Data processing agreement

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

DATA PROCESSING AGREEMENT (DPA PURSUANT TO ART. 28 GDPR)

Effective Date: 01/2026 - Last Updated: 11/2026

Privacy and DPO Contact: privacy@loricai.io

This Data Processing Agreement ("DPA") is entered into pursuant to Article 28 of Regulation (EU) 2016/679 ("GDPR"), the UK GDPR, and the Swiss Federal Act on Data Protection ("FADP/nLPD") between:
The Customer (enterprise, professional firm, or practitioner executing the Terms of Service or a Commercial Order Form / Technical Trial), acting as Data Controller ("Controller" or "Data Controller"); and
DEXIMA TECH LLC, with registered office at 5830 E 2nd St, Ste 7000 #32263, Casper, Wyoming 82609, USA, acting as Data Processor ("Processor", "Company", or "Data Processor").
This DPA constitutes an integral and substantial part of the Terms of Service ("ToS") and the Global Privacy & Data Protection Policy ("Privacy Policy") of LoricAI.

ARTICLE 1 - PRIMACY OF TECHNICAL SPECIFICATIONS AND DEFINITIONS

1.1. Systematic Integration and Principle of Technical Impossibility. The Parties acknowledge that the performance of this DPA is founded upon the Zero-Knowledge and Confidential Computing technical architecture of LoricAI. Every obligation set forth in this DPA shall be interpreted and performed in accordance with the principle of technical inability of the Processor to access content in plaintext.

1.2. Binding Definitions. For the purposes of this DPA, the same definitions set forth in Section 1 of the Privacy Policy and Article 2 of the ToS apply:
"Blind Conduit": The technical and legal qualification of the Processor as a provider of encrypted computing and processing infrastructure, mathematically unable to view, decrypt, or know in plaintext the content of Payload Data.
"Zero-Knowledge Architecture and Confidential Computing (TEE)": The infrastructure in which Payload Data is protected by on-device encryption during transit and while at rest in storage, decryption keys (DEK/KEK) are managed separately via Google Cloud KMS (EU region) under a Key Release Policy constraint, and temporary decryption takes place exclusively inside the isolated volatile memory (RAM/VRAM) of AMD CPUs with SEV-SNP technology and NVIDIA RTX PRO 6000 Blackwell Server Edition / NVIDIA B200 GPUs hardware enclaves physically located in Finland (European Union).
"Payload Data": Any file, document, case file, text input (prompt), query, audio fragment, image, or content uploaded or generated by the Controller or its authorized users within the workspaces for processing, including any personal data, special categories of data (Art. 9 GDPR), or data subject to professional secrecy contained therein.

ARTICLE 2 - SUBJECT MATTER, DURATION, NATURE, AND DETAILS OF PROCESSING (ART. 28.3 GDPR)

2.1. Subject Matter and Purpose. The processing carried out by the Processor consists exclusively of making available the Confidential Computing infrastructure in Finland (EU), encrypted storage of case files (on Cloudflare R2 and isolated Qdrant vector database in the EU region), management of encrypted backups (on Backblaze B2 in the EU region), and local execution inside the hardware enclave of language models (e.g., Qwen 3.6 Flash Next) for the sole purpose of providing the LoricAI Service requested by the Controller. Any use of Payload Data for training or

improving artificial intelligence models (No AI Training) is strictly excluded.

2.2. Duration. This DPA takes effect upon activation of the account, Commercial Order Form, or Preliminary Technical Trial and remains in force until the complete Cryptographic Erasure of Payload Data pursuant to Article 11.

2.3. Categories of Data Subjects and Types of Personal Data. Because the Processor operates in Zero-Knowledge mode without plaintext access to Payload Data, the categories of Data Subjects and Personal Data depend exclusively on the documents uploaded by the Controller into the workspaces and may include, at the Controller's discretion: clients, patients, assisted persons, employees, suppliers, contractual counterparties, or third parties mentioned in the case files; identification, contact, contractual, financial, and judicial data, as well as special categories of personal data under Art. 9 of the GDPR (e.g., health or psychological data).

2.4. Enclave Processing Cycle and VRAM Scrubbing. To process a request from the Controller, Payload Data is decrypted exclusively inside the isolated volatile memory (RAM/VRAM) of the authorized hardware enclave for the time strictly necessary to complete inference (with a Time-To-Live of inactive post-inference buffers not exceeding 60 seconds). At the end of each request, the system forcibly executes cryptographic zeroization of GPU memory (cudaMemset(ptr, 0, size) and cudaDeviceReset()) and wipes allocated volatile memory (VRAM Scrubbing), guaranteeing the total absence of plaintext forensic residues.

