (including the US CLOUD Act). The Company undertakes in any case to formally challenge any non-EU governmental request conflicting with Art. 48 of the GDPR, promptly informing the Customer where legally permitted.

2.3. CALIFORNIA RESIDENTS' RIGHTS (CCPA/CPRA). Pursuant to United States privacy laws, DEXIMA TECH LLC provides this 'Notice at Collection'.
Categories of data collected: Professional identifiers and contact details (first name, last name, e-mail, phone number, company, temporary IP address/hash for security), commercial and billing information (transaction history), and internet network activity (technical security and access logs), as detailed in Section 4. The Company DOES NOT collect, access, or "share" Sensitive Personal Information (SPI). Payload Data uploaded by the User is subject to Zero-Knowledge hardware encryption; consequently, the Company does not possess the decryption keys and treats such data as opaque cryptographic fragments that cannot be linked to personal information readable by the Company.
Purpose: Service provision and IT security.
Rights: The Company does not 'Sell' or 'Share' personal data for cross-context behavioral advertising. United States residents may exercise their rights of access, correction, and deletion by sending a request to privacy@loricai.io. We apply the same hardware protection standards (Root of Trust) to all data of US residents.

3. PROCESSING MECHANICS AND AI INFERENCE HARDENING The Company acts as a Blind Conduit with respect to Payload Data. Legal and technical liability is bounded by the following operational parameters:

3.1. Separation Between Encrypted Storage and Enclave Decryption. On-device encryption protects documents during transit and while at rest in storage. Payload Data and its encrypted vector representations (embeddings on Qdrant) reside on persistent storage in the European Union solely as opaque ciphertext. To process a User request, data is decrypted solely inside the isolated volatile memory (RAM/VRAM) of the authorized hardware enclave, where the AI model operates locally.

3.2. Compute Session Volatility. Inside the hardware enclave, decrypted data resides exclusively in protected volatile memory (tmpfs / encrypted VRAM) for the time strictly necessary to complete inference and transmit the encrypted response to the User's workspace over a secure channel, with immediate destruction of temporary session buffers upon completion of computation (and in any event with a Time-To-Live of inactive post-inference buffers not exceeding 60 seconds).

3.3. Memory Zeroization (VRAM Scrubbing). At the end of each processing request inside the enclave, the system forcibly executes cryptographic zeroization of GPU memory buffers (cudaMemset(ptr, 0, size) and cudaDeviceReset()) and wipes allocated volatile memory, guaranteeing the total absence of plaintext forensic residues of Payload Data.

3.4. AI Model Isolation and Training Prohibition (NO AI TRAINING). Processing is performed via language models (e.g., Qwen 3.6 Flash Next) executed directly and entirely inside the isolated hardware enclave in Finland. Payload Data is never transmitted to external third-party AI services nor is it ever used for training, fine-tuning, or improving any Artificial Intelligence model. Every inference is executed in stateless mode with respect to model weights.
3.5. Legal and Technical Nature of Encrypted Archives and Embeddings. Encrypted documents (stored on Cloudflare R2 in the EU region) and their Encrypted Vector Representations (embeddings stored on a Qdrant vector database running in an isolated instance on the Company's European infrastructure) constitute digital extensions of the User's Payload. They remain under the full and exclusive legal ownership and sovereignty of the Customer. The Company acts exclusively as technical custodian (Bailee) of such encrypted blocks, without any right of plaintext access, use for its own purposes, or claim of intellectual property.

4. CATEGORIES OF DATA COLLECTED AS CONTROLLER, PURPOSES, AND LEGAL BASES In its capacity as Data Controller for managing the commercial relationship and service security, the Company collects exclusively the following personal data (Art. 5.1.c GDPR):

4.1. Registration and Authentication Data (Account Data)
Collected elements: First name, last name, professional e-mail address, role/organization, and authentication credentials.
Cryptographic processing: No password is stored in plaintext; cryptographic hashing (Argon2id) with random salt is applied in accordance with current OWASP parameters.
Legal Basis: Performance of a contract (Art. 6.1.b GDPR).

4.2. Pre-Contractual Data, Demo Requests, and Customer Support
Collected elements: First and last name, company or professional firm, work e-mail address, phone number, and use-case information voluntarily provided by the User via the "Book a demo" form, via e-mail (contact@loricai.io, support@loricai.io), or via scheduled telephone contact. Users are advised not to enter confidential or sensitive data in the public contact form.
Legal Basis: Implementation of pre-contractual measures taken at the data subject's request and contractual support (Art. 6.1.b GDPR). Maximum retention in case of non-contracting: 12 months from the last contact.

