



PRIVACY POLICY

Revised: February 3, 2026

Zion Call Management, LLC (doing business as “Zion Call Management” and “Storage Unit Management,” and referred to herein as “Zion,” “we,” “our,” or “us”) respects your privacy and is committed to protecting personal information. This Privacy Policy explains how we collect, use, disclose, store, transfer, and safeguard personal information when you use our Services, including through our website (www.zioncallmgmt.com), integrations with your management software, or interactions with our agents (live or AI). This Policy applies to information from you (our clients, e.g., storage facility owners or managers in the United States or Canada) and end-users (e.g., your tenants or customers).

We operate primarily in the United States and Canada, and this Policy is designed to comply with applicable privacy laws in these jurisdictions, including but not limited to the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), other U.S. state privacy laws (such as those in Virginia, Colorado, Connecticut, Utah, and others as they come into effect), and Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) and relevant provincial privacy laws (e.g., British Columbia’s Personal Information Protection Act or Quebec’s Act Respecting the Protection of Personal Information in the Private Sector). If you are located outside the U.S. or Canada, your use of the Services may involve the transfer of your personal information to these countries, and by using the Services, you consent to such transfers and processing in accordance with this Policy.

By using the Services, you consent to the practices described in this Policy. We may update this Policy from time to time; changes will be posted here with a revised effective date. Continued use of the Services after changes constitutes your acceptance. If changes are material, we may provide additional notice (e.g., via email).

1. Information We Collect. We collect personal information that identifies, relates to, describes, or could reasonably be linked to an individual (“Personal Information”). The categories we collect include:

- a. **Identifiers:** Name, postal address, email address, phone number, unique identifiers (e.g., account ID, IP address).
- b. **Customer Records:** Payment information (e.g., credit card details, bank account info via ACH), rental or lease details, gate codes.
- c. **Commercial Information:** Transaction history, products/services purchased or considered (e.g., storage unit rentals, tenant protection plans).
- d. **Internet/Network Activity:** Browsing history on our site, device information, logs, cookies, and analytics data.

- e. **Geolocation Data:** Approximate location (e.g., from IP address or facility details), but not precise geolocation unless necessary for Services.
- f. **Audio/Visual Data:** Call or chat recordings for quality assurance and training.
- g. **Sensitive Personal Information:** Limited collection, such as payment details (processed securely) or, if provided, government IDs for verification; we do not collect health, racial, or biometric data unless incidentally in communications.
- h. **Inferences:** Derived from the above, such as preferences or behavior patterns to improve Services.

We do not knowingly collect Personal Information from children under 13 (or under 16 in certain jurisdictions); if we learn we have, we will delete it.

2. Sources of Information:

- a. **Directly from You or End-Users:** Via registration, interactions (e.g., calls, chats, payments), or submissions.
- b. **Automatically:** Through cookies, pixels, logs, and similar technologies on our site or Services.
- c. **From Clients:** Tenant data shared via management software integrations or as our authorized representatives.
- d. **From Third Parties:** Service providers (e.g., Talkdesk for AI/phone systems), payment processors, or public sources.

3. How We Use Information.

We use Personal Information for the following business or commercial purposes:

- a. To provide, maintain, and improve the Services (e.g., processing payments, handling rentals, sending past due notices, AI interactions).
- b. For customer support, integrations, and analytics.
- c. To communicate with you (e.g., Service updates, billing, marketing with consent).
- d. For security, fraud prevention, and legal compliance (e.g., auditing, dispute resolution).
- e. To create de-identified or aggregated data for internal insights or sharing (with consent where required).
- f. As otherwise described at collection or with your consent.

Under applicable laws (e.g., CCPA/CPRA), these uses do not constitute a “sale” or “sharing” of Personal Information for targeted advertising, but we may disclose for operational purposes as described below.