ARTICLE 3 - OBLIGATIONS OF THE DATA PROCESSOR (ART. 28 GDPR)

3.1. Processing on Documented Instructions (Art. 28.3.a GDPR). The Processor processes Payload Data solely on documented instructions from the Controller - consisting of this DPA, the ToS, and the technical commands issued by the Controller via the Software interface - unless required to do so by Union or Member State law; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions.

3.2. Confidentiality and Hardware Barriers (Art. 28.3.b GDPR). The Processor ensures that all persons authorized to manage the infrastructure are bound by strict contractual or statutory confidentiality obligations. The Parties acknowledge that the confidentiality of Payload Data is primarily enforced by physical barriers in the silicon (AMD and NVIDIA Hardware Root of Trust) that technically prevent even the Processor's system administrators from accessing data in plaintext.

3.3. Technical and Organizational Security Measures (Art. 28.3.c and Art. 32 GDPR). The Processor implements and maintains state-of-the-art security measures as described in Sections 1, 2, and 3 of the Privacy Policy and in the technical verification documentation, including: (i) on-device encryption in transit (TLS 1.3) and at rest (AES-256-GCM); (ii) Confidential Computing isolation on AMD SEV-SNP CPUs and NVIDIA RTX PRO 6000 Blackwell / B200 GPUs in Finland; (iii) key separation on Google Cloud KMS (EU region) with a Key Release Policy bound to Remote Attestation; (iv) automatic end-of-session VRAM Scrubbing; (v) logical separation of environments via Blind Indexing (HMAC-SHA256).

3.4. Assistance with Data Subject Rights, DPIA, and Prior Consultation (Art. 28.3.e-f GDPR). Taking into account the Zero-Knowledge nature of the processing:
(a) Data Subject Requests (Arts. 15-22 GDPR): Because the Processor cannot decrypt Payload Data, the extraction, rectification, portability, and erasure of documents are natively guaranteed to the Controller in full autonomy via the platform functions (Art. 7.4 Privacy Policy). The Processor assists the Controller by providing all necessary technical attestations regarding the infrastructure;
(b) Data Protection Impact Assessment (DPIA under Art. 35 GDPR) and Prior Consultation (Art. 36

GDPR): The Processor assists the Controller in ensuring compliance with the obligations pursuant to Arts. 32-36 of the GDPR by making available all architectural documentation, AMD/NVIDIA Remote Attestation verification guides, and information on the cryptographic measures adopted.

ARTICLE 4 - OBLIGATIONS AND RESPONSIBILITIES OF THE DATA CONTROLLER (THE CUSTOMER)

4.1. Lawfulness of Processing and Data Ownership. The Controller represents and warrants that it has an appropriate legal basis pursuant to Arts. 6 and 9 of the GDPR for processing the personal data contained in the Payload Data and that it has provided Data Subjects with the required statutory privacy notices.

4.2. Human Oversight ("Human-in-the-Loop") and Credential Safeguarding. In accordance with Arts. 5.2, 6, and 12.1 of the ToS, the Controller is solely responsible for safeguarding the credentials of its authorized users and for the mandatory human verification of cited sources and generated Outputs prior to any professional or decision-making use.
ARTICLE 5 - EUROPEAN CONFINEMENT, TRANSFERS, AND "SCHREMS II" COMPLIANCE

5.1. Residency and Processing in the European Union. The processing of Payload Data (servers in Finland), encrypted storage (Cloudflare R2 and Qdrant in the EU region), encrypted backups (Backblaze B2 in the EU region), and the key management service (Google Cloud KMS in the EU region) are entirely confined within the European Union.

5.2. Standard Contractual Clauses (SCCs) and UK/Swiss Addenda. To the extent that the contractual relationship with the Processor (established in the United States) entails a transfer of personal data or metadata under Chapter V of the GDPR, the Standard Contractual Clauses (SCCs) approved by the European Commission by Implementing Decision (EU) 2021/914 (Module 2: Controller-to-Processor for processing carried out as Processor; Module 1: Controller-to-Controller for metadata processed as Controller), supplemented by the International Data Transfer Addendum (IDTA) for the United Kingdom and the FDPIC (IFPDT) integrative clauses for Switzerland, are incorporated by reference into this DPA.

5.3. Supplementary Technical Measures (Schrems II Compliance and EDPB Recommendations 01/2020). For the purposes of full compliance with the judgment of the Court of Justice of the EU C-311/18 (Schrems II) and EDPB Recommendations 01/2020, the Parties acknowledge that on-device encryption, confinement of compute servers in Finland (EU), key separation, and processing exclusively inside AMD and NVIDIA hardware enclaves (Data-in-use encryption) constitute effective supplementary technical measures that materially prevent anyone - including the Processor and any US or third-country governmental authority - from accessing Payload Data in plaintext.

