Privacy Policy

Last updated: June 18, 2026

CadreIQ Inc. ("CadreIQ," "we," "us," or "our") provides a software platform that helps business and revenue teams analyze sales, customer relationship management, performance, workflow, and related operational data.

This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information when you visit our website, use our platform, communicate with us, or otherwise interact with CadreIQ.

This Privacy Policy should be reviewed with legal counsel before publication.

1. Scope

This Privacy Policy applies to:

- Visitors to CadreIQ websites.
- Users of CadreIQ products and services.
- Customer administrators and authorized users.
- Individuals who communicate with us by email, form submission, demo request, sales process, support request, or other business interaction.

This Privacy Policy does not apply to third-party websites, products, or services that we do not control.

2. Personal Information We Collect

We may collect the following categories of personal information.

Account and Contact Information

We may collect information such as:

- Name.
- Business email address.
- Company name.
- Job title or role.
- Phone number.
- Account credentials or authentication-related information.

- Customer, tenant, or organization identifiers.

Customer and Platform Data

Customers and authorized users may provide or connect data to the CadreIQ platform. Depending on customer configuration and integrations, this may include:

- CRM data, such as account, opportunity, lead, contact, activity, task, event, pipeline, and sales process information.
- Performance, coaching, workflow, playbook, goal, team, manager, and analytics data.
- Calendar, email, meeting, or scheduling metadata where integrations are enabled.
- User-generated content, prompts, notes, configuration settings, and platform activity.
- Outputs, recommendations, scores, summaries, insights, and analytics generated through the platform.

CadreIQ processes customer-provided data to provide the services requested by the customer.

Integration Data

If a customer enables integrations, we may process information from connected services such as Salesforce, Nylas-supported calendar or communication services, or other customer-authorized systems.

The information processed depends on the integration enabled, customer configuration, user permissions, and the data made available by the connected service.

AI and Model-Related Data

CadreIQ may use AI and model service providers to support product functionality, analysis, recommendations, summaries, and related workflows.

Depending on product use, this may involve processing customer-provided business context, prompts, retrieved context, generated outputs, and related metadata. We use these services to provide and improve the functionality of the CadreIQ platform, subject to customer agreements and applicable vendor terms.

CadreIQ does not approve the use of plaintext secrets, credentials, or unnecessary sensitive personal information in prompts or AI workflows.

Usage, Device, and Log Data

When you use our website or platform, we may automatically collect:

- IP address.
- Browser type and version.
- Device type.
- Operating system.
- Pages or features used.
- Date and time of activity.
- Referring pages.
- Authentication, access, application, diagnostic, and security logs.
- Error, performance, and usage information.

We use this information for security, troubleshooting, operations, analytics, support, and service improvement.

Communications and Support Information

If you contact us, we may collect:

- Message contents.
- Contact information.
- Support request details.
- Attachments or screenshots you provide.
- Sales, demo, or customer success communications.

Please do not send plaintext passwords, API keys, access tokens, private keys, or other secrets through support channels.

3. How We Use Personal Information

We may use personal information to:

- Provide, operate, maintain, and secure the CadreIQ platform.
- Create and manage accounts.
- Authenticate users and manage access.
- Process customer-authorized integrations.
- Generate analytics, recommendations, summaries, scores, workflows, or other platform outputs.
- Provide customer support.

- Communicate about product, security, account, billing, support, or administrative matters.
- Monitor, troubleshoot, and improve service performance.
- Detect, prevent, and investigate fraud, misuse, security incidents, vulnerabilities, or unauthorized access.
- Maintain records, audit logs, and compliance evidence.
- Enforce agreements and policies.
- Comply with legal, regulatory, contractual, or customer obligations.
- Evaluate and improve our website, platform, and business operations.

4. How We Share Personal Information

We may share personal information in the following circumstances.

With Service Providers and Vendors

We may share information with vendors that help us provide, secure, operate, monitor, support, or improve our services.

Current vendor categories may include:

- Cloud infrastructure and hosting providers, such as AWS.
- Source code, development, and operational tooling providers, such as GitHub.
- Compliance and evidence management providers, such as Drata.
- AI and model providers, such as OpenAI.
- Search, enrichment, integration, or data-processing providers, such as Tavily and Nylas where applicable.
- CRM and customer-authorized integration providers, such as Salesforce.
- Communication, productivity, documentation, and ticket-tracking providers, such as email providers and Notion where applicable.
- Contractors and technical service providers supporting CadreIQ operations.

