Zimna

Privacy Policy

Effective Date: October 13, 2026 • Last Updated: October 13, 2026

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

Zimna is an operations and financial management platform for project-based industrial companies. Because the Service handles payroll, accounting, banking, and payment records, this Policy describes our financial data practices in detail in Sections 3 and 4.

1. Our Role: Controller and Processor

Zimna acts in two distinct capacities:

- **As a processor (service provider).** For substantially all data in the platform — employee records, payroll data, project financials, accounting records, customer and vendor information — your employer or the contracting company (the "Tenant") is the controller. Zimna processes that data solely on the Tenant's documented instructions and under our agreement with them. If you are an employee, customer, or vendor of a Tenant, the Tenant decides what is collected and how long it is kept.
- **As a controller.** For our own business relationship with the Tenant — subscription billing, account administration, support communications, security telemetry, and this website — Zimna determines the purposes and means of processing.

Where this Policy describes rights or choices, the practical route usually runs through your Tenant. See Section 10.

2. Information We Collect

2.1 Information You Provide

- **Account information:** Full name, email address, phone number, job title, employee code, and PIN or password (never stored in plaintext — see Section 8).
- **Employment data:** Trade or discipline, certifications, training records, skills, and work history.
- **Communications:** Messages sent through the in-app chat, comments, and notes.
- **Documents:** Files uploaded to the document management system, including receipts, invoices, signed agreements, and photos.
- **Signatures:** Handwritten or typed electronic signatures, together with the signing audit trail (timestamp, IP address, and document version).
- **Safety reports:** Incident reports, job hazard analyses, toolbox talk attendance, and safety observations.

© 2026 Zimna Inc. All rights reserved.

2.2 Financial and Payroll Information

Because the Service stores payroll records and runs accounting, it processes categories of data that are sensitive under laws such as the California Privacy Rights Act and comparable state statutes.

Worker payroll and tax data:

- Social Security Number or other taxpayer identification number
- Tax withholding elections (federal, state, and local)
- Pay rate, salary or hourly classification, and earning rates
- Bank account and routing numbers for direct deposit
- Garnishment and child support withholding orders
- Paystubs, W-2 and 1099 statements, and generated tax packages
- Home and work address, used to determine applicable state and local tax jurisdictions

Company financial data:

- Employer Identification Number, legal entity type, and industry classification
- General ledger accounts, journal entries, and chart of accounts
- Customer invoices, accounts receivable, and payment applications
- Vendor bills, accounts payable, expense reports, and employee reimbursements
- Corporate card transactions and attached receipts
- Bank account connections, balances, and transaction feeds (see Section 4.3)
- Project budgets, cost records, change orders, and job costing data

Counterparty data. When a Tenant records a customer or vendor, we process business contact and financial information about that organization and its representatives: legal name and DBA, taxpayer identification number, W-9 status, addresses, contact names, emails and phone numbers, payment terms, 1099 eligibility, and banking details held on file for payment.

Subscription billing data. For the Tenant's own subscription to Zimna: billing contact, plan tier, and subscription status. Zimna never receives or stores full payment card numbers. Card details are collected and held by our payment processor (see Section 7).

2.3 Information Collected Automatically

- **Location data:** GPS coordinates at the moment you clock in or clock out, and when submitting certain field records. Location is captured at the moment of the action only — Zimna does not track your location continuously or in the background.
- **Device information:** Device model, operating system version, app version, and a unique device identifier used for push notifications.
- **Usage data:** Pages visited, features used, and interaction patterns for performance monitoring.
- **Security telemetry:** Authentication events, IP address, session activity, and audit records of actions taken in the platform.
- **Crash data:** Automatic crash reports and diagnostic information.

© 2026 Zimna Inc. All rights reserved.

2.4 Information From Your Employer

Your Tenant provides most of your account and employment data, including your role, assignments, pay rate, and employment status.

2.5 Information From Third Parties

- **Your Tenant's payroll provider:** Payroll records the Tenant imports into Zimna from its own payroll provider, which may include hours, wages, withholding, payroll run status, tax filing status, tax deposit records, compliance notices, and tax documents (see Section 4.1).
- **Bank connection provider:** Account metadata, balances, and transaction records for accounts the Tenant has connected (see Section 4.3).
- **Email delivery provider:** Delivery, bounce, and open events for transactional emails such as invoices and notifications.

3. How We Use Your Information

PURPOSE	DATA USED	LEGAL BASIS
Authentication and account security	Name, credentials, device info, IP	Contract; legitimate interest
Time tracking and attendance	Clock times, GPS at clock action	Contract
Storing and reporting on imported payroll records	Hours, wages, pay rate, tax elections, withholding, TIN, bank details, jurisdiction	Contract; legal obligation
Accounting and general ledger	Transactions, invoices, bills, payments	Contract; legal obligation
Bank reconciliation and expense management	Bank and card transaction feeds, receipts	Contract
Accounts receivable and payable	Customer and vendor records, invoices, bills	Contract
Project cost tracking and job costing	Labor, material, and expense records	Contract
Safety and regulatory compliance	Incident reports, training, certifications	Legal obligation
Communication	Chat messages, notifications	Contract

© 2026 Zimna Inc. All rights reserved.