4. How We Disclose or Share Information. We do not sell Personal Information. We may disclose it to:

- a. **Service Providers and Contractors:** Third parties performing services for us, such as AI/phone platforms (e.g., Talkdesk), payment processors, IT support, or analytics providers. These include contractors in foreign countries (outside of U.S. and Canada) who assist with operations (e.g., call handling, data processing). We require them to use data only for our purposes and protect it via contracts with appropriate safeguards.
- b. **Affiliates and Business Partners:** For Service delivery, such as management software providers or insurers for tenant protection plans.
- c. **Your Authorized Parties:** As your representatives, we may share with your tenants, vendors, or others as needed (e.g., confirming rentals).
- d. **Legal and Safety Reasons:** To comply with laws, respond to legal processes (e.g., subpoenas), protect rights/safety, or prevent fraud.
- e. **Business Transfers:** In mergers, acquisitions, or asset sales, subject to confidentiality. Disclosures are limited to the categories above and bound by contracts ensuring compliance with privacy laws.

5. International Data Transfers. Personal Information may be transferred to, stored, and processed in, but not limited to, the United States, Canada, India, Philipines, Guatemala, and Belize. For transfers from Canada, we ensure compliance with PIPEDA by using safeguards like standard contractual clauses or relying on adequacy decisions where applicable. For transfers to Guatemala and Belize (for example, non-adequate jurisdictions under some frameworks), we implement appropriate measures, such as data processing agreements requiring equivalent protections. By using the Services, you consent to these transfers. If you are in a jurisdiction with stricter requirements (e.g., under PIPEDA), you may contact us to discuss additional safeguards.

6. Data Security. We implement reasonable administrative, technical, and physical safeguards (e.g., encryption, access controls, PCI DSS compliance for payments, secure APIs) to protect Personal Information from unauthorized access, loss, or misuse. Data processed via AI is transient and not stored on third-party servers beyond what’s necessary. However, no system is completely secure, and we cannot guarantee absolute security.

7. Data Retention. We retain Personal Information as long as necessary for the purposes described (e.g., during your account’s active period, for legal obligations like tax records—typically 7 years—or for dispute resolution). When no longer needed, we delete or anonymize it securely.

8. Your Privacy Rights. Depending on your location and applicable law, you may have the following rights regarding your Personal Information:

- a. **Access/Know:** Request details on what we collect, use, disclose, or sell/share.
- b. **Deletion:** Request deletion, subject to exceptions (e.g., legal retention).
- c. **Correction/Rectification:** Request inaccurate information be corrected.
- d. **Opt-Out of Sale/Sharing:** We do not sell, but you can opt out of any “sharing” for cross-context behavioral advertising (if applicable).
- e. **Limit Use of Sensitive Information:** Request limits on sensitive data use (e.g., under CCPA/CPRA).
- f. **Portability:** Receive your data in a portable format.
- g. **Non-Discrimination:** We will not discriminate against you for exercising rights (e.g., no price increases).
- h. **Withdraw Consent:** For consent-based processing (e.g., marketing).
- i. **Complain:** File a complaint with regulators (e.g., California Attorney General, Office of the Privacy Commissioner of Canada).

U.S. State-Specific Rights: Residents of California, Virginia, Colorado, Connecticut, Utah, and other states with comprehensive privacy laws have the above rights. For CCPA/CPRA metrics from the the prior calendar year, please inquire by contacting us as provided below. We do not use Personal Information for automated decision-making with legal effects.

Canadian Rights: Under PIPEDA and provincial laws, you have rights to access, correct, and challenge compliance. We provide transparency on cross-border transfers.

To exercise rights, submit a verifiable request via email to info@zioncallmgmt.com or call 435-216-0799. We respond within required timelines (e.g., 45 days under CCPA, 30 days under PIPEDA), may require verification, and will not charge unless requests are excessive. Authorized agents may submit on your behalf with proof. For tenants/end-users: Contact your storage facility first; we process as directed by our clients.

9. Cookies and Tracking. We use cookies and similar technologies for functionality, analytics, and preferences. You can manage via browser settings, but this may limit Services. We do not use for cross-site tracking without consent.

10. Third-Party Links. Our Services may link to third-party sites; their privacy practices differ, and we are not responsible.

11. Contact Us. For questions, rights requests, or complaints:

Email: info@zioncallmgmt.com

Phone: 435-216-0799

Mail:

Zion Call Management, LLC

37 W 1070 S

Saint George, UT 84770

For Canadian residents: Contact our Privacy Officer via the above methods.

This Policy is incorporated into our Terms of Service and is subject to all terms of that Agreement. If conflict arises between this Policy and the Terms of Service/Agreement, this Policy shall prevail. If conflicts arises with laws, privacy laws prevail.