Privacy Policy

This Website Privacy Policy ("Privacy Policy") describes the privacy practices of LanceDB Systems, Inc. and its subsidiaries and affiliates (collectively, "LanceDB," "we," "us," or "our"). This Privacy Policy explains how we collect, use, disclose, secure, and otherwise process personal information from individuals in connection with our website and any other website that we own or control and which posts or links to this Privacy Policy (collectively, the "Websites"), and the rights and choices available to individuals with respect to their information.

This Privacy Policy does not govern how we may process personal information on behalf of our enterprise customers as part of the LanceDB Services. We process such personal data only as instructed by our customers and in accordance with a data processing agreement between our customers and us.

We use your data to provide and improve our Services. By using our Services, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, the terms used in this Privacy Policy have the same meanings as in our Terms and Conditions.

Our Terms and Conditions ("Terms") govern all use of our Services and, together with the Privacy Policy, constitute your agreement with us ("agreement").

Information Collected

From Whom We Collect Personal Information

- **Customers**: Individuals or authorized representatives of entities who register for, access, or use our Services under contractual agreements.
- **Website Visitors**: Individuals who interact with our Websites and voluntarily provide contact information (e.g., via forms, subscriptions, or cookie consent mechanisms).
- **Social Media Users**: Individuals engaging with our official social media profiles, whose interactions (e.g., comments, direct messages) are processed in accordance with platform-specific terms and our legitimate business interests.
- **Participants in LanceDB events, conferences**: Individuals or authorized representatives of entities who register for LanceDB events or conferences.

What Personal Information We Collect

We collect and process the following categories of personal data, limited to what is necessary for stated purposes:

- **Business contact data**: Name, email, phone number, IP address, third-party account identifiers.

- **Employment information**: Employer name, job title, business address.
- **Location data**: Approximate location derived from IP addresses (not precise GPS coordinates).
- **Usage data**: Device information, browser type, cookies, usage patterns, error logs.
- **Marketing data**: Opt-in/opt-out status, communication channel selections.
- **Third-party integrations**: If logging in via services like Google or GitHub, we may collect user ID and public profile data.

Privacy Policy Updates & Notifications

1. Public Communication of Policy

This Privacy Policy is made permanently accessible to all users and stakeholders through our official website, mobile application interfaces, and dedicated legal documentation portals. Transparency is foundational to our data governance practices; accordingly, this policy is maintained in machine-readable and human-readable formats to ensure universal accessibility. Historical versions of this policy are archived and available upon written request to support@lancedb.com for audit or compliance verification purposes.

2. Advance Notification of Material Changes

We commit to providing users with prior written notice of no less than thirty (30) calendar days before implementing any modifications to this Privacy Policy that materially affect (i) the categories of personal data collected, (ii) the purposes or legal bases for processing, or (iii) third-party data-sharing practices. Such notifications will:

- Clearly articulate the nature, rationale, and effective date of changes.
- Highlight user rights and options to consent, object, or terminate service under revised terms.
- Comply with jurisdictional requirements (e.g., GDPR Article 13, CCPA Section 1798.135).

3. Multi-Channel Communication of Updates

Modifications to this Privacy Policy will be disseminated through the following primary channels, e.g. email, in-product alerts, or website announcements. We will notify users at least 30 days before implementing material changes (e.g., data use purposes, third-party sharing).

4. Legal Effectiveness of Modifications

No modification to this Privacy Policy shall be binding unless executed in writing by authorized corporate officers and published through the channels above. Changes become effective

immediately upon posting unless otherwise stated (e.g., “Effective: [Date]”). Continued use of our services, platforms, or products after the effective date constitutes:

- Unconditional acceptance of revised terms.
- Waiver of objections to enforceability, except where prohibited by law.

For material changes requiring explicit consent under applicable regulations (e.g., GDPR Article 7), users will be required to reaffirm acceptance through opt-in mechanisms prior to continued access.

Legal Basis for Processing Personal Data

We process personal data with a **lawful or legitimate basis** under **GDPR**, such as:

- **Consent**: When you voluntarily provide data (e.g., marketing preferences).
- **Contractual Necessity:** To fulfill services you request (e.g., account creation).
- **Legitimate Interests**: For purposes like improving our Services, fraud prevention, and business operations.
    - *Example*: We process business contact data (name, email) under legitimate interests to communicate with potential customers.
- **Legal Obligation**: To comply with laws (e.g., tax reporting).

For **HIPAA-covered data**, we only process **Protected Health Information (PHI)** in compliance with **Business Associate Agreements (BAAs)**.

