ALRM Privacy Policy Effective Date: January 1, 2026 Last Updated: [July 7, 2026]

KEY PRIVACY PRINCIPLES

● Privacy-First Design: All sound detection happens on your device. ● No Recording: We do not record or store audio files. ● No Selling: We do not sell your personal information. ● No Biometrics: ALRM identifies sound classes (e.g., sirens), not individual voices or biometric "voiceprints." ● Children: We do not knowingly collect personal information from children under 13.

---

1. Information We Collect

A. Audio & AI Processing

● Real-Time Only: Audio is processed in real-time on your device and immediately discarded. Audio data never leaves your device. ● Metadata Logging: When a sound detection event occurs, we log the sound classification (e.g., "fire alarm"), confidence score, and timestamp. These logs are associated with your account if you are signed in, or stored anonymously if you are not. They are never linked to audio recordings, biometric data, or your physical location beyond the zone in which the detection occurred. ● No Conversations: We do not listen to, record, or upload your conversations or ambient audio.

B. Location & Zones

● Geofencing: We use GPS to determine when you enter or exit an ALRM Zone. ● No Tracking: We do not maintain a continuous history of your movements. We record zone entry and exit events only. ● Zone Identity: We record which zone triggered a detection event, but not your precise coordinates within that zone.

C. Account & Device Data

● Optional Accounts: You may provide a name and email address for account management. This information is stored securely and used only to manage your account and communicate with you about the service. ● Technical Data: We collect device models and OS versions to ensure app compatibility and diagnose technical issues.

D. Children Under 13 (COPPA)

ALRM is not directed to children under the age of 13. We do not knowingly collect personal information from children under 13. If ALRM is deployed in a school or educational environment, it operates using geofence-only zone detection — no account creation or personal data

collection is required to receive alerts within a zone. If we discover that we have inadvertently collected personal information from a child under 13, we will delete it promptly. Parents or guardians who believe their child has provided personal information to ALRM may contact us at support@getalrm.com to request deletion.

---

2. How We Use & Share Information

● Service Delivery: To activate detection and send alerts when you are in a zone. ● Improvement: We use aggregated, de-identified metadata to improve our AI detection accuracy. Individual detection logs are never sold or shared with third parties for commercial purposes. ● Business Zones: If you enter a Business Zone, the zone operator may see anonymized usage counts (e.g., number of app activations within the zone during a given period). Zone operators never receive your personal identity, account information, precise location, or individual detection logs. ● Service Providers: We share data with third-party service providers only as necessary to operate the service. Current categories of service providers include: — Cloud infrastructure (e.g., AWS or Google Cloud) for secure data hosting — Crash reporting and diagnostics tools for app stability — Payment processors for Business Zone billing All service providers are contractually barred from using your data for their own purposes and are required to maintain appropriate security standards. ● Legal Requirements: We may disclose your information if required by law, court order, or government authority, or to protect the rights, property, or safety of ALRM, our users, or the public.

---

3. Data Retention & Security

Data Type Retention Period

Account Info Until account deletion + 30 days Alert Logs 12 months from the date of the detection event (sound classification, confidence score, timestamp, zone ID; not linked to audio) Crash & Diagnostic Logs 90 days Zone Entry/Exit Events 12 months Payment Records 7 years (required by tax/accounting law)

● Encryption: We use TLS/SSL encryption for all data in transit and AES-256 encryption at rest for all stored data. ● Access Controls: Access to personal data is restricted to ALRM personnel and systems that require it to operate the service. We do not grant zone operators or venue partners access to individual user data. ● Data Breach Notification: In the event of a data breach that affects your personal information, we will notify affected users as required by applicable law. Under Maine law (10 M.R.S. § 1347), we are required to notify you as expediently as possible and without unreasonable delay, no later than 30 days after we discover the breach. We will

notify you by email to the address associated with your account, and will post a notice on our website at getalrm.com.

---

4. Your Global Privacy Rights

U.S. State Rights (California, Virginia, Colorado, and others)

Residents of states with comprehensive privacy laws have the right to:

● Request a copy of the personal data we have collected about you. ● Request correction of inaccurate personal data. ● Request the deletion of your personal information, subject to certain exceptions. ● Opt out of the "sale" or "sharing" of your data for targeted advertising (ALRM does not sell or share data for these purposes). ● Non-discrimination: We will not discriminate against you for exercising any of these rights.

To exercise these rights, contact us at support@getalrm.com. We will respond within 45 days. We may need to verify your identity before fulfilling your request.

European Users (GDPR)

If you are located in the European Union or European Economic Area, you have additional rights under the General Data Protection Regulation (GDPR), including:

● The right to access, correct, or delete your personal data. ● The right to data portability. ● The right to restrict or object to processing. ● The right to lodge a complaint with your local supervisory authority.

Legal Basis for Processing: We process your personal data on the following legal bases: (a) performance of our contract with you (providing the ALRM service); (b) our legitimate interests in improving the service and ensuring security; and (c) compliance with legal obligations.

International Data Transfers: ALRM is based in the United States. If you are accessing the service from the EU/EEA, your data may be transferred to and processed in the United States. We rely on Standard Contractual Clauses (SCCs) approved by the European Commission as the legal mechanism for such transfers. Copies of the applicable SCCs are available upon request at support@getalrm.com.

---

5. Changes to This Policy

We may update this Privacy Policy from time to time. When we make material changes, we will update the "Last Updated" date at the top of this document and, where appropriate, notify you by email or in-app notification. Your continued use of ALRM after any changes constitutes acceptance of the updated policy.

---

6. Contact Us

To exercise your rights, ask a privacy question, or submit a data deletion request:

Email: support@getalrm.com Address: ALRM, LLC, Privacy Team, Portland, Maine, USA

For urgent data breach or security concerns, please include "URGENT PRIVACY" in your subject line.