PURPOSE	DATA USED	LEGAL BASIS
AI-assisted features	Content you submit to the assistant (see Section 5)	Contract; consent where required
Push notifications	Device token, preferences	Consent
Subscription billing	Tenant billing contact, plan, usage	Contract
Service improvement and reliability	Usage data, crash reports, aggregated metrics	Legitimate interest
Fraud prevention and audit	Audit logs, security telemetry	Legal obligation; legitimate interest

We do not use your personal or financial information for advertising, for credit scoring or underwriting, for building consumer profiles, or to train general-purpose AI models. See Section 5.

4. Financial Data and Money Movement

This section explains, plainly, what Zimna does and does not do with money and financial data.

Zimna is not a bank, money transmitter, lender, or financial adviser. We record and coordinate financial activity; we do not hold customer funds.

4.1 Payroll Records

Zimna does not run payroll. A Tenant may import payroll records — for example hours, wages, withholding, and tax records — into Zimna from its own payroll provider. Zimna stores these records and uses them to provide the Service to that Tenant, such as accounting and reporting.

Zimna does not calculate payroll, withhold or file taxes, generate ACH or NACHA files, or initiate wage payments or bank transfers. Those functions remain with the Tenant and its payroll provider.

4.2 Vendor Payments, Reimbursements, and Customer Payments

Zimna records payments; it does not execute them. When a Tenant pays a vendor bill, reimburses an employee, or receives a customer payment, the actual transfer happens outside Zimna — by check, wire, or the company's own banking channel — and an authorized user records the completed payment in the platform. Zimna has no external payment rail for accounts payable or accounts receivable and does not have the ability to move money out of a Tenant's bank account.

4.3 Bank and Card Connections

A Tenant may connect its business bank and corporate card accounts through Plaid Inc. to import transactions for reconciliation and expense capture. This connection is read-only: Zimna receives account details, balances, and transaction history, and cannot initiate payments or transfers through it.

© 2026 Zimna Inc. All rights reserved.

Access credentials for these connections are stored as encrypted tokens; Zimna never receives or stores your online banking username or password — those are entered directly with Plaid and your financial institution. A Tenant administrator can disconnect a linked account at any time, which revokes Zimna's access to that account's data going forward.

Imported card transactions are presented for human review. A transaction becomes an accounting record only when a person confirms it.

4.4 Subscription Payments

Zimna's own subscription fees are processed by Stripe, Inc. Payment card data is submitted directly to Stripe and is never transmitted to or stored on Zimna systems. Zimna retains only the subscription status, plan, and billing contact.

4.5 What We Will Not Do With Financial Data

We do not sell financial data. We do not share it with data brokers, advertisers, or marketing partners. We do not use it to make automated decisions with legal or similarly significant effects about you, and we do not provide it to consumer reporting agencies.

5. AI-Assisted Features

The Service includes AI-assisted features: an in-app assistant, form and document assistance, receipt and transaction classification, question answering over Tenant data, and optional voice interaction.

How it works. When you use an AI feature, the relevant content — your question and the specific records needed to answer it — is sent to a third-party model provider (currently OpenAI and Anthropic) acting as our processor under contract. These providers are contractually prohibited from using your content to train their models.

Sensitive fields are withheld by design. The assistant is blocked at the application layer from accessing the most sensitive categories in the system, including: Social Security Numbers and taxpayer identification numbers, bank account and direct deposit details, individual pay rates, per-person gross and net pay, garnishment records, and per-person tax withholding. This is enforced in code, not by policy alone.

Humans stay in the loop. AI suggestions — expense categorization, transaction classification, form prefill — are recommendations only. They never post an accounting entry, approve a document, or finalize a record without a person confirming.

Voice features. When you use voice interaction, audio is processed to produce a transcript and a response. Network relay infrastructure (Twilio's Network Traversal Service) is used to establish the connection; it carries encrypted media and cannot read the content.

Availability. AI features can be disabled by a Tenant administrator.

6. Automated Decision-Making

Zimna does not make decisions producing legal or similarly significant effects about you through automated means alone. Approvals, disciplinary matters, pay changes, and payment authorizations

© 2026 Zimna Inc. All rights reserved.

are performed by authorized people at your employer, using the platform as a tool.

7. How We Share Your Information

With your employer. Your Tenant's administrators can access your employment data and your activity within the platform, subject to the permissions the Tenant configures.

With other participants in a transaction. Where you are a customer or vendor contact, relevant records (invoices, orders, signed documents, portal messages) are visible to the Tenant that engaged you.