4.3. Financial and Billing Data (Billing Data)
Collected elements: Company name, tax identifiers (VAT number / Tax ID), billing address, opaque

transaction tokens, bank wire details, amounts, and contractual history.
Processing: For electronic card payments (PCI-DSS SAQ A compliance), card details are handled exclusively by Stripe Payments Europe Ltd. and PayPal (Europe) S.à r.l. et Cie, S.C.A.; for corporate contracts settled via bank transfer, flows are managed through authorized banking institutions. Through environment separation techniques (Blind Indexing), billing data is isolated from the Tenant's cryptographic keys.
Legal Basis: Performance of a contract (Art. 6.1.b GDPR) and compliance with statutory tax, accounting, and AML/KYC obligations (Art. 6.1.c GDPR).
Nature of Provision (Art. 13.2.e GDPR): The provision of data under Sections 4.1, 4.2, and 4.3 is necessary for the conclusion and performance of the contract or pre-contractual measures; failure to provide such data makes it impossible to activate the account, deliver the demo, or provide the Service.

4.4. Operational Data, Security Logs, and Key Access Control (Audit & Security Logs)
Collected elements: IP Address hash, timestamp, queried endpoint, and KMS key integrity check/release events.
Processing: In the application database, IP Addresses are stored exclusively as SHA-256 hashes with a daily rotating salt. In Perimeter Infrastructure Logs only (e.g., Cloudflare WAF and GCP Cloud Logging), raw IP Addresses are temporarily logged for a strict maximum period of thirty (30) days for the sole purpose of mitigating DDoS attacks, preventing abuse, and ensuring network security, without any profiling purpose.
Legal Basis: Legitimate interest in network and information security (Art. 6.1.f and Recital 49 of the GDPR).

4.5. Data Breach Management. In the event of a security breach compromising Personal Data or Metadata processed by the Company as Controller, the Company shall carry out statutory notifications within 72 hours (Arts. 33 and 34 GDPR). Should a security incident involve the infrastructure relating to Payload Data, the Company shall inform the Controller Customer without undue delay pursuant to Art. 33(2) of the GDPR and in accordance with the timelines established in the DPA.

4.6. Data Retention Period
(a) Security Logs and Perimeter IPs: Maximum 30 days for IT security purposes.
(b) Cryptographic Traceability and Audit Logs (Non-Content Hashes): Pseudonymized technical records devoid of plaintext content (cryptographic session hashes, hardware attestation logs, and key access tracking) are retained for
5 (five) 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).
(c) Account Data, Billing, and Contractual Records: Account authentication data (Sec. 4.1) is deleted within 30 days of contract termination (concurrently with the closure procedure under Sec. 7.1), while accounting, tax, and contractual records (Sec. 4.3) are retained for 10 years from the termination of the relationship in compliance with applicable tax and civil law obligations.
(d) Payload Data: Remains under the exclusive control of the Controller Customer and follows the deletion instructions set forth in Section 7 and the DPA.

5. NEGATIVE COVENANTS (DECLARATIONS OF NON-PROCESSING) As a guarantee of transparency and as a binding contractual commitment toward the User and third parties, the Company formally declares that it DOES NOT collect, process, or retain the following categories:

5.1. No Behavioral Tracking: Total absence of behavioral telemetry, psychological profiling, Google Analytics, Meta Pixel, or session-replay software (e.g., Hotjar).

5.2. No Model Training: No Payload Data, prompt, or User interaction is used for fine-tuning, pre-

training, or improving proprietary or third-party Artificial Intelligence models.

5.3. Exclusivity of Technical Cookies: The Company uses exclusively essential technical cookies (or JWT tokens) for the sole purpose of keeping the User's authenticated session active in the Dashboard. Such elements do not perform cross-site behavioral profiling. Proprietary authentication tokens are destroyed at the end of the session, while security and fraud-prevention cookies managed by Sub-Processors (e.g., Stripe, Cloudflare) maintain the strictly necessary technical persistence specified in the dedicated Cookie Policy.

