

Xmore AI – Lithos Privacy Notice

Effective date: August 1, 2025

Last updated: August 1, 2025

This Privacy Notice explains how **Xmore AI** (“**Xmore**”, “**we**”, “**our**”, or “**us**”) processes personal data in connection with the **Lithos** security-automation platform and related services. It also describes your choices and rights. If you use Lithos under a contract with an organization, that organization is the **Controller** of **Customer Data** and Xmore acts as a **Processor/Service Provider**. For our public website, sales, and support activities, Xmore is the Controller of **Service Data**.

Summary: Lithos is typically deployed in a customer-controlled environment (on-premises or private cloud). Customer Data remains in that environment by default. We do not use Customer Data to train foundation models unless the customer opts in by contract.

1) Scope

This Notice applies to:

- **Product:** Lithos platform, agentic automation services, adapters/SDKs, and managed cloud instances.
- **Support & Services:** Customer success, technical support, professional services, and incident response.
- **Website & Sales:** xmore.ai and associated marketing channels (collectively, **Service Data**).

This Notice does **not** apply to third-party tools integrated with Lithos; their privacy practices are governed by their own notices.

2) Key Roles & Definitions

- **Customer Data:** Data ingested or generated within a customer’s tenancy (e.g., security logs, alerts, artifacts, tickets, configuration metadata, user identifiers). The Customer is the **Controller**; Xmore is the **Processor/Service Provider**.
- **Service Data:** Business contact details, telemetry, billing, support records, and website analytics that Xmore processes as **Controller**.
- **Model/AI Features:** Planner–executor agents, retrieval-augmented generation (RAG), and automation. By default, models operate on Customer Data within the customer’s environment; training/tuning is **opt-in** and tenant-scoped.

3) What We Collect

A. Customer Data (Processor)

Collected under the Customer's instructions and configuration:

- **Security inputs:** Logs/events (e.g., SIEM, EDR, DNS, IAM), alerts, NetFlow, cases/tickets, and indicators.
- **Artifacts (optional):** PCAPs, binaries, documents for analysis (subject to customer policy).
- **Operational metadata:** Workflow definitions, approval records, simulation results, and audit trails.
- **User data:** Work email, role, group/RBAC assignments, and in-product actions.

B. Service Data (Controller)

- **Account & billing:** Names, business contact details, organization, payment details (handled by payment processors), and subscription info.
- **Telemetry:** Product usage metrics and health signals (pseudonymized where feasible), crash reports.
- **Website data:** Cookies/identifiers, IP address, device/browser info, pages viewed, and referral sources.
- **Support:** Messages, tickets, call recordings (with notice), and related attachments.

We do **not** intentionally collect sensitive personal data unless necessary for support and only with safeguards.

4) Sources of Data

- Directly from users and administrators.
- From integrated systems/tools (per customer configuration and contracts).
- From our service providers (e.g., payment, hosting, analytics) and publicly available sources for business contact enrichment where permitted by law.

5) Purposes & Legal Bases

A. For Customer Data (Processor)

We process Customer Data **solely** to provide, secure, and support Lithos under the Customer's instructions and our agreement, including:

- Ingesting, analyzing, correlating, and automating security workflows.
- Generating recommendations and executing approved actions (with auditability).
- Providing support, maintenance, backups, high availability, and security monitoring for managed offerings.

B. For Service Data (Controller)

- **Provide the services** (contract performance).
- **Security & fraud prevention** (legitimate interests/legal obligation).
- **Improve the services** and develop features (legitimate interests; privacy-preserving telemetry where feasible).
- **Marketing communications** to business contacts (with consent where required, opt-out anytime).

Where required (e.g., in the EEA/UK), we rely on appropriate legal bases including consent, contract, legitimate interests, and compliance with legal obligations.

6) AI/Model Practices

- **Data locality:** AI features operate within the tenant scope; prompts/inputs are restricted to the customer's configured data sources.
 - **No default training:** We do **not** use Customer Data to train foundation models. Tenant-level fine-tuning or caching is **opt-in**, isolated to that tenant, and controlled by contract and configuration.
 - **Explainability & audit:** Outputs include evidence references and are logged with metadata for traceability.
 - **Human-in-the-loop:** Automated actions require approval according to customer policies unless the Customer expressly enables auto-execute.
-

7) Sharing & Disclosures

We share personal data only as described below:

- **Sub-processors (Processor context):** Infrastructure and platform providers necessary to deliver managed cloud (e.g., **Microsoft Azure** services). A current list of sub-processors is available upon request and included in the DPA.
- **Service Providers (Controller context):** Payment processors, CRM, support tools, analytics, and security vendors under contract and confidentiality.
- **Legal & safety:** To comply with law, enforce agreements, protect rights, or respond to lawful requests. We scrutinize requests and notify customers where permitted.

