Zimna

Privacy Policy

Effective Date: March 21, 2026 | Last Updated: March 21, 2026

Zimna Inc. ("Zimna," "we," "us," or "our") operates the Zimna ERP platform, including the web application at zimna.app and the Zimna mobile application (collectively, the "Service"). This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our Service.

1. Information We Collect

1.1 Information You Provide

- **Account Information:** Full name, email address, phone number, job title, employee code, and PIN (hashed) when your employer creates your account.
- **Employment Data:** Trade/discipline, certifications, training records, skills, and work history as entered by you or your employer.
- **Financial Data:** Pay rate, tax withholding elections, direct deposit information (encrypted at rest with AES-256-GCM), and garnishment orders.
- **Communications:** Messages sent through the in-app chat feature, including text content and timestamps.
- **Documents:** Files uploaded to the document management system, including safety forms, certifications, and project documents.
- **Safety Reports:** Incident reports, toolbox talk attendance, and safety observations.

1.2 Information Collected Automatically

- **Location Data:** GPS coordinates when you clock in or clock out using the mobile app. Location is collected only at the moment of clock action and is not tracked continuously.
- **Device Information:** Device model, operating system version, app version, and a unique device identifier for push notification delivery and session management.
- **Usage Data:** Pages visited, features used, timestamps, and interaction patterns for performance monitoring.
- **Crash Data:** Automatic crash reports and diagnostic information to identify and fix bugs.

1.3 Information From Your Employer

Your employer (the "Tenant") provides most of your account and employment data. Zimna processes this data on behalf of the Tenant as a data processor. Your employer is the data controller and determines what data is collected.

2. How We Use Your Information

Purpose	Data Used	Legal Basis
Authentication	Name, PIN, device info	Contract
Time tracking	Clock times, GPS	Contract
Payroll processing	Hours, pay rate, tax	Contract / Legal
Safety compliance	Incidents, training	Legal obligation
Communication	Chat messages	Contract
Push notifications	Device token, prefs	Consent
Service improvement	Usage, crash data	Legitimate interest

3. How We Share Your Information

- **With Your Employer:** Your Tenant administrator has access to your employment data, timesheets, and activity within the platform.
- **Payroll Providers:** Relevant employment and tax data is transmitted to integrated payroll processing services.
- **Cloud Infrastructure:** Data is stored on Google Cloud Platform (GCP) infrastructure in the United States.
- **Legal Requirements:** We may disclose information if required by law, regulation, legal process, or governmental request.
- **Business Transfers:** In connection with a merger or acquisition, your data may be transferred to the acquiring entity.

We do not sell your personal information. We do not share your data with third parties for advertising purposes.

4. Data Security

- **Encryption in Transit:** All data transmitted between your device and our servers uses TLS 1.2 or higher.
- **Encryption at Rest:** Sensitive data including direct deposit information is encrypted using AES-256-GCM.
- **Authentication:** JWT tokens with Ed25519 signatures, stored in httpOnly cookies (web) or device Keychain (mobile). Optional MFA via TOTP.
- **Access Control:** Role-based access control (RBAC) ensures users only see data appropriate to their role. Row-level security (RLS) enforces tenant isolation.
- **Audit Logging:** All data access and modifications are logged in an immutable audit trail.
- **Infrastructure:** Hosted on Google Cloud Platform with SOC 2 Type II certified infrastructure.

5. Data Retention

- **Active Accounts:** Data retained for subscription duration plus 90 days after termination.
- **Payroll Records:** Retained minimum 7 years (IRS regulations and state labor laws).
- **Safety Records:** Retained minimum 5 years (OSHA regulations).
- **Audit Logs:** Retained 7 years.
- **Chat Messages:** Retained for subscription duration.

- **After Deletion:** Data permanently deleted within 90 days, except where retention is required by law.

6. Your Rights

Depending on your jurisdiction, you may have the following rights:

- **Access:** Request a copy of your personal data.
- **Correction:** Request correction of inaccurate data.
- **Deletion:** Request deletion of your personal data (subject to legal retention requirements).
- **Portability:** Request your data in a structured, machine-readable format.
- **Restriction:** Request restriction of processing in certain circumstances.
- **Objection:** Object to processing based on legitimate interests.

To exercise these rights, contact your employer (Tenant administrator) first. For platform-level requests, contact privacy@zimna.app.

7. California Privacy Rights (CCPA)

If you are a California resident, you have the right to know what personal information is collected, request deletion, opt out of sale (we do not sell data), and non-discrimination for exercising your rights.

8. Children's Privacy

The Service is not intended for individuals under 16. We do not knowingly collect personal information from children.

9. International Data Transfers

Your data is stored and processed in the United States on Google Cloud Platform infrastructure.

10. Changes to This Policy

We may update this Privacy Policy from time to time. We will notify users of material changes through the Service or via email.

11. Contact Us

Email: privacy@zimna.app

Support: zimna.app/support