

Privacy Policy

Last Updated: Sep 16, 2025

Effective Date: July 31, 2025

1. Data Categories & Processing Standards

A. Permissions & Data Mapping

1. Camera Access (NSCameraUsageDescription)

- Data Collected: Live image streams
- Processing Purpose: Capture photos and videos for Private Album
- Storage Location: Device local storage
- Retention Period: Until user deletion

2. Contacts Access (NSContactsUsageDescription)

- Data Collected: Contact names and phone numbers
- Processing Purpose: Duplicate detection and management
- Storage Location: Temporary device memory
- Retention Period: Purged after processing

3. Face ID Authentication (NSFaceIDUsageDescription)

- Data Collected: Biometric template (mathematical representation)
- Processing Purpose: Identity verification for Private Space access
- Storage Location: Secure Enclave
- Retention Period: Never leaves device

4. Photo Library Access (NSPhotoLibraryUsageDescription)

- Data Collected: Media file metadata (date, size, format)
- Processing Purpose: Image/video similarity analysis
- Storage Location: On-device Neural Engine
- Retention Period: Until media deletion

5. Microphone Access

- Data Collected: Audio recordings
- Processing Purpose: Video capture for Private Album
- Storage Location: Device local storage
- Retention Period: While associated video exists

6. Advertising Tracking (NSUserTrackingUsageDescription)

- Data Collected: Device Identifier for Advertisers (IDFA)
- Processing Purpose: Deliver personalized advertisements within our app and measure campaign effectiveness across third-party platforms (e.g., Google Ads).
- User Control: Managed entirely through the system-level App Tracking Transparency prompt. Permission can be revoked at any time in device Settings > Privacy & Security > Tracking.
- Data Linkage: Not linked to other personal data or identities for tracking purposes.

B. Third-Party SDK Compliance

- OpenCV 4.5+
 - Processing type: On-device edge computing
 - Data flow: Zero network transmission
 - Privacy compliance: Apple Required Reason API certified
 - User control: Disable in Settings > Privacy Center

2. Data Security & Encryption Standards

A. Technical Safeguards

- Limited Photo Access: Prevents full-library scanning (iOS14+)
- AES-256 Encryption: For Private Album contents

B. International Data Transfer Compliance

- GDPR Protection: EU Standard Contractual Clauses (SCCs)

3. Policy Updates & Dispute Resolution

- Governing Law:
 - EU: Irish law (Apple HQ jurisdiction)
 - Global: Singapore law
- Dispute Resolution:
 - Binding arbitration via AAA/ICDR
 - Class action waiver

4. Contact Information

- Support: apps_support@letaotech.com
- Privacy Inquiries: Use subject "Privacy Request"