

Mizu CRM Privacy Policy

ENGINEERING DRAFT FOR COUNSEL REVIEW Not counsel-signed. Package 2026.08.22-fix11. Generated 2026-09-30. Authentication: Supabase Auth exclusively.

Mizu CRM Privacy Policy (engineering draft)

Status: DRAFT FOR COUNSEL REVIEW not counsel-signed

Last engineering update: 2026-08-22

HTML: `/legal/privacy`

PDF: `/legal/mizu-crm-privacy.pdf`

1. Who we are

Mizu CRM, Inc. ("Mizu CRM", "we", "us", or "our") operates the Mizu CRM platform and related services. This Privacy Policy explains how we collect, use, share, and protect personal data when you use our services, visit our website, or interact with us.

If you are a customer using Mizu CRM to manage your own contacts and data, you are the data controller for that data and Mizu CRM is your data processor. Our Data Processing Agreement (DPA) governs that relationship. This policy covers our own use of personal data (account, billing, website).

2. Data we collect

Account data: name, email, company, job title, and billing information. Authentication is provided by Supabase Auth.

Usage data: pages visited, features used, and actions taken.

Device and technical data: IP address, browser type, operating system, and device identifiers.

Communications: emails, support tickets, or other messages you send us.

Marketing preferences: opt-in / opt-out status.

We do not collect sensitive personal data (health, financial account, or government ID) as part of our standard service.

3. How we use your data

We use personal data to provide and improve services; process payments; send transactional email; send marketing where consented; respond to support; monitor security and prevent fraud; comply with law; and analyze usage. We do not sell personal data. We do not use customer data to train AI or machine learning models.

4. Data sharing

We share data with subprocessors who help deliver the service (hosting, payments, email, monitoring), when required by law, in connection with a business transfer, or with your consent. See [`/trust#subprocessors`](#) and [`/legal/subprocessors.pdf`](#). We never sell personal data or share it with advertising networks.

5. Data retention

We retain personal data while your account is active, plus a 90-day grace period after deletion, then permanently delete subject to legal retention (e.g. financial records up to 7 years). Audit logs: 12 months. Marketing consent records: 3 years from withdrawal. Request deletion: privacy@mizucrm.com.

6. Your rights

Depending on location: access, correction, deletion, portability, objection, restriction, and withdraw consent. Email privacy@mizucrm.com; we respond within 30 days. EU/EEA users may lodge a complaint with a supervisory authority.

7. Cookies

Essential cookies are required for auth and security. Analytics and marketing cookies follow consent. See Cookie Policy at [`/legal/cookies`](#).

8. International transfers

Mizu CRM is headquartered in the United States. If you are in the EU, EEA, or UK, your data may be transferred to and processed in the US or other countries when you choose a US data region or when required subprocessors operate globally. We use appropriate safeguards (including Standard Contractual Clauses / UK IDTA as applicable). Customers may select regional hosting options where offered. See data residency settings and the Trust Center.

9. Security

We implement TLS, application-layer encryption for sensitive fields, RBAC, MFA/SSO options, and org-scoped audit logging. SOC 2 Type II and ISO 27001 independent attestations are in progress see [`/trust`](#). Report issues: security@mizucrm.com.

10. Children

Mizu CRM is not directed at children under 16. We do not knowingly collect personal data from children.

11. Changes

Material changes are notified by email and site notice at least 30 days before effective date. Continued use after the effective date constitutes acceptance.

12. Contact

privacy@mizucrm.com · dpo@mizucrm.com · eu-rep@mizucrm.com (EU/EEA)