Data Subject Rights & Consent Withdrawal

- Users have the right to **access, correct, delete** (subject to legal obligations)**, transfer their data**, or **restrict processing** under certain conditions.
- **Data Portability** (receive a copy of your data in a structured format).
- Object to processing based on legitimate interests.
- **Consent can be withdrawn at any time**, with an option to request data erasure.
- **Denied requests** will include an explanation and options for appeal.
- Users can **review, correct, amend, or append their data** directly.

To exercise these rights, contact us at privacy@lancedb.com. We respond to requests within 30 days and provide explanations for denied requests. If unsatisfied, you may appeal to your local data protection authority.

If you exclude specific data types from LanceDB, those data will not be indexed, limiting the system’s ability to analyze or retrieve insights from the excluded content. Should you later withdraw permissions for previously shared data, all associated indices and metadata will be permanently deleted from LanceDB. This removal degrades search accuracy and answer comprehensiveness, as historical patterns and semantic connections are lost. To minimize disruption, we recommend selective data sharing (e.g., excluding sensitive fields via metadata)

or using synthetic data, though reindexing will be required to reflect updates. By design, this architecture ensures compliance and transparency but balances privacy with functionality: excluding or removing data proportionally reduces the system's contextual intelligence.

Third-Party Data Sharing & Sub-Processors

- The use of **third-party processors** is disclosed in this policy.
- **Written permission** is required before engaging new sub-processors.
- **BAAs (HIPAA) & DPAs (GDPR)** must be in place for all third-party processors.
- **Explicit user consent is required** before sharing personal data with third parties.

Sub-Processors:
We use third-party sub-processors to deliver our Services. A current list of sub-processors (e.g., cloud providers, analytics tools) can be provided per request. If we engage a new third-party subprocessor that requires access to your personal data, we will notify you of this change 30 days via email before adding new sub-processors. You will have the opportunity to review the new subprocessor's privacy practices before the changes take effect. All sub-processors are bound by GDPR-compliant Data Processing Agreements (DPAs).

As a data controller, we ensure all third-party processors comply with contractual obligations under GDPR Article 28. Data processing agreements are reviewed annually for alignment with evolving regulations.

Security & Safeguards for Personal Data

In the event of a data breach involving personal data, we will:

- Notify authorities within 72 hours of discovery.
- Inform affected users without undue delay if the breach poses a high risk to their rights.

We implement **technical, administrative, and physical safeguards** to protect personal data:

- **Administrative safeguards**: Defined policies to limit unauthorized access.
- **Technical safeguards**: Encryption, access controls, and secure authentication.
- **Physical safeguards**: Restricted access to facilities storing personal data.
- **Breach notification procedures** comply with **HIPAA & GDPR**.

Data Retention & Deletion Policy

Data Type	Retention Period
Marketing Data	2 years after last interaction
Customer Account Data	Until deletion request or 5 years of inactivity
Payment Data	7 years (for tax compliance)
Support Tickets	3 years after resolution
HIPAA(PHI) Data	6 years after last interaction

Data is anonymized or deleted when no longer necessary for its original purpose.

Privacy Event Logging & Compliance Tracking

All data privacy requests are logged and tracked in a secure system. Changes to request-handling procedures are published in our Policy Changelog and communicated via email notifications.

- A **privacy event log** is maintained to track policy updates, user requests, and compliance actions.
- Privacy requests such as **data deletion, access, and corrections** are documented for audit purposes.
- **Compliance with HIPAA & GDPR** is continuously monitored.

EU Data Transfers & International Compliance

While we do not currently have an appointed representative established in the European Union as described in Article 27 of the GDPR, we have designated a qualified internal team member to act as the primary point of contact for EU data subjects and supervisory authorities. This individual is authorized to respond to inquiries and facilitate cooperation with EU data protection authorities as necessary. This setup reflects our current organizational structure and ensures we uphold our data protection obligations under the GDPR.

Children’s Privacy

Our Services are not directed to individuals under 16 (or 13 in regions where local law permits). If we inadvertently collect data from minors, contact us at dpo@lancedb.com immediately for deletion.

Sensitive Personal Information

We request that you **do not submit sensitive personal information**, such as:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs.
- Health or genetic data (unless required for service provision under HIPAA).
- Criminal background or trade union membership.

We obtain granular consent for distinct processing activities (e.g., separate opt-ins for email newsletters and SMS alerts). You may modify consent preferences at any time via your account dashboard or by contacting us.

Roles and Responsibilities

Our Data Protection Officer (DPO) oversees compliance with global privacy regulations. Internal privacy audits are conducted quarterly, and employees undergo mandatory annual privacy training.

Automated Decisions & Profiling

We do not use automated decision-making (including profiling) that produces legal effects or significantly impacts users. If this changes, we will notify you and provide opt-out options.

Contact for Privacy Inquiries

For GDPR-specific inquiries, contact our Data Protection Officer (DPO) or EU Representative:

Email: dpo@lancedb.com