6. MANAGEMENT OF SUB-PROCESSORS (ART. 28 GDPR) Pursuant to Art. 28 of the GDPR and in accordance with the DPA, the Company engages the following qualified Sub-Processors, bound by Data Processing Agreements (DPAs) and, where applicable for entities with a non-EEA parent company, by active certification under the EU-US Data Privacy Framework (DPF) (Art. 45 GDPR) and/or the European Commission's Standard Contractual Clauses (SCCs) (Art. 46 GDPR):
Verda (operated by DataCrunch Oy, Data Center in Finland, European Union): Provision and hosting of dedicated Confidential Computing hardware infrastructure (servers with AMD SEV-SNP CPUs and NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200 GPUs) in Finnish territory (EU).
Google Ireland Limited (European Union): Application infrastructure services and cryptographic key management service (Google Cloud KMS configured in the EU region). The key management service is separated from document storage and operates under a Key Release Policy that subordinates key release to cryptographic verification of AMD and NVIDIA hardware attestation.
Cloudflare, Inc. (Edge Infrastructure and R2 Storage in the European Union): Used for: (i) perimeter network security services (WAF, DDoS mitigation, and edge routing) covered by active certification under the EU-US Data Privacy Framework; (ii) encrypted object storage (Cloudflare R2) with strict geographic confinement (EU Jurisdiction) in the European Union for the Customer's encrypted files.
Backblaze, Inc. (European Union Region): Storage service for encrypted backups (Backblaze B2) located exclusively in data centers situated within the European Union.
AWS EMEA SARL (Luxembourg / Region eu-central-1 Frankfurt, Germany): Transactional e-mail delivery service (AWS SES) entirely confined within the European Union.
Stripe Payments Europe Ltd. (Ireland) and PayPal (Europe) S.à r.l. et Cie (Luxembourg): Used exclusively as independent controllers/processors for electronic payments of Billing Data only (Sec. 4.3), without any involvement in the Payload Data infrastructure.
In accordance with the principle of Privacy by Design (Art. 25 GDPR), no Sub-Processor has access to Payload Data in plaintext: storage providers (Cloudflare R2 and Backblaze B2) host exclusively blocks encrypted on the device/within the enclave, the KMS provider (Google Cloud KMS) never receives the documents, and the hardware provider (Verda) is technically excluded from accessing RAM/VRAM memory by the physical isolation of the AMD and NVIDIA silicon. Pursuant to Art. 28(2) of the GDPR and in accordance with the procedures set forth in the DPA, the Company shall inform the Controller Customer in advance of any intended addition or replacement of the Sub-Processors listed above, guaranteeing the Customer the right to object or to withdraw from the contract with immediate cryptographic erasure (Sec. 7.1) before the new Sub-Processor enters into operation.

7. DELETION CYCLE, BACKUPS, AND RIGHT TO ERASURE (ART. 17 GDPR AND DPA) Deletion requests for Payload Data and workspaces are executed in accordance with the DPA and the instructions of the Controller Customer, subject to passing authentication checks to prevent accidental or malicious destruction (Verifiable Request). Please Note: The User is solely responsible for exporting its data prior to ordering the destruction of cryptographic keys; once the key is destroyed, data recovery is mathematically impossible.

7.1. Immediate Deletion upon Controller Instruction (including Trial End) or Standard Quarantine:

Immediate Deletion (T=0): Upon explicit request of the Controller Customer (as well as automatically at the end of a technical trial should the Customer decide not to execute a contract), the Company proceeds with the immediate deletion of documents from active storage (Cloudflare R2 / Qdrant) and the simultaneous irreversible destruction of the dedicated cryptographic key (DEK/KEK) on Google Cloud KMS (Cryptographic Shredding).
Standard Procedure with Grace Period (T=0 -> T=30): Unless immediate destruction is requested, upon ordinary account closure access tokens are revoked instantaneously (T=0) and a 30-day security period against unintentional deletion applies, at the end of which (T=30) the system executes the permanent destruction of the cryptographic key on Google Cloud KMS.

7.2. Effect on Backups (Backblaze B2) and Physical Overwriting: From the exact moment of destruction of the Customer's cryptographic key (at T=0 or T=30), any residual encrypted copy present in the immutable backups on Backblaze B2 instantaneously becomes mathematically indecipherable entropic waste. Backup rotation cycles subsequently reach natural expiration and physical overwriting in accordance with the business continuity plan defined in the DPA.