ARTICLE 6 - SUB-PROCESSORS (ART. 28.2 AND 28.4 GDPR)

6.1. Authorized List of Sub-Processors. The Controller grants written authorization for the engagement of the Sub-Processors listed in Section 6 of the Privacy Policy, all bound to confinement within the European Union for the Payload infrastructure:
Verda (operated by DataCrunch Oy - Data Center in Finland, EU): Physical hosting of Confidential Computing servers (AMD SEV-SNP CPUs and NVIDIA RTX PRO 6000 Blackwell / NVIDIA B200 GPUs);
Google Ireland Limited (EU Region): Application infrastructure and cryptographic key management (Google Cloud KMS in the EU region) bound by a Key Release Policy;
Cloudflare, Inc. (EU Region): WAF/DDoS network security and encrypted object storage (Cloudflare R2 with EU Jurisdiction);
Backblaze, Inc. (EU Region): Storage of encrypted backups (Backblaze B2 in EU data centers);
AWS EMEA SARL (Region eu-central-1 Frankfurt, Germany): Delivery of transactional service e-mails (AWS SES).

6.2. Prior Notice of Changes and Right to Object/Withdraw (Art. 28.2 GDPR). The Processor shall inform the Controller in writing of any intended addition or replacement of the Sub-Processors listed above with a minimum prior notice of fifteen (15) days (or the longer period agreed in an Enterprise Agreement) prior to deployment. During such period, the Controller may object in writing on legitimate data protection grounds or withdraw from the Agreement without penalty by ordering immediate Cryptographic Erasure (T=0) before the change takes effect.

6.3. Obligations and Liability toward the Controller (Art. 28.4 GDPR). The Processor imposes on each Sub-Processor, by way of a written contract, data protection obligations no less stringent than those set out in this DPA and remains fully liable to the Controller for the performance of the Sub-Processors' obligations pursuant to Art. 28(4) of the GDPR.

ARTICLE 7 - PERSONAL DATA BREACH NOTIFICATION (DATA BREACH - ART. 33.2 GDPR)

7.1. Timing and Content of Notification. In the event of an established security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data processed on behalf of the Controller, the Processor shall notify the Controller without undue delay and, in any event, within forty-eight (48) hours (and never beyond the statutory maximum period set forth in Art. 4.5 of the Privacy Policy) after becoming aware of it, providing all technical information necessary to enable the Controller to assess the event and carry out any notifications to the Supervisory Authority (Art. 33 GDPR) and Data Subjects (Art. 34 GDPR).

7.2. Cryptographic and Hardware Protection of the Payload. The Parties acknowledge that, because Payload Data resides in storage exclusively in encrypted format and is processed only inside AMD/NVIDIA hardware enclaves, a perimeter incident that compromises neither the Controller's cryptographic key nor the integrity of the hardware enclave leaves Payload Data unintelligible within the meaning of Art. 34(3)(a) of the GDPR.

ARTICLE 8 - TECHNICAL VERIFICATION AND RIGHT OF AUDIT (ART. 28.3.H GDPR)

8.1. Continuous Cryptographic Verification and Documentary Audit. In accordance with Art. 28(3)(h) of the GDPR and the procedure published in the Technical Verification section of the official website, the Controller and its IT department have the right to verify the Processor's compliance at any time through:
(a) Real-Time Hardware Remote Attestation: direct verification of cryptographic reports signed by AMD SEV-SNP CPUs and NVIDIA RTX PRO 6000 / B200 GPUs via official AMD and NVIDIA verifiers, as well as verification of enclave code measurements ("Sealed Code") and key release policies on Google Cloud KMS;
(b) Compliance Documentation and Data Center Certifications: examination of the technical security documentation made available by the Processor and independent certification reports (e.g., ISO/IEC 27001, SOC 2 Type II) issued to the infrastructural Sub-Processors and European data centers referred to in Article 6.1;
(c) Written Information Requests: submission of security audit questionnaires to the Processor's Compliance Department (privacy@loricai.io), to which the Processor shall provide documented responses.

8.2. Physical Security of Data Centers. In order to preserve the physical integrity of multi-tenant infrastructures and the cryptographic security of environments, audits are conducted via the cryptographic and documentary tools set forth in Art. 8.1, excluding direct physical access by customers inside data center server rooms.

ARTICLE 9 - THE SEAL CLAUSE AND GOVERNMENT REQUESTS

9.1. Technical Impossibility of Plaintext Production. The Controller and the Processor acknowledge that the LoricAI architecture mathematically prevents the Processor from decrypting Payload Data outside the sessions activated by the Controller inside the hardware enclave. Therefore, the

Processor is technically unable to comply with third-party or governmental authority requests aimed at extracting plaintext content. Upon receipt of a judicial order relating to metadata of the Controller's account, the Processor undertakes to verify its lawfulness, challenge any non-EU request conflicting with Art. 48 of the GDPR, and inform the Controller in advance, unless prohibited by mandatory criminal law.