Vendors are reviewed based on risk, data access, and business purpose. We require vendors to protect information consistent with applicable agreements, standard terms, security commitments, and the nature of the services they provide.

With Customer-Authorized Integrations

If a customer enables or authorizes an integration, we may exchange information with that integration to provide the requested service.

With Customers and Authorized Users

Information may be available to customer administrators, authorized users, or other users within the same customer account or tenant according to product functionality, permissions, and customer configuration.

Business Transactions

We may disclose or transfer information in connection with a merger, acquisition, financing, reorganization, sale of assets, bankruptcy, or similar business transaction.

Legal, Security, and Compliance Purposes

We may disclose information when we believe it is reasonably necessary to:

- Comply with law, legal process, or governmental requests.
- Enforce agreements or policies.
- Protect the rights, property, safety, or security of CadreIQ, customers, users, or others.
- Detect, investigate, or prevent fraud, abuse, security incidents, or unauthorized access.
- Respond to legal claims or regulatory inquiries.

With Consent

We may share information with your consent or at your direction.

5. Cookies and Similar Technologies

We may use cookies, local storage, pixels, logs, and similar technologies to operate our website and platform, remember preferences, authenticate users, analyze usage, improve performance, and support security.

You may be able to control cookies through your browser settings. Some features may not function properly if cookies are disabled.

6. Data Retention

We retain personal information for as long as reasonably necessary to provide the services, maintain business records, comply with legal or contractual obligations, resolve disputes, enforce agreements, maintain security, support audit and compliance needs, and operate our business.

Customer data is generally retained while the customer relationship or business need is active, unless deletion is required by contract, law, approved request, or internal decision.

Backups, logs, audit records, and security evidence may retain data after deletion from primary systems until normal retention or lifecycle periods expire, unless a specific deletion process is legally required and technically feasible.

Retention periods may vary by system, data type, customer agreement, legal requirement, and operational need.

7. Deletion, Access, and Correction

Depending on your location, relationship with CadreIQ, and applicable law, you may have rights to request access, correction, deletion, restriction, portability, or objection regarding personal information.

Customers and users may contact us to request access, correction, deletion, or other privacy-related assistance.

We may need to verify your identity or authority before fulfilling a request. We may also retain certain information when required or permitted for legal, security, fraud prevention, contractual, audit, backup, or operational reasons.

If your information is processed by CadreIQ on behalf of a customer, we may direct your request to the applicable customer or process the request according to the customer agreement.

8. Security

CadreIQ uses administrative, technical, and organizational safeguards designed to protect personal information.

These safeguards may include:

- Access controls and least privilege.
- Multi-factor authentication for critical systems where supported.
- Cloud-native logging and monitoring.
- Encryption in transit and at rest where supported.
- AWS-managed and vendor-managed security controls.
- Secrets management through approved systems.
- Backup and recovery processes.
- Vendor risk review.

- Security policies, incident response procedures, and vulnerability management processes.

No method of transmission or storage is completely secure. We cannot guarantee absolute security.

9. International Data Transfers

CadreIQ is based in the United States. We and our vendors may process information in the United States and other locations where we or our service providers operate.

Where required, we use appropriate safeguards for cross-border processing based on applicable law, customer agreements, and vendor terms.

10. Children's Privacy

CadreIQ services are not directed to children under 13, and we do not knowingly collect personal information from children under 13.

If we learn that we have collected personal information from a child under 13 without appropriate consent, we will take steps to delete it as required by law.

11. Third-Party Links and Services

Our website or platform may contain links to third-party websites or services. We are not responsible for the privacy practices, security practices, or content of third-party services that we do not control.

Your use of third-party integrations may also be subject to the privacy policies and terms of those third parties.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. When we update it, we will revise the "Last updated" date above.

If changes are material, we may provide additional notice through the website, platform, email, or other appropriate means.

13. Contact Us

If you have questions about this Privacy Policy or CadreIQ's privacy practices, you may contact us at:

Email: james@cadreiq.com

CadreIQ Inc.
Dallas, TX
United States