7.3. Fiscal Exception (Fiscal Ledger): Only accounting, contractual, and transaction records (Sec. 4.3) are excluded from deletion and are retained for ten (10) years in compliance with Wyoming Title 17 W.S. and European tax and VAT regulations.

7.4. Export and Deletion Autonomy in a Zero-Knowledge Environment: The right of access (Art. 15 GDPR), data portability (Art. 20 GDPR), and erasure over Payload Data is natively guaranteed within the Software interface: the Customer may at any time download, export, or delete its case files and documents without any intermediation by the Company.

8. EU AI ACT COMPLIANCE AND TECHNICAL SUPPORT TOOL The Company provides the Service exclusively as a technical support tool ("Human-in-the-Loop"). In accordance with the AI Act and Art. 22 of the GDPR, the User has the right not to be subject to a decision based solely on automated processing. The User is informed that the Software operates on probabilistic natural language processing models. However, as the Company acts as a Blind Conduit (Zero-Knowledge infrastructure) devoid of plaintext access to Payload Data, it is technically impossible for the Company itself to perform a "human review" of generated outputs. The obligation of human oversight, interpretation, and validation of results falls entirely and exclusively on the end User or the professional appointed by the User, as established in the Terms of Service (ToS). The User acknowledges the statistical nature of the output; the processing logic relies exclusively on the semantic parameters of the Payload and the User's instructions, without the use of hidden decision-making filters.

8.1. Transparency Obligation (Art. 50 AI Act). Pursuant to Art. 50 of Regulation (EU) 2024/1689 (AI Act), formal notice is hereby given that the User is interacting with an artificial intelligence system and that outputs are generated by probabilistic models susceptible to hallucinations, logical errors, or inaccuracies, always requiring
verification of cited sources by a human professional.

8.2. AI Act Classification (Regulation (EU) 2024/1689). 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 Art. 6(3) of Regulation (EU) 2024/1689 (AI Act). LoricAI does not constitute a "High-Risk" AI system under Annex III of the AI Act as it does not make autonomous or binding decisions. The User is strictly prohibited from using the Outputs of the Service to take fully automated decisions, devoid of effective human verification and validation, in areas classified as "High-Risk" by Annex III of the AI Act (such as automated recruitment screening, autonomous creditworthiness scoring or access to essential services, biometric profiling, or emotion recognition).

9. PROTECTION OF MINORS Use of the infrastructure 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 and professional audience. Detection of accounts registered to minors shall result in the unilateral termination of the service without notice.

10. GOVERNING LAW, JURISDICTION, AND CLASS ACTION WAIVER

10.1. Governing Law (Segmentation). The governing law applicable to this Policy follows the same contractual segmentation established by Article 8 of the Terms of Service (ToS). Specifically:
for Business and Professional Users established in the USA and in Non-European jurisdictions (excluding the EEA, the United Kingdom, and Switzerland), the law of the State of Wyoming (USA) applies;
for Business and Professional Users established in the European Union, the European Economic Area (EEA), the United Kingdom, and Switzerland, the law of the Republic of Ireland applies;
for Consumers, the non-derogable rights provided by the law of their respective place of residence remain unaffected.

10.2. Arbitration and Exclusive Jurisdiction (Jurisdictional Segmentation)
(a) Business and Professional Users (USA and Non-European Jurisdictions, excluding EEA, UK, and Switzerland): Any dispute arising out of or relating to this Policy shall be resolved exclusively through binding arbitration administered by the American Arbitration Association (AAA) seated in Casper, Wyoming, USA. The parties waive the jurisdiction of any other court.
(b) Business and Professional Users (B2B - European Union, EEA, UK, and Switzerland): Without prejudice to the non-derogable rights of Data Subjects under Arts. 77, 78, and 79 of the GDPR, for corporate and professional customers established in the European Union, EEA, United Kingdom, or Switzerland, any contractual, commercial, or tort dispute arising out of this Policy shall be subject to the exclusive jurisdiction of the Courts of Dublin (Republic of Ireland). The Parties explicitly waive Wyoming AAA arbitration for this specific category.
(c) Consumers (B2C - European Union): Where the User acts as a consumer, this clause does not prejudice the non-derogable rights provided by EU regulations (including Regulation (EU) 1215/2012).
The consumer may bring proceedings before the courts of their place of residence, acknowledging the objective technical characteristics of impossibility of plaintext access resulting from the Zero-Knowledge Architecture. Without prejudice to the foregoing, disputes subject to United States jurisdiction and the American Arbitration Association (AAA) pursuant to point (a) above shall also be strictly bound by the Mass Arbitration Protocol defined in the Terms of Service (ToS).