ARTICLE 10 - LIABILITY AND REFERENCE TO THE TERMS OF SERVICE

10.1. Alignment with Contractual Liability Cap (Art. 7 ToS). The total aggregate liability of the Parties arising out of this DPA is governed by the provisions and caps established in Article 7 (Limitation of Liability and Indemnification) of the Terms of Service (ToS) (or the higher cap specifically agreed in writing in the Enterprise Agreement executed with the Controller):
(1) for Customers with an active contract, the ordinary cap is equal to the total amount of fees actually paid by the Controller during the preceding twelve (12) months, increased to twice (2x) the fees paid during the preceding twelve (12) months in the event of an established Data Breach attributable to a breach of the Processor's security obligations;
(2) for Users in a free trial phase or with expenditure below EUR 100.00 during the preceding twelve (12) months, the cap is equal to EUR 100.00 (or $100.00 USD). Mandatory provisions of applicable law, including Art. 82 of the GDPR and non-derogable clauses of the SCCs, remain unaffected in all cases.

10.2. Exclusion of Liability on Outputs and Controller Indemnification. In accordance with Arts. 5.2, 7.2, and 7.3 of the ToS, because language models (e.g., Qwen 3.6 Flash Next) are executed inside a blind enclave without the possibility of human review by the Processor, the Controller retains sole responsibility for the lawfulness of uploaded Payload Data and for the professional validation of generated Outputs, indemnifying and holding harmless the Processor from third-party claims arising from breaches of obligations incumbent upon the Controller under the GDPR or the EU AI Act.

ARTICLE 11 - CONTRACT TERMINATION, RETURN, AND CRYPTOGRAPHIC ERASURE (ART. 28.3.G GDPR)

11.1. Data Export and Return. In accordance with Art. 28(3)(g) of the GDPR, Art. 7.4 of the Privacy Policy, and Art.
12.2 of the ToS, throughout the term of the Agreement and until the execution of Cryptographic Erasure, the Controller has the full technical ability to autonomously export and download in plaintext all of its Payload Data and documents via the interface protected by its key.

11.2. Cryptographic Erasure (T=0 or T=30) and Backup Rotation. Upon termination of the contractual relationship or upon instruction from the Controller, the Processor executes the deletion protocol established in Section 7 of the Privacy Policy:
(a) Immediate Deletion (T=0): upon explicit request of the Controller (as well as automatically at the end of a Preliminary Technical Trial not followed by a contract), the Processor immediately deletes the documents from active storage (Cloudflare R2 and Qdrant) and executes the simultaneous irreversible destruction of the Controller's dedicated cryptographic key (DEK/KEK) on Google Cloud KMS (Cryptographic Shredding);
(b) Standard Procedure with Grace Period (T=0 -> T=30): unless immediate destruction is requested, upon ordinary account closure access tokens are revoked at T=0, leaving the Controller thirty (30) days to complete the export of its archives, upon expiration of which (T=30) the system executes the permanent destruction of the cryptographic key on Google Cloud KMS;
(c) Backups (Backblaze B2): from the exact moment of destruction of the key (at T=0 or T=30), any residual encrypted block in the immutable backups on Backblaze B2 instantaneously becomes mathematically indecipherable entropic waste and reaches permanent physical overwriting at the end of the thirty-five (35) day rotation cycle.

ARTICLE 12 - GOVERNING LAW, JURISDICTION, AND EU POINT OF CONTACT

12.1. Governing Law and Exclusive Jurisdiction. This DPA follows the exact jurisdictional segmentation established by Article 8 of the Terms of Service (ToS) and Section 10 of the Privacy Policy:
for Controllers established in the European Union, the European Economic Area (EEA), the United Kingdom, and Switzerland, this DPA is governed by the law of the Republic of Ireland and any dispute is subject to the exclusive jurisdiction of the Courts of Dublin (Republic of Ireland), without prejudice to the non-derogable rights of Data Subjects and the powers of Supervisory Authorities under Arts. 77, 78, and 79 of the GDPR;
for Controllers established in the United States and in Non-European jurisdictions (excluding the EEA, UK, and Switzerland), this DPA is governed by the law of the State of Wyoming (USA) with binding arbitration before the American Arbitration Association (AAA) in Casper, Wyoming.

12.2. Privacy Contact and EU Representative (Art. 27 GDPR). For any communication relating to this DPA, the exercise of audit rights, or notification of processing instructions, the Processor's official point of contact is: DEXIMA TECH LLC - Data Protection & Legal Compliance Department, E-mail: privacy@loricai.io.