- **Business transfers:** In connection with a merger, financing, acquisition, or dissolution, subject to this Notice and applicable law.

We do **not** sell personal information, and we do **not** share it for cross-context behavioral advertising.

8) International Transfers

For managed cloud and Service Data, we may transfer personal data internationally. We use appropriate safeguards such as **Standard Contractual Clauses (SCCs)** and apply regional data-location commitments where agreed. On-prem deployments keep Customer Data within the customer's environment.

9) Retention

- **Customer Data:** Retained according to the customer's configuration and contract (typical defaults: operational logs ~90 days; transient processing data ~14 days). Backups follow rolling schedules and secure deletion practices.
 - **Service Data:** Retained for as long as needed to fulfill the purposes described, then deleted or anonymized; specific periods are available upon request.
-

10) Security

We employ administrative, technical, and physical safeguards, including encryption in transit/at rest, role-based access control, key management, network isolation, vulnerability management, logging, and regular testing. For managed offerings, we maintain business continuity and incident response plans and will notify customers of security incidents as required by contract and law.

11) Your Rights & Choices

Depending on your location, you may have rights to access, correct, delete, port, restrict, or object to certain processing of your personal data. For Customer Data, please contact your organization's administrator; for Service Data, contact Xmore using the information below. You can opt out of marketing communications at any time.

If your jurisdiction recognizes **Global Privacy Control (GPC)** or provides specific rights (e.g., under the **CCPA/CPRA**, **GDPR/UK GDPR**, **VCDPA**, etc.), we honor those rights in accordance with applicable law.

12) Children's Privacy

Lithos is a business product not intended for children. We do not knowingly collect personal data from children.

13) Cookies & Similar Technologies (Website/Console)

We use essential cookies for authentication and security, and (where permitted) analytics to improve the service. You may control non-essential cookies via our cookie banner and browser settings.

14) Controller, Processor & Contact Details

- **Controller for Service Data:** Xmore AI Inc.
 - **Processor for Customer Data:** Xmore AI acts under the Customer's instructions pursuant to the Data Processing Addendum (DPA).
 - **Contact:** privacy@xmore.ai.
-

15) Changes to this Notice

We may update this Notice to reflect changes in our practices or legal requirements. If changes are material, we will provide notice (e.g., in-product message or email) and indicate the latest revision date above.

16) Region-Specific Disclosures

California (CPRA)

We do not sell or share personal information as defined by the CPRA. We disclose personal information to service providers and contractors for business purposes described above. California residents may exercise CPRA rights as described in **Section 11**. If we operate a consumer-facing website, we honor **Do Not Sell or Share** signals and **GPC** where applicable.

EEA/UK (GDPR/UK GDPR)

For Service Data, our legal bases include contract, legitimate interests, consent (where required), and legal obligation. You may lodge a complaint with your local supervisory authority. For Customer Data, your organization is the Controller; please contact them to exercise GDPR rights.

17) Data Processing Addendum (DPA)

For enterprise customers, our DPA forms part of the Master Services Agreement and includes: subject matter and duration, nature and purpose of processing, types of personal data, categories of data subjects, confidentiality, security measures, sub-processor controls, breach notification, assistance with data subject requests, audits, and international transfer mechanisms (e.g., SCCs). A copy is available upon request.

Annex A – Data Categories & Example Mapping

- **Identifiers:** Work email, user ID (Service Data & Customer Data).
- **Professional/role info:** Team, RBAC role (Customer Data).
- **Network data:** IP addresses, device identifiers (Service Data; Customer Data if present in logs).
- **Security events & artifacts:** Alerts, hashes, indicators (Customer Data).
- **Telemetry:** Performance metrics, feature usage (Service Data; pseudonymized where feasible).

Questions? Contact us at privacy@xmore.ai.

Annex A – Illustrative Sub-Processors (Managed Cloud)

- **Microsoft Azure** (compute, storage, networking, Key Vault).
- **Azure Monitor/Log Analytics** (telemetry/metrics).
- **[Support ticketing/CRM provider]**.
- **[Payments processor]**.

The current, authoritative list is maintained at: [\[link to sub-processor page\]](#) and is incorporated into the DPA.