With subprocessors. We use the following categories of service providers, each bound by contract to process data only on our instructions:

PROVIDER	PURPOSE	DATA CATEGORIES	LOCATION
Google Cloud Platform	Hosting, database, file storage	All platform data	United States
Plaid	Bank and card transaction feeds	Bank connection tokens, account and transaction data	United States
Stripe	Subscription billing for Zimna	Tenant billing contact; card data held by Stripe	United States
SendGrid (Twilio) / Resend	Transactional email and delivery events	Recipient address, message content, delivery status	United States
Twilio Network Traversal	Voice session network relay	Connection metadata only	Global
OpenAI / Anthropic	AI assistant and classification	Submitted content, excluding blocked sensitive fields (Section 5)	United States

A current list of subprocessors is available on request at privacy@zimna.app.

For legal reasons. We may disclose information where required by law, subpoena, or valid legal process, or to protect the rights, safety, or property of Zimna, our customers, or the public.

In a business transfer. If Zimna is involved in a merger, acquisition, or sale of assets, data may transfer as part of that transaction, subject to this Policy.

We do not sell your personal information, and we do not share it for cross-context behavioral advertising.

8. Data Security

- **Encryption in transit:** TLS for all client and service-to-service traffic. SSL-required PostgreSQL connections.

© 2026 Zimna Inc. All rights reserved.

- **Encryption at rest:** AES-256-GCM with envelope encryption and per-operation nonces for sensitive fields, including bank account details, taxpayer identification numbers, and third-party access tokens such as bank connection credentials.
- **Authentication:** JWTs signed with Ed25519, with algorithm-confusion protection; optional multi-factor authentication via TOTP; passwords and PINs hashed with Argon2id.
- **Access control:** Granular role-based access control combined with PostgreSQL row-level security. The application connects to the database under non-superuser roles that cannot bypass row-level security policies, with per-module database roles limiting the blast radius of any single component.
- **Audit logging:** Immutable audit trail enforced at the database layer — UPDATE and DELETE on audit tables are blocked by triggers. Personal data in audit payloads is masked by a declarative policy that fails closed for unrecognized event types, with automated checks in the build pipeline to catch drift.
- **Sensitive export controls:** Bulk exports containing taxpayer identification numbers require elevated permissions and are rate-limited and individually audited.
- **Webhook integrity:** Inbound and outbound webhooks are signed with HMAC-SHA256 and protected against replay.
- **Secrets management:** All credentials, signing keys, and API tokens are stored in Google Cloud Secret Manager — never in source code or environment files.
- **Resilience:** Daily database backups, point-in-time recovery, and a transactional outbox pattern that guarantees event delivery atomicity.
- **Continuous hardening:** Changes are gated by automated security scanning, dependency vulnerability checks, and architectural conformance tests before merge.

Zimna is built in alignment with SOC 2 controls. A formal SOC 2 Type I audit is on our roadmap. No system is perfectly secure, and we cannot guarantee absolute security.

9. Data Retention

Retention is driven by the Tenant's instructions and by legal minimums:

CATEGORY	RETENTION
Active accounts	Duration of subscription + 90 days
Payroll and tax records	Minimum 7 years
Accounting records, invoices, bills, payments	Minimum 7 years
Bank and card transaction feeds	Duration of subscription + 90 days, unless attached to an accounting record
Safety records	Minimum 5 years (OSHA)

© 2026 Zimna Inc. All rights reserved.

CATEGORY	RETENTION
Signed documents and signature audit trails	Minimum 7 years
Audit logs	7 years
Chat messages and operational communications	Per Tenant configuration
AI interaction logs	Retained short-term for reliability and abuse prevention

Where a record must be retained for legal reasons, we may anonymize the personal elements rather than delete the record.

10. Your Rights

Depending on your jurisdiction, you may have the right to access, correct, delete, port, restrict, or object to the processing of your personal data, and to withdraw consent where processing is based on consent.

Sensitive personal information. Some data we process — Social Security Numbers, financial account details, and precise geolocation — is treated as sensitive personal information under laws including the California Privacy Rights Act. We use it only to provide the Service and to meet legal obligations, and never to infer characteristics about you.

How to exercise your rights. Because Zimna acts as a processor for most data, contact your employer or the Tenant administrator first — they control the record and can act immediately. For platform-level requests, or if you cannot reach the Tenant, write to privacy@zimna.app. We will respond within the timeframe required by applicable law and will not discriminate against you for exercising a right.

Complaints. If you are in a jurisdiction with a supervisory authority, you may lodge a complaint with it.

11. International Data Transfers

The Service is hosted in the United States, and our subprocessors process data primarily in the United States. If you access the Service from outside the United States, your information will be transferred to and processed there, under appropriate safeguards where required by law.

12. Children's Privacy

The Service is not intended for individuals under 16. We do not knowingly collect data from children. If we learn that we have collected such data, we will delete it.

© 2026 Zimna Inc. All rights reserved.

13. Changes to This Policy

We will update this Policy as the Service changes. Material changes will be announced in-product or by email to Tenant administrators before they take effect, and the "Last Updated" date above will be revised.

14. Contact Us

- Privacy: privacy@zimna.app
- Security reports: security@zimna.app
- Support: zimna.app/support

© 2026 Zimna Inc. All rights reserved.