10.3. Class Action Waiver. To the maximum extent permitted by applicable laws, and without prejudice to the non-derogable rights of consumers residing in the European Union or other jurisdictions that prohibit such waiver, the User expressly agrees to bring legal actions against the Company solely in an individual capacity. The User is explicitly prohibited from acting as a plaintiff or class member in any class, representative, or consolidated action (Class Action or Representative Proceeding). The arbitrator may not consolidate more than one person's claims.

11. EXERCISE OF RIGHTS (GDPR & CCPA) AND INTERNATIONAL TRANSFERS Without prejudice to the technical impossibility limitations outlined in Sections 2 and 3 (the Company cannot access Payload Data in plaintext), the User may at any time exercise the rights of Access, Rectification, Erasure, Restriction, Portability, and Objection (Arts. 15-22 GDPR), as well as the right to lodge a complaint with a Supervisory Authority (Art. 77 GDPR). For Users residing in the European Economic Area (EEA), the United Kingdom, and Switzerland, any potential transfer of Personal Data (limited strictly to account, contact, and security Metadata) to the Company in the United

States is governed by the Standard Contractual Clauses (SCCs) approved by the European Commission (Implementing Decision (EU) 2021/914), supplemented by the International Data Transfer Addendum (IDTA) for the United Kingdom and the FDPIC (IFPDT) integrative clauses for Switzerland, while processing entrusted to Sub-Processors with a US parent company is covered by their respective active certification under the EU-US / UK-US / Swiss-US Data Privacy Framework (DPF) (Art. 45 GDPR) and/or current SCCs. The User may request information or a copy of the transfer safeguards adopted by writing to privacy@loricai.io (Art. 13.1.f GDPR). Any request to exercise rights or formal communication may be sent via ordinary or certified e-mail (without formalities) to: DEXIMA TECH LLC - Data Protection & Legal Compliance Department, E-mail: privacy@loricai.io. The Company shall respond to legitimate requests without undue delay and, in any event, within thirty (30) days of receipt of the request pursuant to Art. 12(3) of the GDPR (or within forty-five (45) days for requests subject to the US CCPA), extendable in cases of particular complexity provided for by law.

12. SEVERABILITY. Should any provision of this Policy be held invalid, illegal, or unenforceable by a court of competent jurisdiction, the remaining provisions shall remain in full force and effect, and the invalid provision shall be modified to the minimum extent necessary to render it valid and enforceable, reflecting the original intent as closely as possible.

13. TRANSPARENCY ON GOVERNMENT REQUESTS AND HARDWARE GUARANTEE. The Company undertakes not to disclose Users' Personal Data or Metadata to governmental authorities, except in the presence of a valid, binding, and enforceable judicial order. With respect to Payload Data, thanks to Confidential Computing, documents are decrypted only temporarily inside the isolated volatile memory (protected RAM/VRAM) of the hardware enclave for the time necessary for processing, being immediately overwritten at the end of the session (Memory Scrubbing). Because security is enforced by physical barriers in the silicon (Hardware Root of Trust) and by Remote Attestation protocols verified prior to key release, no judicial order or human intervention can force the extraction of plaintext content that the Company itself is mathematically unable to view or intercept.

14. AMENDMENTS AND UPDATES TO THIS POLICY The Company reserves the right to update this Policy to adapt it to regulatory developments or infrastructural improvements that do not reduce the guaranteed level of cryptographic and hardware protection. Any material changes shall be notified to registered Users with a minimum prior notice of fifteen (15) days via e-mail or Dashboard notification, publishing the updated version with its effective date.

Indicative estimates and contact
An estimate can be requested without email, with an automatic abuse check on this website and no external tracking. When email verification is enabled, the code lasts 15 minutes and guest access 60 minutes. Each request uses a dedicated identity and encryption key, separate from customer accounts. Descriptions and responses are stored encrypted in LoricAI infrastructure; the configured website-estimate archive period is 30 days. Access expiry does not erase all encrypted records. Audio is transcribed in memory and is never archived. The estimate does not use the protected area: describe your work without customer names or confidential data. Email delivery and contact require the visitor’s explicit choice. Requests with email are delivered to the team with their estimate code. The contacts in this notice apply to data rights requests.